

WIPO/PCT

WO 2023/212903 A1

中继通信的方法及设备

技术领域

本申请实施例涉及通信领域，并且更具体地，涉及一种中继通信的方法及设备。

5

背景技术

在通过中继设备 (relay) 实现源终端和目标终端通信的架构 (终端至终端中继 (UE-to-UE relay)) 中，如何保证终端身份安全与通信数据的机密性与完整性，是一个需要解决的问题。

10 发明内容

本申请实施例提供了一种中继通信的方法及设备，能够保证终端身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

第一方面，提供了一种中继通信的方法，该方法包括：

第一终端设备接收第二终端设备通过中继设备发送的认证请求消息；

15

其中，该认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该中继设备所属用户的信息，该第二终端设备生成的第一临时公钥，该第二终端设备的签名，该中继设备的签名，该中继设备的相关信息；

20

其中，该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK；该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK；该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥；该中继设备的签名的输入参数包括以下至少之一：该第二终端设备的签名和该中继设备所属用户的信息；该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥；该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

第二方面，提供了一种中继通信的方法，该方法包括：

25

第二终端设备通过中继设备向第一终端设备发送认证请求消息；

其中，该认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该第二终端设备生成的第一临时公钥，该第二终端设备的签名，该中继设备的相关信息；

30

其中，该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK；该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥；该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥；该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

第三方面，提供了一种中继通信的方法，该方法包括：

35

中继设备接收第二终端设备发送的认证请求消息；其中，该认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该第二终端设备生成的第一临时公钥，该第二终端设备的签名；其中，该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK；该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥；该第一临时公钥和该中继设备的相关信息用于第一终端设备派生第一密钥；

40

在该第二终端设备的 KPAK 有效，且基于该第二终端设备的标识和该第二终端设备的 PVT 对该第二终端设备的签名验证成功的情况下，该中继设备向该第一终端设备发送验证之后的认证请求消息；其中，该验证之后的认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该中继设备所属用户的信息，该第一临时公钥，该第二终端设备的签名，该中继设备的签名，该中继设备的相关信息；其中，该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK；该中继设备的签名的输入参数包括以下至少之一：该第二终端设备的签名和该中继设备所属用户的信息；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

45

第四方面，提供了一种中继通信的方法，该方法包括：

第一终端设备通过中继设备向第二终端设备发送第一消息；

50

其中，该第一消息包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的第二临时公钥，该第一终端设备生成的第一密钥的标识的 M 个比特位，该第一终端设备的签名，第一消息验证码；

其中，该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和

KPAK; 该第一终端设备的签名的输入参数包括以下至少之一: 该第一终端设备所属用户的信息, 该第二临时公钥, 该 M 个比特位, 该第二终端设备的签名;

其中, 该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护, 且该第一消息验证码的输入参数包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该第一随机数, 该第二临时公钥, 该 M 个比特位, 该第一终端设备的签名;

其中, 该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥, 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥, 该第二密钥用于派生完整性保护密钥和/或机密性保护密钥, 该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数;

其中, 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器。

第五方面, 提供了一种中继通信的方法, 该方法包括:

第二终端设备接收第一终端设备通过中继设备发送的第一消息;

其中, 该第一消息包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该中继设备所属用户的信息, 该第一终端设备生成的第一随机数, 该第一终端设备生成的第二临时公钥, 该第一终端设备生成的第一密钥的标识的 M 个比特位, 该第一终端设备的签名, 该中继设备的签名, 第一消息验证码;

其中, 该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK; 该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK; 该第一终端设备的签名的输入参数包括以下至少之一: 该第一终端设备所属用户的信息, 该第二临时公钥, 该 M 个比特位, 该第二终端设备的签名; 该中继设备的签名的输入参数包括以下至少之一: 该中继设备所属用户的信息, 该第一终端设备的签名, 该第二终端设备的签名, 该第一消息;

其中, 该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护, 且该第一消息验证码的输入参数包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该第一随机数, 该第二临时公钥, 该 M 个比特位, 该第一终端设备的签名;

其中, 该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥, 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥, 该第二密钥用于派生完整性保护密钥和/或机密性保护密钥, 该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数;

其中, 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器。

第六方面, 提供了一种中继通信的方法, 该方法包括:

中继设备接收第一终端设备发送的第一消息; 其中, 该第一消息包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该第一终端设备生成的第一随机数, 该第一终端设备生成的第二临时公钥, 该第一终端设备生成的第一密钥的标识的 M 个比特位, 该第一终端设备的签名, 第一消息验证码; 其中, 该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK; 该第一终端设备的签名的输入参数包括以下至少之一: 该第一终端设备所属用户的信息, 该第二临时公钥, 该 M 个比特位, 该第二终端设备的签名; 其中, 该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护, 且该第一消息验证码的输入参数包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该第一随机数, 该第二临时公钥, 该 M 个比特位, 该第一终端设备的签名;

在该第一终端设备的 KPAK 有效, 且基于该第一终端设备的标识和该第一终端设备的 PVT 对该第一终端设备的签名验证成功的情况下, 该中继设备向该第二终端设备发送验证之后的第一消息; 其中, 该验证之后的第一消息包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该中继设备所属用户的信息, 该第一终端设备生成的第一随机数, 该第一终端设备生成的与该第二临时私钥配对的第二临时公钥, 该第一终端设备生成的该第一密钥的标识的 M 个比特位, 该第一终端设备的签名, 该中继设备的签名, 该中继设备的相关信息, 该第一消息验证码; 其中, 该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK; 该中继设备的签名的输入参数包括以下至少之一: 该中继设备所属用户的信息,

该第一终端设备的签名, 该第二终端设备的签名, 该验证之后的第一消息;

其中, 该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥, 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥, 该第二密钥用于派生完整性保护密钥和/或机密性保护密钥, 该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数; 其中, 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器。

第七方面, 提供了一种中继通信的方法, 该方法包括:

第一终端设备通过中继设备向第二终端设备发送直接通信请求;

其中, 该直接通信请求包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备生成的第一临时公钥, 该第一终端设备生成的第一随机数;

其中, 该直接通信请求通过第一加密密钥进行加密, 以及该直接通信请求通过第一完整性保护密钥进行完整性保护, 该第一加密密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥, 该第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥;

其中, 该第一临时公钥和该中继设备的相关信息用于该第二终端设备派生第一密钥; 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥, 且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥, 或者, 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥;

其中, 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器。

第八方面, 提供了一种中继通信的方法, 该方法包括:

第二终端设备接收第一终端设备通过中继设备发送的直接通信请求;

其中, 该直接通信请求包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备生成的第一临时公钥, 该第一终端设备生成的第一随机数, 该中继设备的标识, 该中继设备的相关信息;

其中, 该直接通信请求通过第一加密密钥进行加密, 以及该直接通信请求通过第一完整性保护密钥进行完整性保护, 该第一加密密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥, 该第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥;

其中, 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器; 该第一临时公钥和该中继设备的相关信息用于该第二终端设备派生第一密钥; 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥, 且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥, 或者, 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

第九方面, 提供了一种中继通信的方法, 该方法包括:

中继设备接收第一终端设备发送的直接通信请求; 其中, 该直接通信请求包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备生成的第一临时公钥, 该第一终端设备生成的第一随机数; 其中, 该直接通信请求通过第一加密密钥进行加密, 以及该直接通信请求通过第一完整性保护密钥进行完整性保护, 该第一加密密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥, 该第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥;

该中继设备验证是否被配置为转发直接通信请求, 在验证通过之后该中继设备使用该第一加密密钥解密该直接通信请求以获取 QoS 和计费信息, 以及该中继设备使用该第一完整性保护密钥验证该直接通信请求的完整性, 在验证通过之后该中继设备在该直接通信请求中添加该中继设备的相关信息和该中继设备的标识, 并且该中继设备使用该第一加密密钥加密该直接通信请求, 使用该第一完整性保护密钥保护该直接通信请求的完整性;

其中, 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器; 该第一临时公钥和该中继设备的相关信息用于第二终端设备派生第一密钥; 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥, 且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥, 或者, 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

第十方面, 提供了一种终端设备, 用于执行上述第一方面中的方法。

具体地，该终端设备包括用于执行上述第一方面中的方法的功能模块。

第十一方面，提供了一种终端设备，用于执行上述第二方面中的方法。

具体地，该终端设备包括用于执行上述第二方面中的方法的功能模块。

第十二方面，提供了一种中继设备，用于执行上述第三方面中的方法。

5 具体地，该中继设备包括用于执行上述第三方面中的方法的功能模块。

第十三方面，提供了一种终端设备，用于执行上述第四方面中的方法。

具体地，该终端设备包括用于执行上述第四方面中的方法的功能模块。

第十四方面，提供了一种终端设备，用于执行上述第五方面中的方法。

10 具体地，该终端设备包括用于执行上述第五方面中的方法的功能模块。

第十五方面，提供了一种中继设备，用于执行上述第六方面中的方法。

具体地，该中继设备包括用于执行上述第六方面中的方法的功能模块。

第十六方面，提供了一种终端设备，用于执行上述第七方面中的方法。

具体地，该终端设备包括用于执行上述第七方面中的方法的功能模块。

15 第十七方面，提供了一种终端设备，用于执行上述第八方面中的方法。

具体地，该终端设备包括用于执行上述第八方面中的方法的功能模块。

第十八方面，提供了一种中继设备，用于执行上述第九方面中的方法。

具体地，该中继设备包括用于执行上述第九方面中的方法的功能模块。

第十九方面，提供了一种终端设备，包括处理器和存储器；该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，使得该终端设备执行上述第一方面或第二方面中的方法，或者，使得该终端设备执行上述第四方面或第五方面中的方法，或者，使得该终端设备执行上述第七方面或第八方面中的方法。

第二十方面，提供了一种中继设备，包括处理器和存储器；该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，使得该中继设备执行上述第三方面中的方法，或者，使得该中继设备执行上述第六方面中的方法，或者，使得该中继设备执行上述第九方面中的方法。

25 第二十一方面，提供了一种装置，用于实现上述第一方面至第九方面中的任一方面的方法。

具体地，该装置包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有该装置的设备执行如上述第一方面至第九方面中的任一方面的方法。

第二十二方面，提供了一种计算机可读存储介质，用于存储计算机程序，该计算机程序使得计算机执行上述第一方面至第九方面中的任一方面的方法。

30 第二十三方面，提供了一种计算机程序产品，包括计算机程序指令，所述计算机程序指令使得计算机执行上述第一方面至第九方面中的任一方面的方法。

第二十四方面，提供了一种计算机程序，当其在计算机上运行时，使得计算机执行上述第一方面至第九方面中的任一方面的方法。

35 通过上述第一方面至第三方面的技术方案，第一终端设备可以基于第二终端设备通过中继设备发送的认证请求消息生成第一密钥，且该认证请求消息通过签名验证的方式进行保护。以及第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥，第二密钥用于派生完整性保护密钥和/或机密性保护密钥，能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

40 通过上述第四方面至第六方面的技术方案，第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥，第二密钥用于派生完整性保护密钥和/或机密性保护密钥，能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

45 通过上述第七方面至第九方面的技术方案，第一终端设备可以基于第二终端设备通过中继设备发送的直接通信请求生成第一密钥，且该直接通信请求通过第一加密密钥进行加密，以及直接通信请求通过第一完整性保护密钥进行完整性保护。以及第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥，第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，第一终端设备生成的第一随机数、第一密钥和第二终端设备用于派生第二随机数生成第二加密密钥和/或第二完整性保护密钥，能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

50

附图说明

图1是本申请实施例应用的一种通信系统架构的示意性图。

图 2 至图 4 分别是本申请提供的 UE-to-UE 中继场景中的建立安全通信的示意性流程图。

图 5 是本申请提供的一种 UE-to-UE 中继通信的示意性流程图。

图 6 是本申请提供的另一种 UE-to-UE 中继通信的示意性流程图。

图 7 是根据本申请实施例提供的一种中继通信的方法的示意性流程图。

5 图 8 是本申请实施例所涉及的密钥分层结构的示意性图。

图 9 是根据本申请实施例提供的另一种中继通信的方法的示意性流程图。

图 10 是根据本申请实施例提供的再一种中继通信的方法的示意性流程图。

图 11 是根据本申请实施例提供的再一种中继通信的方法的示意性流程图。

图 12 是根据本申请实施例提供的再一种中继通信的方法的示意性流程图。

10 图 13 是根据本申请实施例提供的再一种中继通信的方法的示意性流程图。

图 14 至图 15 分别是本申请实施例提供的 UE-to-UE 中继场景中的建立安全通信的示意性流程图。

图 16 是根据本申请实施例提供的再一种中继通信的方法的示意性流程图。

图 17 是根据本申请实施例提供的再一种中继通信的方法的示意性流程图。

图 18 是根据本申请实施例提供的再一种中继通信的方法的示意性流程图。

15 图 19 至图 22 分别是本申请实施例提供的 UE-to-UE 中继场景中的建立安全通信的示意性流程图。

图 23 至图 31 分别是根据本申请实施例提供的终端设备的示意性框图。

图 32 是根据本申请实施例提供的一种通信设备的示意性框图。

图 33 是根据本申请实施例提供的一种装置的示意性框图。

图 34 是根据本申请实施例提供的一种通信系统的示意性框图。

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。针对本申请中的实施例，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。

25

本申请实施例的技术方案可以应用于各种通信系统，例如：全球移动通讯 (Global System of Mobile communication, GSM) 系统、码分多址 (Code Division Multiple Access, CDMA) 系统、宽带码分多址 (Wideband Code Division Multiple Access, WCDMA) 系统、通用分组无线业务 (General Packet Radio Service, GPRS)、长期演进 (Long Term Evolution, LTE) 系统、先进的长期演进 (Advanced long term evolution, LTE-A) 系统、新无线 (New Radio, NR) 系统、NR 系统的演进系统、非授权频谱上的 LTE (LTE-based access to unlicensed spectrum, LTE-U) 系统、非授权频谱上的 NR (NR-based access to unlicensed spectrum, NR-U) 系统、非地面通信网络 (Non-Terrestrial Networks, NTN) 系统、通用移动通信系统 (Universal Mobile Telecommunication System, UMTS)、无线局域网 (Wireless Local Area Networks, WLAN)、物联网 (internet of things, IoT)、无线保真 (Wireless Fidelity, WiFi)、第五代通信 (5th-Generation, 5G) 系统或其他通信系统等。

30

35

通常来说，传统的通信系统支持的连接数有限，也易于实现，然而，随着通信技术的发展，移动通信系统将不仅支持传统的通信，还将支持例如，设备到设备 (Device to Device, D2D) 通信，机器到机器 (Machine to Machine, M2M) 通信，机器类型通信 (Machine Type Communication, MTC)，车辆间 (Vehicle to Vehicle, V2V) 通信，或车联网 (Vehicle to everything, V2X) 通信等，本申请实施例也可以应用于这些通信系统。

40

在一些实施例中，本申请实施例中的通信系统可以应用于载波聚合 (Carrier Aggregation, CA) 场景，也可以应用于双连接 (Dual Connectivity, DC) 场景，还可以应用于独立 (Standalone, SA) 布网场景，或者应用于非独立 (Non-Standalone, NSA) 布网场景。

45

在一些实施例中，本申请实施例中的通信系统可以应用于非授权频谱，其中，非授权频谱也可以认为是共享频谱；或者，本申请实施例中的通信系统也可以应用于授权频谱，其中，授权频谱也可以认为是非共享频谱。

在一些实施例中，本申请实施例中的通信系统可以应用于 FR1 频段 (对应频段范围 410 MHz 到 7.125 GHz)，也可以应用于 FR2 频段 (对应频段范围 24.25 GHz 到 52.6 GHz)，还可以应用于新的频段例如对应 52.6 GHz 到 71 GHz 频段范围或对应 71GHz 到 114.25 GHz 频段范围的高频频段。

50

本申请实施例结合网络设备和终端设备描述了各个实施例，其中，终端设备也可以称为用户设备 (User Equipment, UE)、接入终端、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置等。

终端设备可以是 WLAN 中的站点 (STATION, ST)，可以是蜂窝电话、无绳电话、会话启动协议 (Session Initiation Protocol, SIP) 电话、无线本地环路 (Wireless Local Loop, WLL) 站、个人数

字助理 (Personal Digital Assistant, PDA) 设备、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备、下一代通信系统例如 NR 网络中的终端设备, 或者未来演进的公共陆地移动网络 (Public Land Mobile Network, PLMN) 网络中的终端设备等。

在本申请实施例中, 终端设备可以部署在陆地上, 包括室内或室外、手持、穿戴或车载; 也可以部署在水面上 (如轮船等); 还可以部署在空中 (例如飞机、气球和卫星上等)。

在本申请实施例中, 终端设备可以是手机 (Mobile Phone)、平板电脑 (Pad)、带无线收发功能的电脑、虚拟现实 (Virtual Reality, VR) 终端设备、增强现实 (Augmented Reality, AR) 终端设备、工业控制 (industrial control) 中的无线终端设备、无人驾驶 (self driving) 中的无线终端设备、远程医疗 (remote medical) 中的无线终端设备、智能电网 (smart grid) 中的无线终端设备、运输安全 (transportation safety) 中的无线终端设备、智慧城市 (smart city) 中的无线终端设备或智慧家庭 (smart home) 中的无线终端设备、车载通信设备、无线通信芯片/专用集成电路 (application specific integrated circuit, ASIC)/系统级芯片 (System on Chip, SoC) 等。

作为示例而非限定, 在本申请实施例中, 该终端设备还可以是可穿戴设备。可穿戴设备也可以称为穿戴式智能设备, 是应用穿戴式技术对日常穿戴进行智能化设计、开发出可以穿戴的设备的总称, 如眼镜、手套、手表、服饰及鞋等。可穿戴设备即直接穿在身上, 或是整合到用户的衣服或配件的一种便携式设备。可穿戴设备不仅仅是一种硬件设备, 更是通过软件支持以及数据交互、云端交互来实现强大的功能。广义穿戴式智能设备包括功能全、尺寸大、可不依赖智能手机实现完整或者部分的功能, 例如: 智能手表或智能眼镜等, 以及只专注于某一类应用功能, 需要和其它设备如智能手机配合使用, 如各类进行体征监测的智能手环、智能首饰等。

在本申请实施例中, 网络设备可以是用于与移动设备通信的设备, 网络设备可以是 WLAN 中的接入点 (Access Point, AP), GSM 或 CDMA 中的基站 (Base Transceiver Station, BTS), 也可以是 WCDMA 中的基站 (NodeB, NB), 还可以是 LTE 中的演进型基站 (Evolutional Node B, eNB 或 eNodeB), 或者中继站或接入点, 或者车载设备、可穿戴设备以及 NR 网络中的网络设备或者基站 (gNB) 或者未来演进的 PLMN 网络中的网络设备或者 NTN 网络中的网络设备。

作为示例而非限定, 在本申请实施例中, 网络设备可以具有移动特性, 例如网络设备可以为移动的设备。在一些实施例中, 网络设备可以为卫星、气球站。例如, 卫星可以为低地球轨道 (low earth orbit, LEO) 卫星、中地球轨道 (medium earth orbit, MEO) 卫星、地球同步轨道 (geostationary earth orbit, GEO) 卫星、高椭圆轨道 (High Elliptical Orbit, HEO) 卫星等。在一些实施例中, 网络设备还可以为设置在陆地、水域等位置的基站。

在本申请实施例中, 网络设备可以为小区提供服务, 终端设备通过该小区使用的传输资源 (例如, 频域资源, 或者说, 频谱资源) 与网络设备进行通信, 该小区可以是网络设备 (例如基站) 对应的小区, 小区可以属于宏基站, 也可以属于小小区 (Small cell) 对应的基站, 这里的小小区可以包括: 城市小区 (Metro cell)、微小区 (Micro cell)、微微小区 (Pico cell)、毫微微小区 (Femto cell) 等, 这些小小区具有覆盖范围小、发射功率低的特点, 适用于提供高速率的数据传输服务。

示例性的, 本申请实施例应用的通信系统 100 如图 1 所示。该通信系统 100 可以包括网络设备 110, 网络设备 110 可以是与终端设备 120 (或称为通信终端、终端) 通信的设备。网络设备 110 可以为特定的地理区域提供通信覆盖, 并且可以与位于该覆盖区域内的终端设备进行通信。

图 1 示例性地示出了一个网络设备和两个终端设备, 在一些实施例中, 该通信系统 100 可以包括多个网络设备并且每个网络设备的覆盖范围内可以包括其它数量的终端设备, 本申请实施例对此不做限定。

在一些实施例中, 该通信系统 100 还可以包括网络控制器、移动管理实体等其他网络实体, 本申请实施例对此不作限定。

应理解, 本申请实施例中网络/系统中具有通信功能的设备可称为通信设备。以图 1 示出的通信系统 100 为例, 通信设备可包括具有通信功能的网络设备 110 和终端设备 120, 网络设备 110 和终端设备 120 可以为上文所述的具体设备, 此处不再赘述; 通信设备还可包括通信系统 100 中的其他设备, 例如网络控制器、移动管理实体等其他网络实体, 本申请实施例中对此不做限定。

应理解, 本文中术语“系统”和“网络”在本文中常被可互换使用。本文中术语“和/或”, 仅仅是一种描述关联对象的关联关系, 表示可以存在三种关系, 例如, A 和/或 B, 可以表示: 单独存在 A, 同时存在 A 和 B, 单独存在 B 这三种情况。另外, 本文中字符“/”, 一般表示前后关联对象是一种“或”的关系。

应理解, 本文涉及第一通信设备和第二通信设备, 第一通信设备可以是终端设备, 例如手机, 机器设备, 用户前端设备 (Customer Premise Equipment, CPE), 工业设备, 车辆等; 第二通信设备可

以是第一通信设备的对端通信设备，例如网络设备，手机，工业设备，车辆等。本文中第一通信设备是终端设备和第二通信设备是网络设备为具体实例进行描述。

本申请的实施方式部分使用的术语仅用于对本申请的具体实施例进行解释，而非旨在限定本申请。本申请的说明书和权利要求书及所述附图中的术语“第一”、“第二”、“第三”和“第四”等是用于区别不同对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排除的包含。

应理解，在本申请的实施例中提到的“指示”可以是直接指示，也可以是间接指示，还可以是表示具有关联关系。举例说明，A 指示 B，可以表示 A 直接指示 B，例如 B 可以通过 A 获取；也可以表示 A 间接指示 B，例如 A 指示 C，B 可以通过 C 获取；还可以表示 A 和 B 之间具有关联关系。

在本申请实施例的描述中，术语“对应”可表示两者之间具有直接对应或间接对应的关系，也可以表示两者之间具有关联关系，也可以是指示与被指示、配置与被配置等关系。

本申请实施例中，“预定义”或“预配置”可以通过在设备（例如，包括终端设备和网络设备）中预先保存相应的代码、表格或其他可用于指示相关信息的方式来实现，本申请对于其具体的实现方式不做限定。比如预定义可以是指协议中定义的。

本申请实施例中，所述“协议”可以指通信领域的标准协议，例如可以是对现有 LTE 协议、NR 协议、Wi-Fi 协议或者与之相关的其它通信系统相关的协议的演进，本申请不对协议类型进行限定。

为便于理解本申请实施例的技术方案，以下通过具体实施例详述本申请的技术方案。以下相关技术作为可选方案与本申请实施例的技术方案可以进行任意结合，其均属于本申请实施例的保护范围。本申请实施例包括以下内容中的至少部分内容。

为实现 UE-to-UE 中继场景中的安全通信，现阶段主要包含如下三种方案。

方案一，如图 2 所示，使用非对称加密技术来保护源 UE 和目标 UE 之间的通信的方法。在源 UE 和目标 UE 互相认证的基础上，并假设中继是可信的，在源 UE 和目标 UE 之间建立连接，利用双方公钥来保护端到端安全。

方案二，如图 3 所示，UE-to-UE 中继场景中 UE1 和 UE2 之间的安全建立过程，UE1 和 UE2 分别与中继设备 1 (relay 1) 建立 PC5 连接，然后假定 UE1 和 UE2 之间与配置了共享密钥和密钥 ID，最后 UE1 通过中继设备 1 给 UE2 发送消息验证码 (Message Authentication Code, MAC)，UE2 验证消息 MAC 后再回复消息给 UE1。

方案三，如图 4 所示，远端 UE1 和远端 UE2 与中继设备建立安全 PC5 链路，远端 UE1、中继设备、远端 UE2 被 5G 直接发现名称管理网元 (Direct Discovering Name Management Function, DDNMF) 和邻近通信服务的密钥管理网元 (ProSe Key Management Function, PKMF) 提供发现和中继安全秘密材料。远端 UE1 和远端 UE2 预先从 PKMF 获得共享密钥 (key) 标识 (Identity, ID) 以及 key。然后，UE (远端 UE1 和远端 UE2) 和中继设备也会从 PKMF 获得相应密钥，分别建立 PC5 安全连接，最后远端 UE1 和远端 UE2 之间利用共享密钥建立安全通道。

为便于更好的理解本申请实施例，对本申请所涉及的终端至终端中继 (UE-to-UE relay) 通信架构及相关流程进行说明。

在 UE-to-UE relay 通信中，通信架构和对应的流程，分为两类，分别是针对层 2 (layer2, L2) 的连接和针对层 3 (layer3, L3) 的基于互联网协议 (Internet Protocol, IP) 的连接。建立 L2 的 UE-to-UE relay 的连接包括两种情况：连接建立整合在 UE-to-UE relay 的发现和选择中、连接建立在 UE-to-UE relay 的发现和选择之后。下面以连接建立整合在 UE-to-UE relay 的发现和选择中为例介绍相关流程，流程图如图 5 所示，具体可以包括如下步骤：

0. UE-to-UE Relay 向网络注册并提供 UE-to-UE Relay 功能，UE-to-UE Relay 配置了中继策略参数。

1. 目标终端 (即 UE2、UE3 和 UE4) 确定 PC5 单播链路建立时信令接收的目的 L2 ID。

2. 在源终端 (即 UE1) 上，应用层向邻近业务 (Proximity-based Services, ProSe) 层提供 PC5 单播通信的信息 (如广播 L2 ID、ProSe 应用层 ID、终端应用层 ID、目标终端应用层 ID、中继适用指示)，ProSe 层通过发送端到端广播直接通信请求消息触发终端的发现机制。消息使用源 L2 ID 和广播 L2 ID 作为目的发送，并包含其他与应用程序相关的参数。

3. UE-to-UE Relay 接收广播的直接通信请求消息，并验证它是否配置为转发这个应用程序，例如，它将宣布的 ProSe 应用 (application) ID 与它所提供的中继策略/参数进行比较。UE-to-UE Relay 转发端到端广播的直接通信请求消息时，使用自己的 L2 ID 作为源 (Source) L2 ID，并在消息中添加中继 (Relay) UE ID，在适配层指定标识 UE1 的信息。UE-to-UE Relay 在 ProSe 层处理此端到端广播消息，并根据适配层信息转发任何后续的端到端 PC5-S 消息。

4a. 目标 UE3 对宣布的应用程序感兴趣，如果 UE3 和 UE-to-UE Relay 之间不存在每跳链路，它

会触发 UE-to-UE Relay 建立每跳链路。UE3 发送每跳链路建立过程消息，源地址是 UE3 L2 ID，目的地址是中继的 L2 ID。

4b. 如果 UE-to-UE relay 和 UE1 之间不存在每跳链路，则执行 UE-to-UE relay 和 UE1 之间的每跳链路建立过程。UE1 将自己的 L2 ID 作为源地址，中继的 L2 ID 作为目的地址。

5 5. 如果步骤 4a 成功，UE1 和 UE3 之间通过 UE-to-UE Relay 交换端到端认证和安全建立消息。包括识别源终端和/或目标终端的适配层。在通过中继接收到来自 UE3 的第一个消息时，如果在中继和 UE1 之间没有现有的每跳链路，则在 UE-to-UE 中继和 UE1 之间执行每跳链路建立过程。

6. 一旦 UE3 和 UE1 之间建立了端到端的安全连接，UE3 通过发送端到端单播直接通信接受消息来完成 UE3 和 UE1 之间的端到端链路建立，该消息中包含了识别 UE1 的适配层信息。

10 7. UE-to-UE Relay 转发端到端单播直接通信接受消息，包括标识 UE3 的适配层信息。在此过程中，中继设备通过修改源字段和目标字段，发送消息到各个终端。

为便于更好的理解本申请实施例，对本申请所涉及的 ProSe 中一对多通信的安全连接建立过程进行说明。

15 ProSe 一对多通信中的密钥管理功能邻近业务的密钥管理功能（Prose Key Management Function, PKMF）网元为多个 UE 生成对称密钥，一对多的 ProSe 安全通信过程的流程如图 6 所示，具体可以包括如下步骤：

20 0a 或 0b: 如果需要，终端为了与 PKMF 连接，可以配置任何私钥，相关证书或根证书，保证密钥可以对运营商保密。如果没有提供，则使用全球用户身份模块（Universal Subscriber Identity Module, USIM）凭据来保护该接口。终端也可以预先配置 PKMF 的地址。注 1: PKMF 是一个独立的逻辑实体，允许网络运营商提供无线电级别参数，而第三方（如公共安全服务）可以控制密钥的发放。

0c 和 0d: 属于各个组的订阅者需要配置 ProSe 功能和 ProSe 密钥管理功能。PKMF 需要根据本地策略，为每个组预先选择加密算法。

25 1a 或 1b: 终端从 ProSe 功能中获取一对多的通信参数。作为这个过程的一部分，终端获得它的组身份，并被告知是否需要该组的承载层安全。此外，还可以为 UE 提供用于获取该组密钥的 PKMF 的地址。

2a.ii 或 2b.ii: PKMF 根据 UE 演进型分组系统（Evolved Packet System, EPS）安全能力检查 UE 是否支持组加密算法，即组加密算法是否包含在 UE 支持的 EPS 加密算法集中。

30 2a.iii 或 2b.iii: PKMF 以密钥响应消息进行响应。如果步骤 2a.ii 或 2b.ii 对特定组的检查成功，则该消息包含组成员身份和 UE 在发送或接收该组的受保护数据时应使用的 EPS 加密算法标识符。否则，该消息包含算法支持失败的指示符，因为 UE 不支持所需的算法。如果 PKMF 决定使用新的成对的主密钥（Pairwise Master Key, PMK），则该消息还可能包含 PMK 和相关联的 PMK ID。

2a.iv 或 2b.iv: PKMF 使用多媒体网络密钥（Multimedia Internet KEYing, MIKEY）向 UE 发送相关的 ProSe 组密钥（Prose Group Key, PGK）、PGK ID 和到期时间。

35 3a 或 3b: UE 计算 ProSe 传输密钥（Prose Traffic Key, PTK）和 ProSe 加密密钥（Prose Encrypt Key, PEK）以保护它发送到组的流量。它通过选择 PGK 并使用下一个未使用的 PTK 的身份和计数器组合来实现这一点。然后它使用步骤 2x.ii 中给出的算法保护数据。

4a 或 4b: 接收 UE 从第 2 层报头中获取逻辑信道标识（Logical Channel Identity, LC ID）、组身份和组成员身份。然后，它使用收到的 PGK 身份来识别发送方使用了哪个 PGK。UE 首先检查 PGK 是否有效，如果有效，则计算 PTK 和 PEK 以处理接收到的消息。

40 为便于更好的理解本申请实施例，对本申请所解决的问题进行说明。

45 UE-to-UE 中继场景安全通信方案均存在部分缺陷，比如上述方案一中默认 relay 是可信的，因此存在强假设条件的限制，并且在 UE 协商安全能力时均为明文消息，可能遭受篡改，另外方案一中公钥的来源和真实性、以及通信密钥来源不明确，（比如没有确定通过协商方式还是单向加密来确定通信密钥来源），同时未涉及采用公钥技术下的密钥管理方案。方案二未提及预配置共享密钥的过程，同时方案流程存在争议。方案三的流程较为复杂，交互次数过多，不够轻便。因此需探究更为简便且不失安全性的安全连接建立方式，并探究更为高效的密钥管理结构，从而保证 UE 身份安全与通信数据的机密性与完整性。

基于上述问题，本申请提出了一种中继通信的方案，能够保证终端身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

50 以下通过具体实施例详述本申请的技术方案。

图 7 是根据本申请实施例的中继通信的方法 200 的示意性流程图，如图 7 所示，该中继通信的方法 200 可以包括如下内容中的至少部分内容：

S210, 第一终端设备接收第二终端设备通过中继设备发送的认证请求消息; 其中, 该认证请求消息包括以下至少之一: 该第二终端设备所属用户的信息, 该中继设备所属用户的信息, 该第二终端设备生成的第一临时公钥, 该第二终端设备的签名, 该中继设备的签名, 该中继设备的相关信息; 其中, 该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK; 该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK; 该第二终端设备的签名的输入参数包括以下至少之一: 该第二终端设备所属用户的信息和该第一临时公钥; 该中继设备的签名的输入参数包括以下至少之一: 该第二终端设备的签名和该中继设备所属用户的信息; 该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥; 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器。

本实施例基于 ECCSI 签名方案, 建立 L2 架构下的 UE-to-UE 中继场景下的安全连接。具体的, 本申请实施例应用于 L2 架构下的 UE-to-UE 中继场景, 也即, 第一终端设备与第二终端设备之间通过中继设备进行通信。例如, 第一终端设备与第二终端设备之间的中继连接可以是 PC5 链路。

在本申请实施例中, 该第一终端设备可以是源设备或源终端, 该第二终端设备可以是目标设备或目标终端。该中继设备可以是中继终端。

在本申请实施例中, 该第二终端设备的签名的输入参数包括以下至少之一: 该第二终端设备所属用户的信息和该第一临时公钥。也即, 该第二终端设备可以基于该第二终端设备所属用户的信息和该第一临时公钥中的至少之一, 生成该第二终端设备的签名。

在本申请实施例中, 该中继设备的签名的输入参数包括以下至少之一: 该第二终端设备的签名和该中继设备所属用户的信息。也即, 该中继设备可以基于该第二终端设备的签名和该中继设备所属用户的信息中的至少之一, 生成该中继设备的签名。

在一些实施例中, 该第二终端设备的签名由该第二终端设备的秘密签名密钥 (Secret Signing Key, SSK) 生成。可选地, 该第二终端设备的公共验证令牌 (Public Validation Token, PVT) 和密钥管理服务服务器的公共认证密钥 (Key Management Service Public Authentication Key, KPAK)、以及秘密签名密钥 (SSK) 可以是可信中心密钥管理服务服务器 (Key Management Service, KMS) 通过安全通道为该第二终端设备预先配置的。该安全通道可以基于应用程序的身份验证和密钥管理 (Authentication and Key Management for Applications, AKMA) 机制或者通用引导架构 (Generic Bootstrapping Architecture, GBA) 机制来建立该第二终端设备与 KMS 的安全连接, 该 KMS 可以直接由运营商来负责管理或者是与运营商有商业关系的第三方服务提供商。

在一些实施例中, 该中继设备的签名由该中继设备的秘密签名密钥 (SSK) 生成。可选地, 该中继设备的 PVT 和 KPAK、以及秘密签名密钥 (SSK) 可以是可信中心 KMS 通过安全通道为该中继设备预先配置的。该安全通道可以基于 AKMA 机制或者 GBA 机制来建立该中继设备与 KMS 的安全连接, 该 KMS 可以直接由运营商来负责管理或者是与运营商有商业关系的第三方服务提供商。

在一些实施例中, 在该第二终端设备的 KPAK 和该中继设备的 KPAK 有效, 且基于该第二终端设备的标识和该第二终端设备的 PVT 对该第二终端设备的签名验证成功, 以及基于该中继设备的标识和该中继设备的 PVT 对该中继设备的签名验证成功的情况下, 该第一终端设备生成第二临时私钥, 以及该第一终端设备根据该第一临时公钥、该中继设备的相关信息和该第二临时私钥派生该第一密钥。

具体的, 该第一终端设备可以基于其本地存储的一个或多个 KPAK, 验证该第二终端设备的 KPAK 和该中继设备的 KPAK 的有效性。例如, 在第一终端设备本地存储的 KPAK 中存在与第二终端设备的 KPAK 一致的 KPAK 的情况下, 该第二终端设备的 KPAK 有效; 以及在第一终端设备本地存储的 KPAK 中存在与中继设备的 KPAK 一致的 KPAK 的情况下, 该中继设备的 KPAK 有效。可选地, 该第一终端设备本地存储的一个或多个 KPAK 可以由 KMS 预配置。

具体的, 在本申请实施例中, 第一终端设备可以根据第二终端设备生成的第一临时公钥、中继设备的相关信息和第一终端设备生成的第二临时私钥派生第一密钥。可选地, 第一终端设备可以根据第二终端设备生成的第一临时公钥、中继设备的相关信息和第一终端设备生成的第二临时私钥派生第一密钥; 其中, 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器。

相应的, 第二终端设备可以根据第一终端设备生成的第二临时公钥、中继设备的相关信息和第二终端设备生成的第一临时私钥派生第一密钥。可选地, 第二终端设备可以根据第一终端设备生成的第二临时公钥、中继设备的相关信息和第二终端设备生成的第一临时私钥派生第一密钥; 其中, 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器。

其中,第二终端设备生成的第一临时公钥与第二终端设备生成的第一临时私钥配对,第一终端设备生成的第二临时公钥与第一终端设备生成的第二临时私钥配对。

具体例如,第一终端设备可以根据第一临时公钥和第二临时私钥,并使用 ECIES 算法计算出第一密钥;第二终端设备可以根据第二临时公钥和第一临时私钥,并使用 ECIES 算法计算出第一密钥。

5 在一些实施例中,该第一终端设备通过该中继设备向该第二终端设备发送第一消息;

其中,该第一消息包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该第一终端设备生成的第一随机数,该第一终端设备生成的与该第二临时私钥配对的第二临时公钥,该第一终端设备生成的该第一密钥的标识的 M 个比特位,该第一终端设备的签名,第一消息验证码;

10 其中,该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK;该第一终端设备的签名的输入参数包括以下至少之一:该第一终端设备所属用户的信息,该第二临时公钥,该第一密钥的标识的 M 个比特位,该第二终端设备的签名;

15 其中,该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护,且该第一消息验证码的输入参数包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该第一随机数,该第二临时公钥,该 M 个比特位,该第一终端设备的签名。

20 具体的,该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥,该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥,该第二密钥用于派生完整性保护密钥和/或机密性保护密钥,该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数。

25 在本申请实施例中,第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥。也即,第一终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥,以及第一终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥,从而第一终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。同理,第二终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥,以及第二终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥,从而第二终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。

30 在本申请实施例中,该第一消息验证码的输入参数包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一随机数,该第二临时公钥,该 M 个比特位。也即,该第一终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第一终端设备所属用户的信息、该第二临时公钥、该 M 个比特位、该第一终端设备的签名中的至少之一,生成该第一消息验证码。

35 具体例如,假设该第一消息验证码的输入参数包括:该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第一终端设备所属用户的信息、该第二临时公钥、该 M 个比特位、该第一终端设备的签名。该第二终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位生成第一消息验证码,并与该第一消息中包含的该第一消息验证码进行比较,若比较一致的情况下,该第一消息验证码有效。

在一些实施例中,该第一消息为认证响应消息,或者,该第一消息为安全模式命令消息。

40 在一些实施例中,该第一终端设备的安全能力信息可以是该第一终端设备支持的密码算法列表。

在一些实施例中,该第一终端设备的安全策略信息可以是该第一终端设备是否支持机密性保护或完整性保护。其中,该第一终端设备的安全策略信息包括:该第一终端设备在控制面的安全策略信息,和/或,该第一终端设备在用户面的安全策略信息。

45 在一些实施例中,该 M 个比特位可以是该第一密钥的标识的最高 M 个比特位,该 N 个比特位可以是该第一密钥的标识的最低 N 个比特位;或者,该 M 个比特位可以是该第一密钥的标识的前 M 个比特位,该 N 个比特位可以是该第一密钥的标识的后 N 个比特位;或者,该 M 个比特位可以是该第一密钥的标识的偶数位的比特位,该 N 个比特位可以是该第一密钥的标识的奇数位的比特位。

在一些实施例中, M 与 N 的取值可以相同,也可以不同,本申请对此并不限定。

在一些实施例中,该第一终端设备接收该第二终端设备通过该中继设备发送的第二消息;

50 其中,该第二消息包括以下至少之一:该第二终端设备生成的该第二随机数,该第二终端设备生成的该第一密钥的标识的 N 个比特位,该第二终端设备生成的该第二密钥的标识的 x 个比特位,该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,第二消息验证码;

其中,该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护,或者,该第二

消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护,且该第二消息验证码的输入参数包括以下至少之一:该第二随机数,该N个比特位,该x个比特位,该第二终端设备选取的安全算法,该第二终端设备选取的安全策略;

其中,该第二密钥的标识由该x个比特位与该第二密钥的标识的另外y个比特位合并得到,x和y均为正整数。

在一些实施例中,该x个比特位可以是该第二密钥的标识的最高x个比特位,该y个比特位可以是该第二密钥的标识的最低y个比特位;或者,该x个比特位可以是该第二密钥的标识的前x个比特位,该y个比特位可以是该第二密钥的标识的后y个比特位;或者,该x个比特位可以是该第二密钥的标识的偶数位的比特位,该y个比特位可以是该第二密钥的标识的奇数位的比特位。

在一些实施例中,x与y的取值可以相同,也可以不同,本申请对此并不限定。

在一些实施例中,在该第二消息中携带的信息未遭受篡改的情况下,该第一终端设备至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥,该第一终端设备根据该第二密钥生成完整性保护密钥和/或机密性保护密钥,以及该第一终端设备将该M个比特位和该N个比特位合并得到该第一密钥的标识,该第一终端设备生成该第二密钥的标识的y个比特位,并将该x个比特位和该y个比特位合并得到该第二密钥的标识;

在该第二消息验证码有效的情况下,该第一终端设备根据该第二终端设备选取的安全算法、该第二密钥、基于该第二密钥生成完整性保护密钥和/或机密性保护密钥、该第二终端设备选取的安全策略,与该第二终端设备进行通信。

具体例如,假设该第二消息验证码的输入参数包括:该第二随机数、该N个比特位、该x个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略。该第一终端设备可以基于该第二随机数、该N个比特位、该x个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略生成第二消息验证码,并与该第二消息中包含的该第二消息验证码进行比较,若比较一致的情况下,该第二消息验证码有效。

在一些实施例中,该第二消息通过该第一密钥进行加密。当然,该第二消息也可以不通过该第一密钥进行加密,或者,该第二消息也可以不加密。

在一些实施例中,该第一终端设备根据该第一密钥解密该第二消息;在该第二消息中携带的信息未遭受篡改的情况下,该第一终端设备至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥,该第一终端设备根据该第二密钥生成完整性保护密钥和/或机密性保护密钥,以及该第一终端设备将该M个比特位和该N个比特位合并得到该第一密钥的标识,该第一终端设备生成该第二密钥的标识的y个比特位,并将该x个比特位和该y个比特位合并得到该第二密钥的标识;

在该第二消息验证码有效的情况下,该第一终端设备根据该第二终端设备选取的安全算法、该第二密钥、基于该第二密钥生成完整性保护密钥和/或机密性保护密钥、该第二终端设备选取的安全策略,与该第二终端设备进行通信。

具体的,该第二终端设备可以基于该第一终端设备的安全能力信息选取安全算法,和/或,该第二终端设备可以基于该第一终端设备的安全策略信息选取安全策略。

在一些实施例中,该第一终端设备可以根据该第一随机数、该第一密钥、该第二随机数,以及源标识、目标标识、该第一随机数的长度、该第二随机数的长度、该源标识的长度、该目标标识的长度中的至少之一,生成该第二密钥。其中,该源标识用于标识该第一终端设备与该第二终端设备之间的中继连接的源端,该目标标识用于标识该第一终端设备与该第二终端设备之间的中继连接的目标端。另外,该第二密钥的输入参数还可以包括其他系统设定参数,如3GPP指定的一个或多个固定参数。

在一些实施例中,该第一消息为认证响应消息,该第二消息为安全模式命令(Secure Mode Command, SMC)消息。

在一些实施例中,该第一消息为安全模式命令(SMC)消息,该第二消息为安全模式响应消息。

在一些实施例中,该第一终端设备通过该中继设备向该第二终端设备发送第三消息;

其中,该第三消息用于指示安全模式建立完成,该第三消息通过目标密钥进行加密,且该第三消息包括以下至少之一:该第二密钥的标识的该y个比特位,第三消息验证码;

其中,该目标密钥包括以下之一:该第一密钥,该第二密钥,该第二密钥派生的机密性保护密钥;

其中,该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护,或者,该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护,该第三消息验证码的输入参数包括该y个比特位。

也即,该第三消息通过该第三消息验证码进行完整性保护,该第三消息验证码基于该第二密钥生成,或者,该第三消息验证码基于该第二密钥派生的完整性保护密钥生成。

在一些实施例中,对于该第二终端设备,该第二终端设备通过该目标密钥对该第三消息进行解密;在该第三消息中携带的信息未遭受篡改的情况下,且该第三消息验证码有效的情况下,该第二终端设备将该 x 个比特位与该 y 个比特位合并得到该第二密钥的标识。具体的,该第二终端设备可以基于该 y 个比特位生成第三消息验证码,并与该第三消息中包含的该第三消息验证码进行比较,若比较一致的情况下,该第三消息验证码有效。

具体例如,该第三消息为安全模式结束消息(security mode complete)。

在一些实施例中,该第一终端设备接收该第二终端设备通过该中继设备发送的错误消息;其中,该错误消息包括以下至少之一:原因信息,第四消息验证码;其中,该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突,或者,该原因信息用于指示该第一消息验证码验证失败,或者,该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败,该第四消息验证码的输入参数包括以下至少之一:该原因信息;

在该第四消息验证码有效的情况下,该第一终端设备确定安全模式建立失败,和/或,该第一终端设备重新发起安全模式建立流程。

在一些实施例中,该错误消息也可以受完整性保护。

具体例如,该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突,例如,该第二终端设备不支持该第一消息中携带的该第一终端设备的安全策略信息。

具体例如,该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败,例如,该第二终端设备不支持该第一消息中携带的该第一终端设备的安全能力信息。

在一些实施例中,该第一密钥可以是 K_D ,该第一密钥的标识可以是 K_D ID;该第二密钥可以是 K_{D-SESS} ,该第二密钥的标识可以是 K_{D-SESS} ID。

在一些实施例中,对于第一终端设备而言,生成第一密钥时的输入参数包括:第一终端设备生成的第二临时私钥(Ephemeral private key2)、第二终端设备生成的第一临时公钥(Ephemeral public key1),以及中继设备的相关信息(如中继设备的身份信息,或者中继设备生成的随机数,或者中继设备生成的计数器(COUNT))。对于第二终端设备而言,生成第一密钥时的输入参数包括:第一终端设备生成的第二临时公钥(Ephemeral public key2)、第二终端设备生成的第一临时私钥(Ephemeral private key1),以及中继设备的相关信息(如中继设备的身份信息,或者中继设备生成的随机数,或者中继设备生成的计数器(COUNT))。其中,第一临时公钥与第一临时私钥配对,第二临时公钥与第二临时私钥配对。

在一些实施例中,该完整性保护密钥包括控制面的完整性保护密钥($K_{D-CPint}$)和用户面的完整性保护密钥($K_{D-UPint}$);和/或,该机密性保护密钥包括控制面的机密性保护密钥($K_{D-CPenc}$)和用户面的机密性保护密钥($K_{D-UPenc}$)。

在一些实施例中,该完整性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度。也即,可以基于该第二密钥、选定的算法类型标识符、选定的算法类型标识符的长度、完整性保护算法标识、完整性保护算法标识的长度中的至少之一,生成该完整性保护密钥。

可选地,该完整性保护密钥的输入参数还可以包括一些系统设定参数。在该第二密钥自动刷新时,该完整性保护密钥自动更新。

在一些实施例中,该机密性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。也即,可以基于该第二密钥、选定的算法类型标识符、选定的算法类型标识符的长度、机密性保护算法标识、机密性保护算法标识的长度中的至少之一,生成该机密性保护密钥。

可选地,该机密性保护密钥的输入参数还可以包括一些系统设定参数。在该第二密钥自动刷新时,该机密性保护密钥自动更新。

在一些实施例中,对于控制面的完整性保护密钥($K_{D-CPint}$),选定的算法类型标识符可以通过“控制面完整性保护算法”或设置特定值来表示。

在一些实施例中,对于控制面的机密性保护密钥($K_{D-CPenc}$),选定的算法类型标识符可以通过“控制面机密性保护算法”或设置特定值来表示。

在一些实施例中,对于用户面的完整性保护密钥($K_{D-UPint}$),选定的算法类型标识符可以通过“用户面完整性保护算法”或设置特定值来表示。

在一些实施例中,对于用户面的机密性保护密钥($K_{D-UPenc}$),选定的算法类型标识符可以通过“用户面机密性保护算法”或设置特定值来表示。

具体例如,本申请所涉及的密钥分层结构可以如图8所示。

根密钥: 签名私钥/秘密签名密钥 (Secret Signing Key, SSK) 是 UE-to-UE relay 单播链路安全的信任根。SSK 与用户标识 (UE ID), 公钥参数 PVT 组成基于身份的公钥签名算法 (Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption, ECCSI) 算法中用户的签名公私钥对。用户各自生成临时公私钥对, 通过使用基于椭圆曲线的加密方案 (Elliptic Curve Integrated Encryption Scheme, ECIES) 算法来生成 K_D , 另外, 源设备用户生成的签名, 从而保证身份真实性与临时公钥的完整性、不可否认性。目标设备用户生成的签名, 从而保证身份真实性与临时公钥的完整性、不可否认性。从而保证仅有源设备和目标设备双方才可以获得密钥 K_D , 故签名私钥或 SSK 是保障源设备与目标设备之间安全通信的信任根。

K_D : 密钥长度至少为 256 比特 (bits), 由源设备和目标设备双方通过临时公私钥协商生成。基于根密钥, 通过重新运行认证流程来更新 K_D 。 K_D 用于生成下一层密钥 K_{D-sess} 。即使源设备与目标设备之间没有活动的通信会话, 那么也可以保存该密钥。 K_D ID 可以用来标识 K_D 。

KD: 对于 UE-1 而言, 生成时的输入参数包括: UE-1 的临时私钥 Ephemeral private key2、UE-2 的临时公钥 Ephemeral public key1、以及 UE-relay 的身份信息, 或者 UE-relay 生成的随机数, 或者 UE-relay 生成的计数器 COUNT; 对于 UE-2 而言, 生成时的输入参数包括: UE-1 的临时公钥 Ephemeral public key2、UE-2 的临时私钥 Ephemeral private key1、以及 UE-relay 的身份, 或者 UE-relay 生成的随机数, 或者 UE-relay 生成的计数器 COUNT。

K_{D-sess} : 密钥长度至少为 256bits, K_{D-sess} 用于派生下一层完整性保护或机密性保护密钥。可以基于 K_D , 通过重新运行安全连接建立流程或者相关的密钥更新流程来刷新 K_{D-sess} 。 K_{D-sess} ID 用于标识 K_{D-sess} 。 K_{D-sess} 由 K_D 使用 HMAC-SHA-256 或 HMAC-SM3 等密钥派生算法衍生而成。 K_{D-sess} 的输入参数至少必须含有密钥 K_D 、随机数 Nonce_1 (即第一终端设备生成的第一随机数)、随机数 Nonce_2 (即第二终端设备生成的第二随机数)。可选地, K_{D-sess} 的输入参数还可以包括但不限于以下至少之一: 源标识 (Source ID)、目标标识 (Destination ID)、随机数 Nonce_1 的长度、随机数 Nonce_2 的长度、源标识 (Source ID) 的长度、目标标识 (Destination ID) 的长度。另外, K_{D-sess} 的输入参数还可以包括其他系统设定参数, 如 3GPP 指定的一个或多个固定参数。

$K_{D-CPint}$: 密钥长度至少为 128bits, 该密钥可以用于控制面数据完整性保护, 该密钥由 K_{D-sess} 使用 HMAC-SHA-256 或 HMAC-SM3 等密钥派生算法衍生而来。 $K_{D-CPint}$ 的输入参数至少必须含有密钥 K_{D-sess} 、所选定的算法类型标识符 (比如“控制面完整性保护算法”或设置特定值来表示) 及该选定的算法类型标识符的长度, 完整性保护算法标识以及该完整性保护算法标识的长度, 其他系统设定参数可以作为可选输入参数。在 K_{D-sess} 自动刷新时, $K_{D-CPint}$ 自动更新。

$K_{D-CPenc}$: 密钥长度至少为 128bits, 该密钥可以用于控制面数据机密性保护, 该密钥由 K_{D-sess} 使用 HMAC-SHA-256 或 HMAC-SM3 等密钥派生算法衍生而来。 $K_{D-CPenc}$ 的输入参数至少必须含有密钥 K_{D-sess} 、所选定的算法类型标识符 (比如“控制面机密性保护算法”或设置特定值来表示) 及选定的算法类型标识符的长度, 机密性保护算法标识以及该机密性保护算法标识的长度, 其他系统设定参数可以作为可选输入参数。在 K_{D-sess} 自动刷新时, $K_{D-CPenc}$ 自动更新。

$K_{D-UPint}$: 密钥长度至少为 128bits, 该密钥可以用于用户面数据完整性保护, 该密钥由 K_{D-sess} 使用 HMAC-SHA-256 或 HMAC-SM3 等密钥派生算法衍生而来。 $K_{D-UPint}$ 的输入参数至少必须含有密钥 K_{D-sess} 、所选定的算法类型标识符 (比如“用户面完整性保护算法”或设置特定值来表示) 及该选定的算法类型标识符的长度, 完整性保护算法标识以及该完整性保护算法标识的长度, 其他系统设定参数可以作为可选输入参数。在 K_{D-sess} 自动刷新时, $K_{D-UPint}$ 自动更新。

$K_{D-UPenc}$: 密钥长度至少为 128bits, 该密钥可以用于用户面数据机密性保护, 该密钥由 K_{D-sess} 使用 HMAC-SHA-256 或 HMAC-SM3 等密钥派生算法衍生而来。 $K_{D-UPenc}$ 的输入参数至少必须含有密钥 K_{D-sess} 、所选定的算法类型标识符 (比如“用户面机密性保护算法”或设置特定值来表示) 及该选定的算法类型标识符的长度, 机密性保护算法标识以及该机密性保护算法标识的长度, 其他系统设定参数可以作为可选输入参数。在 K_{D-sess} 自动刷新时, $K_{D-UPenc}$ 自动更新。

在一些实施例中, 本申请中的 ECCSI 仅为示例, 并不局限于该算法, 也可以使用其他基于身份的公钥签名和公钥加密算法来替换, 在替换公钥算法的同时, 所有请求消息中与公钥算法相关的参数需要作相应替换。

在一些实施例中, 本申请中第一终端设备和第二终端设备使用的密钥派生函数不局限于 HMAC-SHA-256 或 HMAC-SM3, 包括任何一种满足计算安全的密钥派生函数。

在一些实施例中, 本申请中密钥派生函数的输入参数不局限于上述提到的必要参数, 可以含有其他可选参数, 比如应用系统设置固定参数。

在一些实施例中, 本申请中的密钥管理中心不限于 KMS、PKMF、5GPKMF, 运营商管理或被第

三方业务提供商管理的合法密钥管理中心均适用于本申请的技术方案。

本方案中, PKMF 为已注册并被授权使用 UE-to-UE relay 功能的终端设备下发的对称密钥不局限于上述方案, 具体配置可根据运营商或业务提供商对 PKMF 的设计而更改。

5 在一些实施例中, 本申请中安全通信建立流程中所有交互消息中的信息元素并不局限于上述方案中提到的内容, 也可以增加由于应用系统要求的可选信息元素。

因此, 在本申请实施例中, 第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥, 第二密钥用于派生完整性保护密钥和/或机密性保护密钥, 能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性, 从而确保双方传输数据的机密性和完整性, 防止其他设备甚至中继设备的窃听。

10 本申请实施例适用于 5G L2 UE-to-UE relay 架构下第一终端设备(源设备)和第二终端设备(目标设备)之间的安全通信建立流程。借助公钥签名技术, 能够确保终端设备的身份真实性和消息不可否认性, 能够抗重放攻击、中间人攻击、伪装等多种主动攻击, 同时保证认证流程消息的完整性, 并且利用 3GPP 标准中使用的 ECIES 算法, 从而建立了源 UE 和目标 UE 之间的端到端安全, 确保双方传输数据的机密性和完整性, 防止外部敌手甚至中继(relay)的窃听; 本申请实施例保证了安全通信建立机制的可扩展性, 另外, 本申请实施例能够实现源 UE 和目标 UE 之间用户面和控制面安全策略、以及双方所支持加密和完整性保护算法的安全协商, 能够实现完整性保护, 抵抗篡改和降级攻击。

15 上文结合图 7 至图 8, 详细描述了本申请的第一终端设备侧实施例, 下文结合图 9, 详细描述本申请的第二终端设备侧实施例, 应理解, 第二终端设备侧实施例与第一终端设备侧实施例相互对应, 类似的描述可以参照第一终端设备侧实施例。

20 图 9 是根据本申请实施例的中继通信的方法 300 的示意性流程图, 如图 9 所示, 该中继通信的方法 300 可以包括如下内容中的至少部分内容:

25 S310, 第二终端设备通过中继设备向第一终端设备发送认证请求消息; 其中, 该认证请求消息包括以下至少之一: 该第二终端设备所属用户的信息, 该第二终端设备生成的第一临时公钥, 该第二终端设备的签名, 该中继设备的相关信息; 其中, 该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK; 该第二终端设备的签名的输入参数包括以下至少之一: 该第二终端设备所属用户的信息和该第一临时公钥; 该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥; 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器。

30 本实施例基于 ECCSI 签名方案, 建立 L2 架构下的 UE-to-UE 中继场景下的安全连接。具体的, 本申请实施例应用于 L2 架构下的 UE-to-UE 中继场景, 也即, 第一终端设备与第二终端设备之间通过中继设备进行通信。例如, 第一终端设备与第二终端设备之间的中继连接可以是 PC5 链路。

在本申请实施例中, 该第一终端设备可以是源设备或源终端, 该第二终端设备可以是目标设备或目标终端。该中继设备可以是中继终端。

35 在本申请实施例中, 该第二终端设备的签名的输入参数包括以下至少之一: 该第二终端设备所属用户的信息和该第一临时公钥。也即, 该第二终端设备可以基于该第二终端设备所属用户的信息和该第一临时公钥中的至少之一, 生成该第二终端设备的签名。

在本申请实施例中, 该中继设备的签名的输入参数包括以下至少之一: 该第二终端设备的签名和该中继设备所属用户的信息。也即, 该中继设备可以基于该第二终端设备的签名和该中继设备所属用户的信息中的至少之一, 生成该中继设备的签名。

40 在一些实施例中, 该第二终端设备的签名由该第二终端设备的秘密签名密钥(SSK)生成。可选地, 该第二终端设备的 PVT 和 KPAK、以及秘密签名密钥(SSK)可以是可信中心 KMS 通过安全通道为该第二终端设备预先配置的。该安全通道可以基于 AKMA 机制或者 GBA 机制来建立该第二终端设备与 KMS 的安全连接, 该 KMS 可以直接由运营商来负责管理或者是与运营商有商业关系的第三方服务提供商。

45 在一些实施例中, 该第二终端设备接收该第一终端设备通过该中继设备发送的第一消息;

其中, 该第一消息包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该中继设备所属用户的信息, 该第一终端设备生成的第一随机数, 该第一终端设备生成的与该第二临时私钥配对的第二临时公钥, 该第一终端设备生成的该第一密钥的标识的 M 个比特位, 该第一终端设备的签名, 该中继设备的签名, 第一消息验证码;

50 其中, 该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK; 该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK; 该第一终端设备的签名的输入参数包括以下至少之一: 该第一终端设备所属用户的信息, 该第二临时公钥, 该

第一密钥的标识的 M 个比特位, 该第二终端设备的签名; 该中继设备的签名的输入参数包括以下至少之一: 该中继设备所属用户的信息, 该第一终端设备的签名, 该第二终端设备的签名;

其中, 该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护, 且该第一消息验证码的输入参数包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该中继设备所属用户的信息, 该第一随机数, 该第二临时公钥, 该 M 个比特位, 该第一终端设备的签名, 该中继设备的签名;

其中, 该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥, 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥, 该第二密钥用于派生完整性保护密钥和/或机密性保护密钥, 该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数。

在本申请实施例中, 该第一消息验证码的输入参数包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息、该中继设备所属用户的信息、该第一随机数, 该第二临时公钥, 该 M 个比特位。也即, 该第一终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位、该第一终端设备的签名、该中继设备的签名中的至少之一, 生成该第一消息验证码。

在本申请实施例中, 第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥。也即, 第一终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥, 以及第一终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥, 从而第一终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。同理, 第二终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥, 以及第二终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥, 从而第二终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。

在一些实施例中, 该第一终端设备的签名由该第一终端设备的秘密签名密钥生成。

在一些实施例中, 该中继设备的签名由该中继设备的秘密签名密钥生成。

在一些实施例中, 该第一消息为认证响应消息, 或者, 该第一消息为安全模式命令消息。

在一些实施例中, 该第一终端设备的安全能力信息可以是该第一终端设备支持的密码算法列表。

在一些实施例中, 该第一终端设备的安全策略信息可以是该第一终端设备是否支持机密性保护或完整性保护。其中, 该第一终端设备的安全策略信息包括: 该第一终端设备在控制面的安全策略信息, 和/或, 该第一终端设备在用户面的安全策略信息。

在一些实施例中, 该 M 个比特位可以是该第一密钥的标识的最高 M 个比特位, 该 N 个比特位可以是该第一密钥的标识的最低 N 个比特位; 或者, 该 M 个比特位可以是该第一密钥的标识的前 M 个比特位, 该 N 个比特位可以是该第一密钥的标识的后 N 个比特位; 或者, 该 M 个比特位可以是该第一密钥的标识的偶数位的比特位, 该 N 个比特位可以是该第一密钥的标识的奇数位的比特位。

在一些实施例中, M 与 N 的取值可以相同, 也可以不同, 本申请对此并不限定。

在一些实施例中, 该第二终端设备分别检查该第一终端设备的 KPAK 和该中继设备的 KPAK, 在该第一终端设备的 KPAK 和该中继设备的 KPAK 有效的情况下, 且基于该第一终端设备的标识和该第一终端设备的 PVT 对该第一终端设备的签名进行验证, 以及基于该中继设备的标识和该中继设备的 PVT 对该中继设备的签名进行验证;

在该第一终端设备的签名和该中继设备的签名验证成功, 且该第一消息中携带的信息未遭受篡改的情况下, 该第二终端设备生成第二随机数, 该第二终端设备至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥, 该第二终端设备根据该第二密钥生成完整性保护密钥和/或机密性保护密钥, 以及该第二终端设备生成该第一密钥的标识的 N 个比特位, 并将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识。

在一些实施例中, 该第二终端设备可以根据该第一随机数、该第一密钥、该第二随机数, 以及源标识、目标标识、该第一随机数的长度、该第二随机数的长度、该源标识的长度、该目标标识的长度中的至少之一, 生成该第二密钥。其中, 该源标识用于标识该第一终端设备与该第二终端设备之间的中继连接的源端, 该目标标识用于标识该第一终端设备与该第二终端设备之间的中继连接的目标端。另外, 该第二密钥的输入参数还可以包括其他系统设定参数, 如 3GPP 指定的一个或多个固定参数。

具体例如, 假设该第一消息验证码的输入参数包括: 该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位。该第二终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位生成第一消息验证码, 并与该第一消息中包含的该第一消息验证码进行比较, 若

比较一致的情况下，该第一消息验证码有效。

在一些实施例中，在该第一消息验证码有效的情况下，该第二终端设备通过该中继设备向该第一终端设备发送第二消息；其中，该第二消息包括以下至少之一：该第二随机数，该 N 个比特位，该第二终端设备生成的该第二密钥的标识的 x 个比特位，该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，第二消息验证码；

其中，该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护，或者，该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护，且该第二消息验证码的输入参数包括以下至少之一：该第二随机数，该 N 个比特位，该 x 个比特位，该第二终端设备选取的安全算法，该第二终端设备选取的安全策略；

其中，该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到，x 和 y 均为正整数。

具体例如，假设该第二消息验证码的输入参数包括：该第二随机数、该 N 个比特位、该 x 个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略。该第一终端设备可以基于该第二随机数、该 N 个比特位、该 x 个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略生成第二消息验证码，并与该第二消息中包含的该第二消息验证码进行比较，若比较一致的情况下，该第二消息验证码有效。

在一些实施例中，该 x 个比特位可以是该第二密钥的标识的最高 x 个比特位，该 y 个比特位可以是该第二密钥的标识的最低 y 个比特位；或者，该 x 个比特位可以是该第二密钥的标识的前 x 个比特位，该 y 个比特位可以是该第二密钥的标识的后 y 个比特位；或者，该 x 个比特位可以是该第二密钥的标识的偶数位的比特位，该 y 个比特位可以是该第二密钥的标识的奇数位的比特位。

在一些实施例中，x 与 y 的取值可以相同，也可以不同，本申请对此并不限定。

在一些实施例中，该第二消息通过该第一密钥进行加密。当然，该第二消息也可以不通过该第一密钥进行加密，或者，该第二消息也可以不加密。

具体的，该第二终端设备可以基于该第一终端设备的安全能力信息选取安全算法，和/或，该第二终端设备可以基于该第一终端设备的安全策略信息选取安全策略。

在一些实施例中，该第一消息为认证响应消息，该第二消息为安全模式命令（SMC）消息。

在一些实施例中，该第一消息为安全模式命令（SMC）消息，该第二消息为安全模式响应消息。

具体的，在本申请实施例中，第一终端设备可以根据第二终端设备生成的第一临时公钥、中继设备的相关信息和第一终端设备生成的第二临时私钥派生第一密钥。相应的，第二终端设备可以根据第一终端设备生成的第二临时公钥、中继设备的相关信息和第二终端设备生成的第一临时私钥派生第一密钥。其中，第二终端设备生成的第一临时公钥与第二终端设备生成的第一临时私钥配对，第一终端设备生成的第二临时公钥与第一终端设备生成的第二临时私钥配对。

具体例如，第一终端设备可以根据第一临时公钥、中继设备的相关信息和第二临时私钥，并使用 ECIES 算法计算出第一密钥；第二终端设备可以根据第二临时公钥、中继设备的相关信息和第一临时私钥，并使用 ECIES 算法计算出第一密钥。

在一些实施例中，该第二终端设备接收该第一终端设备通过该中继设备发送的第三消息；

其中，该第三消息用于指示安全模式建立完成，该第三消息通过目标密钥进行加密，且该第三消息包括以下至少之一：该第一终端设备生成的该第二密钥的标识的 y 个比特位，第三消息验证码；

其中，该目标密钥包括以下之一：该第一密钥，该第二密钥，该第二密钥派生的机密性保护密钥；

其中，该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护，或者，该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护，该第三消息验证码的输入参数包括该 y 个比特位。

在一些实施例中，该第二终端设备通过该目标密钥对该第三消息进行解密；在该第三消息中携带的信息未遭受篡改的情况下，且该第三消息验证码有效的情况下，该第二终端设备将该 x 个比特位与该 y 个比特位合并得到该第二密钥的标识。

具体的，该第二终端设备可以基于该 y 个比特位生成第三消息验证码，并与该第三消息中包含的该第三消息验证码进行比较，若比较一致的情况下，该第三消息验证码有效。

具体例如，该第三消息为安全模式结束消息（security mode complete）。

在一些实施例中，该第二终端设备通过该中继设备向该第一终端设备发送错误消息；其中，该错误消息包括以下至少之一：原因信息，第四消息验证码；其中，该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突，或者，该原因信息用于指示该第一消息验证码验证失败，或者，该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败，该第四消息验证码的输

入参数包括以下至少之一：该原因信息。

具体的，对于该第一终端设备，在该第四消息验证码有效的情况下，该第一终端设备确定安全模式建立失败，和/或，该第一终端设备重新发起安全模式建立流程。

在一些实施例中，该错误消息也可以受完整性保护。

5 具体例如，该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突，例如，该第二终端设备不支持该第一消息中携带的该第一终端设备的安全策略信息。

具体例如，该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败，例如，该第二终端设备不支持该第一消息中携带的该第一终端设备的安全能力信息。

10 在一些实施例中，该第一密钥可以是 K_D ，该第一密钥的标识可以是 K_D ID；该第二密钥可以是 K_{D-SESS} ，该第二密钥的标识可以是 K_{D-SESS} ID。

在一些实施例中，该完整性保护密钥包括控制面的完整性保护密钥 ($K_{D-CPint}$) 和用户面的完整性保护密钥 ($K_{D-UPint}$)；和/或，该机密性保护密钥包括控制面的机密性保护密钥 ($K_{D-CPenc}$) 和用户面的机密性保护密钥 ($K_{D-UPenc}$)。

15 因此，在本申请实施例中，第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥，第二密钥用于派生完整性保护密钥和/或机密性保护密钥，能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

20 本申请实施例适用于 5G L2 UE-to-UE relay 架构下第一终端设备（源设备）和第二终端设备（目标设备）之间的安全通信建立流程。借助公钥签名技术，能够确保终端设备的身份真实性和消息不可否认性，能够抗重放攻击、中间人攻击、伪装等多种主动攻击，同时保证认证流程消息的完整性，并且利用 3GPP 标准中使用的 ECIES 算法，从而建立了源 UE 和目标 UE 之间的端到端安全，确保双方传输数据的机密性和完整性，防止外部敌手甚至中继（relay）的窃听；本申请实施例保证了安全通信建立机制的可扩展性，另外，本申请实施例能够实现源 UE 和目标 UE 之间用户面和控制面安全策略、以及双方所支持加密和完整性保护算法的安全协商，能够实现完整性保护，抵抗篡改和降级攻击。

25 上文结合图 7 至图 9，详细描述了本申请的第一终端设备侧实施例和第二终端设备侧实施例，下文结合图 10，详细描述本申请的中继设备侧实施例，应理解，中继设备侧实施例与第一终端设备侧实施例和第二终端设备侧实施例相互对应，类似的描述可以参照第一终端设备侧实施例和第二终端设备侧实施例。

30 图 10 是根据本申请实施例的中继通信的方法 400 的示意性流程图，如图 10 所示，该中继通信的方法 400 可以包括如下内容中的至少部分内容：

35 S410，中继设备接收第二终端设备发送的认证请求消息；其中，该认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该第二终端设备生成的第一临时公钥，该第二终端设备的签名；其中，该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK；该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥；

40 S420，在该第二终端设备的 KPAK 有效，且基于该第二终端设备的标识和该第二终端设备的 PVT 对该第二终端设备的签名验证成功的情况下，该中继设备向第一终端设备发送验证之后的认证请求消息；其中，该验证之后的认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该中继设备所属用户的信息，该第一临时公钥，该第二终端设备的签名，该中继设备的签名，该中继设备的相关信息；其中，该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK；该中继设备的签名的输入参数包括以下至少之一：该第二终端设备的签名和该中继设备所属用户的信息；其中，该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥；该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

45 本实施例基于 ECCSI 签名方案，建立 L2 架构下的 UE-to-UE 中继场景下的安全连接。具体的，本申请实施例应用于 L2 架构下的 UE-to-UE 中继场景，也即，第一终端设备与第二终端设备之间通过中继设备进行通信。例如，第一终端设备与第二终端设备之间的中继连接可以是 PC5 链路。

在本申请实施例中，该第一终端设备可以是源设备或源终端，该第二终端设备可以是目标设备或目标终端。该中继设备可以是中继终端。

50 在本申请实施例中，该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥。也即，该第二终端设备可以基于该第二终端设备所属用户的信息和该第一临时公钥中的至少之一，生成该第二终端设备的签名。

在本申请实施例中，该中继设备的签名的输入参数包括以下至少之一：该第二终端设备的签名和该中继设备所属用户的信息。也即，该中继设备可以基于该第二终端设备的签名和该中继设备所属用户的信息中的至少之一，生成该中继设备的签名。

具体的，该中继设备可以基于其本地存储的一个或多个 KPAK，验证该第二终端设备的 KPAK 的有效性。例如，在中继设备本地存储的 KPAK 中存在与第二终端设备的 KPAK 一致的 KPAK 的情况下，该第二终端设备的 KPAK 有效。可选地，该第一终端设备本地存储的一个或多个 KPAK 可以由 KMS 预配置。

在本申请实施例中，第一终端设备可以根据第二终端设备生成的第一临时公钥、中继设备的相关信息和第一终端设备生成的第二临时私钥派生第一密钥。相应的，第二终端设备可以根据第一终端设备生成的第二临时公钥、中继设备的相关信息和第二终端设备生成的第一临时私钥派生第一密钥。其中，第二终端设备生成的第一临时公钥与第二终端设备生成的第一临时私钥配对，第一终端设备生成的第二临时公钥与第一终端设备生成的第二临时私钥配对。

具体例如，第一终端设备可以根据第一临时公钥和第二临时私钥，并使用 ECIES 算法计算出第一密钥；第二终端设备可以根据第二临时公钥和第一临时私钥，并使用 ECIES 算法计算出第一密钥。

在一些实施例中，在该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK 的情况下，该第二终端设备的签名由该第二终端设备的秘密签名密钥（SSK）生成。可选地，该第二终端设备的 PVT 和 KPAK、以及秘密签名密钥（SSK）可以是可信中心 KMS 通过安全通道为该第二终端设备预先配置的。该安全通道可以基于 AKMA 机制或者 GBA 机制来建立该第二终端设备与 KMS 的安全连接，该 KMS 可以直接由运营商来负责管理或者是与运营商有商业关系的第三方服务提供商。

在一些实施例中，在该中继设备所属用户的信息包括该中继设备的标识、该中继设备的 PVT 和 KPAK 的情况下，该中继设备的签名由该中继设备的秘密签名密钥（SSK）生成。可选地，该中继设备的 PVT 和 KPAK、以及秘密签名密钥（SSK）可以是可信中心 KMS 通过安全通道为该中继设备预先配置的。该安全通道可以基于 AKMA 机制或者 GBA 机制来建立该中继设备与 KMS 的安全连接，该 KMS 可以直接由运营商来负责管理或者是与运营商有商业关系的第三方服务提供商。

在一些实施例中，该中继设备接收该第一终端设备发送的第一消息；

其中，该第一消息包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的第二临时公钥，该第一终端设备生成的该第一密钥的标识的 M 个比特位，该第一终端设备的签名，第一消息验证码；

其中，该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK；该第一终端设备的签名的输入参数包括以下至少之一：该第一终端设备所属用户的信息，该第二临时公钥，该第一密钥的标识的 M 个比特位，该第二终端设备的签名；

其中，该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护，且该第一消息验证码的输入参数包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一随机数，该第二临时公钥，该 M 个比特位，该第一终端设备的签名；

其中，该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，该第二密钥用于派生完整性保护密钥和/或机密性保护密钥，该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数。

具体的，在该第一终端设备的 KPAK 有效，且基于该第一终端设备的标识和该第一终端设备的 PVT 对该第一终端设备的签名验证成功的情况下，该中继设备向该第二终端设备发送验证之后的第一消息；其中，该验证之后的第一消息包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该中继设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的与该第二临时私钥配对的第二临时公钥，该第一终端设备生成的该第一密钥的标识的 M 个比特位，该第一终端设备的签名，该中继设备的签名，第一消息验证码；其中，该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK；该中继设备的签名的输入参数包括以下至少之一：该中继设备所属用户的信息，该第一终端设备的签名，该第二终端设备的签名，该验证之后的第一消息；

在本申请实施例中，第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥。也即，第一终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密

钥, 以及第一终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥, 从而第一终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。同理, 第二终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥, 以及第二终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥, 从而第二终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。

在本申请实施例中, 该第一消息验证码的输入参数包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一随机数, 该第二临时公钥, 该 M 个比特位。也即, 该第一终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位中的至少之一, 生成该第一消息验证码。

具体例如, 假设该第一消息验证码的输入参数包括: 该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位。该第二终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位生成第一消息验证码, 并与该第一消息中包含的该第一消息验证码进行比较, 若比较一致的情况下, 该第一消息验证码有效。

在一些实施例中, 该第一消息为认证响应消息, 或者, 该第一消息为安全模式命令消息。

在一些实施例中, 该第一终端设备的安全能力信息可以是该第一终端设备支持的密码算法列表。

在一些实施例中, 该第一终端设备的安全策略信息可以是该第一终端设备是否支持机密性保护或完整性保护。其中, 该第一终端设备的安全策略信息包括: 该第一终端设备在控制面的安全策略信息, 和/或, 该第一终端设备在用户面的安全策略信息。

在一些实施例中, 该 M 个比特位可以是该第一密钥的标识的最高 M 个比特位, 该 N 个比特位可以是该第一密钥的标识的最低 N 个比特位; 或者, 该 M 个比特位可以是该第一密钥的标识的前 M 个比特位, 该 N 个比特位可以是该第一密钥的标识的后 N 个比特位; 或者, 该 M 个比特位可以是该第一密钥的标识的偶数位的比特位, 该 N 个比特位可以是该第一密钥的标识的奇数位的比特位。

在一些实施例中, M 与 N 的取值可以相同, 也可以不同, 本申请对此并不限定。

在一些实施例中, 该中继设备将该第二终端设备发送的第二消息转发至该第一终端设备;

其中, 该第二消息包括以下至少之一: 该第二终端设备生成的该第二随机数, 该第二终端设备生成的该第一密钥的标识的 N 个比特位, 该第二终端设备生成的该第二密钥的标识的 x 个比特位, 该第二终端设备选取的安全算法, 该第二终端设备选取的安全策略, 第二消息验证码;

其中, 该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护, 或者, 该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护, 且该第二消息验证码的输入参数包括以下至少之一: 该第二随机数, 该 N 个比特位, 该 x 个比特位, 该第二终端设备选取的安全算法, 该第二终端设备选取的安全策略;

其中, 该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

在一些实施例中, 该 x 个比特位可以是该第二密钥的标识的最高 x 个比特位, 该 y 个比特位可以是该第二密钥的标识的最低 y 个比特位; 或者, 该 x 个比特位可以是该第二密钥的标识的前 x 个比特位, 该 y 个比特位可以是该第二密钥的标识的后 y 个比特位; 或者, 该 x 个比特位可以是该第二密钥的标识的偶数位的比特位, 该 y 个比特位可以是该第二密钥的标识的奇数位的比特位。

在一些实施例中, x 与 y 的取值可以相同, 也可以不同, 本申请对此并不限定。

具体例如, 假设该第二消息验证码的输入参数包括: 该第二随机数、该 N 个比特位、该 x 个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略。该第一终端设备可以基于该第二随机数、该 N 个比特位、该 x 个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略生成第二消息验证码, 并与该第二消息中包含的该第二消息验证码进行比较, 若比较一致的情况下, 该第二消息验证码有效。

在一些实施例中, 该第二消息通过该第一密钥进行加密。当然, 该第二消息也可以不通过该第一密钥进行加密, 或者, 该第二消息也可以不加密。

具体的, 该第二终端设备可以基于该第一终端设备的安全能力信息选取安全算法, 和/或, 该第二终端设备可以基于该第一终端设备的安全策略信息选取安全策略。

在一些实施例中, 该第一终端设备可以根据该第一随机数、该第一密钥、该第二随机数, 以及源标识、目标标识、该第一随机数的长度、该第二随机数的长度、该源标识的长度、该目标标识的长度中的至少之一, 生成该第二密钥。以及该第二终端设备可以根据该第一随机数、该第一密钥、该第二随机数, 以及源标识、目标标识、该第一随机数的长度、该第二随机数的长度、该源标识的长度、该

目标标识的长度中的至少之一，生成该第二密钥。

其中，该源标识用于标识该第一终端设备与该第二终端设备之间的中继连接的源端，该目标标识用于标识该第一终端设备与该第二终端设备之间的中继连接的目标端。另外，该第二密钥的输入参数还可以包括其他系统设定参数，如 3GPP 指定的一个或多个固定参数。

5 在一些实施例中，该第一消息为认证响应消息，该第二消息为安全模式命令（SMC）消息。

在一些实施例中，该第一消息为安全模式命令（SMC）消息，该第二消息为安全模式响应消息。

在一些实施例中，该中继设备将该第一终端设备发送的第三消息转发至该第二终端设备；

其中，该第三消息用于指示安全模式建立完成，该第三消息通过目标密钥进行加密，且该第三消息包括以下至少之一：该第一终端设备生成的该第二密钥的标识的 y 个比特位，第三消息验证码；

10 其中，该目标密钥包括以下之一：该第一密钥，该第二密钥，该第二密钥派生的机密性保护密钥；

其中，该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护，或者，该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护，该第三消息验证码的输入参数包括该 y 个比特位。

15 在一些实施例中，对于该第二终端设备，该第二终端设备通过该目标密钥对该第三消息进行解密；在该第三消息中携带的信息未遭受篡改的情况下，且该第三消息验证码有效的情况下，该第二终端设备将该 x 个比特位与该 y 个比特位合并得到该第二密钥的标识。

具体的，该第二终端设备可以基于该 y 个比特位生成第三消息验证码，并与该第三消息中包含的该第三消息验证码进行比较，若比较一致的情况下，该第三消息验证码有效。

具体例如，该第三消息为安全模式结束消息（security mode complete）。

20 在一些实施例中，该中继设备将该第二终端设备发送的错误消息转发至该第一终端设备；其中，该错误消息包括以下至少之一：原因信息，第四消息验证码；其中，该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突，或者，该原因信息用于指示该第一消息验证码验证失败，或者，该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败，该第四消息验证码的输入参数包括以下至少之一：该原因信息。

25 具体的，在该第四消息验证码有效的情况下，该第一终端设备确定安全模式建立失败，和/或，该第一终端设备重新发起安全模式建立流程。

在一些实施例中，该错误消息也可以受完整性保护。

具体例如，该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突，例如，该第二终端设备不支持该第一消息中携带的该第一终端设备的安全策略信息。

30 具体例如，该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败，例如，该第二终端设备不支持该第一消息中携带的该第一终端设备的安全能力信息。

在一些实施例中，该第一密钥可以是 K_D ，该第一密钥的标识可以是 K_D ID；该第二密钥可以是 K_{D-SESS} ，该第二密钥的标识可以是 K_{D-SESS} ID。

35 在一些实施例中，该完整性保护密钥包括控制面的完整性保护密钥（ $K_{D-CPint}$ ）和用户面的完整性保护密钥（ $K_{D-UPint}$ ）；和/或，该机密性保护密钥包括控制面的机密性保护密钥（ $K_{D-CPenc}$ ）和用户面的机密性保护密钥（ $K_{D-UPenc}$ ）。

40 因此，在本申请实施例中，第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥，第二密钥用于派生完整性保护密钥和/或机密性保护密钥，能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

45 本申请实施例适用于 5G L2 UE-to-UE relay 架构下源设备（第一终端设备）和目标设备（第二终端设备）之间的安全通信建立流程。借助公钥签名技术，能够确保终端设备的身份真实性和消息不可否认性，能够抗重放攻击、中间人攻击、伪装等多种主动攻击，同时保证认证流程消息的完整性，并且利用 3GPP 标准中使用的 ECIES 算法，从而建立了源 UE 和目标 UE 之间的端到端安全，确保双方传输数据的机密性和完整性，防止外部敌手甚至中继（relay）的窃听；本申请实施例保证了安全通信建立机制的可扩展性，另外，本申请实施例能够实现源 UE 和目标 UE 之间用户面和控制面安全策略、以及双方所支持加密和完整性保护算法的安全协商，能够实现完整性保护，抵抗篡改和降级攻击。

上文结合图 7 至图 8，详细描述了本申请的第一终端设备侧实施例，下文结合图 11，详细描述本申请的第一终端设备侧的另一实施例，类似的描述可以参照第一终端设备侧实施例。

50 图 11 是根据本申请实施例的中继通信的方法 500 的示意性流程图，如图 11 所示，该中继通信的方法 500 可以包括如下内容中的至少部分内容：

S510，第一终端设备通过中继设备向第二终端设备发送第一消息；其中，该第一消息包括以下至

少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的第二临时公钥，该第一终端设备生成的第一密钥的标识的 M 个比特位，该第一终端设备的签名，第一消息验证码；其中，该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK；该第一终端设备的签名的输入参数包括以下至少之一：该第一终端设备所属用户的信息，该第二临时公钥，该第一密钥的标识的 M 个比特位，该第二终端设备的签名；其中，该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护，且该第一消息验证码的输入参数包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一随机数，该第二临时公钥，该 M 个比特位，该第一终端设备的签名；其中，该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，该第二密钥用于派生完整性保护密钥和/或机密性保护密钥，该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

本实施例基于 ECCSI 签名方案，建立 L2 架构下的 UE-to-UE 中继场景下的安全连接。具体的，本申请实施例应用于 L2 架构下的 UE-to-UE 中继场景，也即，第一终端设备与第二终端设备之间通过中继设备进行通信。例如，第一终端设备与第二终端设备之间的中继连接可以是 PC5 链路。

在本申请实施例中，第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥。也即，第一终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥，以及第一终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥，从而第一终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。同理，第二终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥，以及第二终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥，从而第二终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。

在本申请实施例中，该第一消息验证码的输入参数包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一随机数，该第二临时公钥，该 M 个比特位。也即，该第一终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位中的至少之一，生成该第一消息验证码。

具体例如，假设该第一消息验证码的输入参数包括：该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位。该第二终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位生成第一消息验证码，并与该第一消息中包含的该第一消息验证码进行比较，若比较一致的情况下，该第一消息验证码有效。

在一些实施例中，该第一消息为认证响应消息，或者，该第一消息为安全模式命令消息。

在一些实施例中，该第一终端设备的安全能力信息可以是该第一终端设备支持的密码算法列表。

在一些实施例中，该第一终端设备的安全策略信息可以是该第一终端设备是否支持机密性保护或完整性保护。其中，该第一终端设备的安全策略信息包括：该第一终端设备在控制面的安全策略信息，和/或，该第一终端设备在用户面的安全策略信息。

在一些实施例中，该 M 个比特位可以是该第一密钥的标识的最高 M 个比特位，该 N 个比特位可以是该第一密钥的标识的最低 N 个比特位；或者，该 M 个比特位可以是该第一密钥的标识的前 M 个比特位，该 N 个比特位可以是该第一密钥的标识的后 N 个比特位；或者，该 M 个比特位可以是该第一密钥的标识的偶数位的比特位，该 N 个比特位可以是该第一密钥的标识的奇数位的比特位。

在一些实施例中，M 与 N 的取值可以相同，也可以不同，本申请对此并不限定。

在一些实施例中，该第一终端设备接收该第二终端设备通过该中继设备发送的第二消息；

其中，该第二消息包括以下至少之一：该第二终端设备生成的该第二随机数，该第二终端设备生成的该第一密钥的标识的 N 个比特位，该第二终端设备生成的该第二密钥的标识的 x 个比特位，该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，第二消息验证码；

其中，该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护，或者，该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护，且该第二消息验证码的输入参数包括以下至少之一：该第二随机数，该 N 个比特位，该 x 个比特位，该第二终端设备选取的安全算法，该第二终端设备选取的安全策略；

其中，该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到，x 和

y 均为正整数。

在一些实施例中，在该第二消息中携带的信息未遭受篡改的情况下，该第一终端设备至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥，该第一终端设备根据该第二密钥生成完整性保护密钥和/或机密性保护密钥，以及该第一终端设备将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识，该第一终端设备生成该第二密钥的标识的 y 个比特位，并将该 x 个比特位和该 y 个比特位合并得到该第二密钥的标识；

在该第二消息验证码有效的情况下，该第一终端设备根据该第二终端设备选取的安全算法、该第二密钥、基于该第二密钥生成完整性保护密钥和/或机密性保护密钥、该第二终端设备选取的安全策略，与该第二终端设备进行通信。

在一些实施例中，该第二消息通过该第一密钥进行加密。当然，该第二消息也可以不通过该第一密钥进行加密，或者，该第二消息也可以不加密。

在一些实施例中，该第一终端设备根据该第一密钥解密该第二消息；在该第二消息中携带的信息未遭受篡改的情况下，该第一终端设备至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥，该第一终端设备根据该第二密钥生成完整性保护密钥和/或机密性保护密钥，以及该第一终端设备将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识，该第一终端设备生成该第二密钥的标识的 y 个比特位，并将该 x 个比特位和该 y 个比特位合并得到该第二密钥的标识；

在该第二消息验证码有效和该第三消息验证码有效的情况下，该第一终端设备根据该第二终端设备选取的安全算法、该第二密钥、基于该第二密钥生成完整性保护密钥和/或机密性保护密钥、该第二终端设备选取的安全策略，与该第二终端设备进行通信。

在一些实施例中，该 x 个比特位可以是该第二密钥的标识的最高 x 个比特位，该 y 个比特位可以是该第二密钥的标识的最低 y 个比特位；或者，该 x 个比特位可以是该第二密钥的标识的前 x 个比特位，该 y 个比特位可以是该第二密钥的标识的后 y 个比特位；或者，该 x 个比特位可以是该第二密钥的标识的偶数位的比特位，该 y 个比特位可以是该第二密钥的标识的奇数位的比特位。

在一些实施例中，x 与 y 的取值可以相同，也可以不同，本申请对此并不限定。

具体例如，假设该第二消息验证码的输入参数包括：该第二随机数、该 N 个比特位、该 x 个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略。该第一终端设备可以基于该第二随机数、该 N 个比特位、该 x 个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略生成第二消息验证码，并与该第二消息中包含的该第二消息验证码进行比较，若比较一致的情况下，该第二消息验证码有效。

具体的，该第二终端设备可以基于该第一终端设备的安全能力信息选取安全算法，和/或，该第二终端设备可以基于该第一终端设备的安全策略信息选取安全策略。

在一些实施例中，该第一终端设备可以根据该第一随机数、该第一密钥、该第二随机数，以及源标识、目标标识、该第一随机数的长度、该第二随机数的长度、该源标识的长度、该目标标识的长度中的至少之一，生成该第二密钥。其中，该源标识用于标识该第一终端设备与该第二终端设备之间的中继连接的源端，该目标标识用于标识该第一终端设备与该第二终端设备之间的中继连接的目标端。另外，该第二密钥的输入参数还可以包括其他系统设定参数，如 3GPP 指定的一个或多个固定参数。

在一些实施例中，该第一消息为认证响应消息，该第二消息为 SMC 消息。

在一些实施例中，该第一消息为 SMC 消息，该第二消息为安全模式响应消息。

在一些实施例中，该第一终端设备通过该中继设备向该第二终端设备发送第三消息；

其中，该第三消息用于指示安全模式建立完成，该第三消息通过目标密钥进行加密，且该第三消息包括以下至少之一：该第二密钥的标识的该 y 个比特位，第三消息验证码；

其中，该目标密钥包括以下之一：该第一密钥，该第二密钥，该第二密钥派生的机密性保护密钥；

其中，该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护，或者，该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护，该第三消息验证码的输入参数包括该 y 个比特位。

在一些实施例中，对于该第二终端设备，该第二终端设备通过该目标密钥对该第三消息进行解密；在该第三消息中携带的信息未遭受篡改的情况下，且该第三消息验证码有效的情况下，该第二终端设备将该 x 个比特位与该 y 个比特位合并得到该第二密钥的标识。具体的，该第二终端设备可以基于该 y 个比特位生成第三消息验证码，并与该第三消息中包含的该第三消息验证码进行比较，若比较一致的情况下，该第三消息验证码有效。

具体例如，该第三消息为安全模式结束消息（security mode complete）。

在一些实施例中，该第一终端设备接收该第二终端设备通过该中继设备发送的错误消息；其中，

该错误消息包括以下至少之一：原因信息，第四消息验证码；其中，该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突，或者，该原因信息用于指示该第一消息验证码验证失败，或者，该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败，该第四消息验证码的输入参数包括以下至少之一：该原因信息；

5 在该第四消息验证码有效的情况下，该第一终端设备确定安全模式建立失败，和/或，该第一终端设备重新发起安全模式建立流程。

在一些实施例中，该错误消息也可以受完整性保护。

具体例如，该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突，例如，该第二终端设备不支持该第一消息中携带的该第一终端设备的安全策略信息。

10 具体例如，该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败，例如，该第二终端设备不支持该第一消息中携带的该第一终端设备的安全能力信息。

在一些实施例中，该第一终端设备接收该第二终端设备通过该中继设备发送的认证请求消息；

其中，该认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该中继设备所属用户的信息，该第二终端设备生成的第一临时公钥，该第二终端设备的签名，该中继设备的签名，该中继设备的相关信息；

15 其中，该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK；该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK；该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥；该中继设备的签名的输入参数包括以下至少之一：该第二终端设备的签名和该中继设备所属用户的信息；该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥。

20 在本申请实施例中，该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥。也即，该第二终端设备可以基于该第二终端设备所属用户的信息和该第一临时公钥中的至少之一，生成该第二终端设备的签名。

25 在本申请实施例中，该中继设备的签名的输入参数包括以下至少之一：该第二终端设备的签名和该中继设备所属用户的信息。也即，该中继设备可以基于该第二终端设备的签名和该中继设备所属用户的信息中的至少之一，生成该中继设备的签名。

30 在一些实施例中，在该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK 的情况下，该第二终端设备的签名由该第二终端设备的秘密签名密钥（SSK）生成。可选地，该第二终端设备的 PVT 和 KPAK、以及秘密签名密钥（SSK）可以是可信中心 KMS 通过安全通道为该第二终端设备预先配置的。该安全通道可以基于 AKMA 机制或者 GBA 机制来建立该第二终端设备与 KMS 的安全连接，该 KMS 可以直接由运营商来负责管理或者是与运营商有商业关系的第三方服务提供商。

35 在一些实施例中，在该中继设备所属用户的信息包括该中继设备的标识、该中继设备的 PVT 和 KPAK 的情况下，该中继设备的签名由该中继设备的秘密签名密钥（SSK）生成。可选地，该中继设备的 PVT 和 KPAK、以及秘密签名密钥（SSK）可以是可信中心 KMS 通过安全通道为该中继设备预先配置的。该安全通道可以基于 AKMA 机制或者 GBA 机制来建立该中继设备与 KMS 的安全连接，该 KMS 可以直接由运营商来负责管理或者是与运营商有商业关系的第三方服务提供商。

40 在一些实施例中，在该第二终端设备的 KPAK 和该中继设备的 KPAK 有效，且基于该第二终端设备的标识和该第二终端设备的 PVT 对该第二终端设备的签名验证成功，以及基于该中继设备的标识和该中继设备的 PVT 对该中继设备的签名验证成功的情况下，该第一终端设备生成第二临时私钥，以及该第一终端设备根据该第一临时公钥、该中继设备的相关信息和该第二临时私钥派生该第一密钥。

45 具体的，该第一终端设备可以基于其本地存储的一个或多个 KPAK，验证该第二终端设备的 KPAK 和该中继设备的 KPAK 的有效性。例如，在第一终端设备本地存储的 KPAK 中存在与第二终端设备的 KPAK 一致的 KPAK 的情况下，该第二终端设备的 KPAK 有效；以及在第一终端设备本地存储的 KPAK 中存在与中继设备的 KPAK 一致的 KPAK 的情况下，该中继设备的 KPAK 有效。可选地，该第一终端设备本地存储的一个或多个 KPAK 可以由 KMS 预配置。

50 具体的，在本申请实施例中，第一终端设备可以根据第二终端设备生成的第一临时公钥、中继设备的相关信息和第一终端设备生成的第二临时私钥派生第一密钥。相应的，第二终端设备可以根据第一终端设备生成的第二临时公钥、中继设备的相关信息和第二终端设备生成的第一临时私钥派生第一密钥。其中，第二终端设备生成的第一临时公钥与第二终端设备生成的第一临时私钥配对，第一终端设备生成的第二临时公钥与第一终端设备生成的第二临时私钥配对。

具体例如，第一终端设备可以根据第一临时公钥和第二临时私钥，并使用 ECIES 算法计算出第一密钥；第二终端设备可以根据第二临时公钥和第一临时私钥，并使用 ECIES 算法计算出第一密钥。

在一些实施例中，该第一密钥可以是 K_D ，该第一密钥的标识可以是 K_D ID；该第二密钥可以是 K_{D-SESS} ，该第二密钥的标识可以是 K_{D-SESS} ID。

5 在一些实施例中，该完整性保护密钥包括控制面的完整性保护密钥 ($K_{D-CPint}$) 和用户面的完整性保护密钥 ($K_{D-UPint}$)；和/或，该机密性保护密钥包括控制面的机密性保护密钥 ($K_{D-CPenc}$) 和用户面的机密性保护密钥 ($K_{D-UPenc}$)。

10 因此，在本申请实施例中，第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥，第二密钥用于派生完整性保护密钥和/或机密性保护密钥，能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

15 本申请实施例适用于 5G L2 UE-to-UE relay 架构下第一终端设备（源设备）和第二终端设备（目标设备）之间的安全通信建立流程。借助公钥签名技术，能够确保终端设备的身份真实性和消息不可否认性，能够抗重放攻击、中间人攻击、伪装等多种主动攻击，同时保证认证流程消息的完整性，并且利用 3GPP 标准中使用的 ECIES 算法，从而建立了源 UE 和目标 UE 之间的端到端安全，确保双方传输数据的机密性和完整性，防止外部敌手甚至中继（relay）的窃听；本申请实施例保证了安全通信建立机制的可扩展性，另外，本申请实施例能够实现源 UE 和目标 UE 之间用户面和控制面安全策略、以及双方所支持加密和完整性保护算法的安全协商，能够实现完整性保护，抵抗篡改和降级攻击。

20 上文结合图 7 至图 8，详细描述了本申请的第一终端设备侧实施例，下文结合图 12，详细描述本申请的第二终端设备侧实施例，应理解，第二终端设备侧实施例与第一终端设备侧实施例相互对应，类似的描述可以参照第一终端设备侧实施例。

图 12 是根据本申请实施例的中继通信的方法 600 的示意性流程图，如图 12 所示，该中继通信的方法 600 可以包括如下内容中的至少部分内容：

25 S610，第二终端设备接收第一终端设备通过中继设备发送的第一消息；其中，该第一消息包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该中继设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的第二临时公钥，该第一终端设备生成的第一密钥的标识的 M 个比特位，该第一终端设备的签名，该中继设备的签名，第一消息验证码；其中，该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK；该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK；该第一终端设备的签名的输入参数包括以下至少之一：该第一终端设备所属用户的信息，该第二临时公钥，该第一密钥的标识的 M 个比特位，该第二终端设备的签名；该中继设备的签名的输入参数包括以下至少之一：该中继设备所属用户的信息，该第一终端设备的签名，该第二终端设备的签名；其中，该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护，且该第一消息验证码的输入参数包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一随机数，该第二临时公钥，该 M 个比特位，该第一终端设备的签名；其中，该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，该第二密钥用于派生完整性保护密钥和/或机密性保护密钥，该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

40 本实施例基于 ECCSI 签名方案，建立 L2 架构下的 UE-to-UE 中继场景下的安全连接。具体的，本申请实施例应用于 L2 架构下的 UE-to-UE 中继场景，也即，第一终端设备与第二终端设备之间通过中继设备进行通信。例如，第一终端设备与第二终端设备之间的中继连接可以是 PC5 链路。

45 在本申请实施例中，第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥。也即，第一终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥，以及第一终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥，从而第一终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。同理，第二终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥，以及第二终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥，从而第二终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。

50 在本申请实施例中，该第一消息验证码的输入参数包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一随机数，该第二临时公钥，该 M 个比特位。也即，

该第一终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位中的至少之一，生成该第一消息验证码。

在一些实施例中，该第一终端设备的签名由该第一终端设备的秘密签名密钥生成；和/或，该中继设备的签名由该中继设备的秘密签名密钥生成。

5 在一些实施例中，该第一消息为认证响应消息，或者，该第一消息为安全模式命令消息。

在一些实施例中，该第一终端设备的安全能力信息可以是该第一终端设备支持的密码算法列表。

在一些实施例中，该第一终端设备的安全策略信息可以是该第一终端设备是否支持机密性保护或完整性保护。其中，该第一终端设备的安全策略信息包括：该第一终端设备在控制面的安全策略信息，和/或，该第一终端设备在用户面的安全策略信息。

10 在一些实施例中，该 M 个比特位可以是该第一密钥的标识的最高 M 个比特位，该 N 个比特位可以是该第一密钥的标识的最低 N 个比特位；或者，该 M 个比特位可以是该第一密钥的标识的前 M 个比特位，该 N 个比特位可以是该第一密钥的标识的后 N 个比特位；或者，该 M 个比特位可以是该第一密钥的标识的偶数位的比特位，该 N 个比特位可以是该第一密钥的标识的奇数位的比特位。

在一些实施例中，M 与 N 的取值可以相同，也可以不同，本申请对此并不限定。

15 在一些实施例中，该第二终端设备分别检查该第一终端设备的 KPAK 和该中继设备的 KPAK，在该第一终端设备的 KPAK 和该中继设备的 KPAK 有效的情况下，且基于该第一终端设备的标识和该第一终端设备的 PVT 对该第一终端设备的签名进行验证，以及基于该中继设备的标识和该中继设备的 PVT 对该中继设备的签名进行验证；在该第一终端设备的签名和该中继设备的签名验证成功，且该第一消息中携带的信息未遭受篡改的情况下，该第二终端设备生成第二随机数，该第二终端设备至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥，该第二终端设备根据该第二密钥生成完整性保护密钥和/或机密性保护密钥，以及该第二终端设备生成该第一密钥的标识的 N 个比特位，并将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识。

20 在一些实施例中，该第二终端设备可以根据该第一随机数、该第一密钥、该第二随机数，以及源标识、目标标识、该第一随机数的长度、该第二随机数的长度、该源标识的长度、该目标标识的长度中的至少之一，生成该第二密钥。其中，该源标识用于标识该第一终端设备与该第二终端设备之间的中继连接的源端，该目标标识用于标识该第一终端设备与该第二终端设备之间的中继连接的目标端。另外，该第二密钥的输入参数还可以包括其他系统设定参数，如 3GPP 指定的一个或多个固定参数。

25 具体例如，假设该第一消息验证码的输入参数包括：该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位。该第二终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位生成第一消息验证码，并与该第一消息中包含的该第一消息验证码进行比较，若比较一致的情况下，该第一消息验证码有效。

30 在一些实施例中，在该第一消息验证码有效的情况下，该第二终端设备通过该中继设备向该第一终端设备发送第二消息；其中，该第二消息包括以下至少之一：该第二随机数，该 N 个比特位，该第二终端设备生成的该第二密钥的标识的 x 个比特位，该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，第二消息验证码；

35 其中，该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护，或者，该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护，且该第二消息验证码的输入参数包括以下至少之一：该第二随机数，该 N 个比特位，该 x 个比特位，该第二终端设备选取的安全算法，该第二终端设备选取的安全策略；

40 其中，该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到，x 和 y 均为正整数。

45 具体例如，假设该第二消息验证码的输入参数包括：该第二随机数、该 N 个比特位、该 x 个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略。该第一终端设备可以基于该第二随机数、该 N 个比特位、该 x 个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略生成第二消息验证码，并与该第二消息中包含的该第二消息验证码进行比较，若比较一致的情况下，该第二消息验证码有效。

50 在一些实施例中，该 x 个比特位可以是该第二密钥的标识的最高 x 个比特位，该 y 个比特位可以是该第二密钥的标识的最低 y 个比特位；或者，该 x 个比特位可以是该第二密钥的标识的前 x 个比特位，该 y 个比特位可以是该第二密钥的标识的后 y 个比特位；或者，该 x 个比特位可以是该第二密钥的标识的偶数位的比特位，该 y 个比特位可以是该第二密钥的标识的奇数位的比特位。

在一些实施例中，x 与 y 的取值可以相同，也可以不同，本申请对此并不限定。

在一些实施例中,该第二消息通过该第一密钥进行加密。当然,该第二消息也可以不通过该第一密钥进行加密,或者,该第二消息也可以不加密。

具体的,该第二终端设备可以基于该第一终端设备的安全能力信息选取安全算法,和/或,该第二终端设备可以基于该第一终端设备的安全策略信息选取安全策略。

5 在一些实施例中,该第一消息为认证响应消息,该第二消息为安全模式命令(SMC)消息。

在一些实施例中,该第一消息为安全模式命令(SMC)消息,该第二消息为安全模式响应消息。

10 具体的,在本申请实施例中,第一终端设备可以根据第二终端设备生成的第一临时公钥、中继设备的相关信息和第一终端设备生成的第二临时私钥派生第一密钥。相应的,第二终端设备可以根据第一终端设备生成的第二临时公钥、中继设备的相关信息和第二终端设备生成的第一临时私钥派生第一密钥。其中,第二终端设备生成的第一临时公钥与第二终端设备生成的第一临时私钥配对,第一终端设备生成的第二临时公钥与第一终端设备生成的第二临时私钥配对。

具体例如,第一终端设备可以根据第一临时公钥和第二临时私钥,并使用 ECIES 算法计算出第一密钥;第二终端设备可以根据第二临时公钥和第一临时私钥,并使用 ECIES 算法计算出第一密钥。

在一些实施例中,该第二终端设备接收该第一终端设备通过该中继设备发送的第三消息;

15 其中,该第三消息用于指示安全模式建立完成,该第三消息通过目标密钥进行加密,且该第三消息包括以下至少之一:该第一终端设备生成的该第二密钥的标识的 y 个比特位,第三消息验证码;

其中,该目标密钥包括以下之一:该第一密钥,该第二密钥,该第二密钥派生的机密性保护密钥;

20 其中,该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护,或者,该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护,该第三消息验证码的输入参数包括该 y 个比特位。

在一些实施例中,该第二终端设备通过该目标密钥对该第三消息进行解密;

在该第三消息中携带的信息未遭受篡改的情况下,且该第三消息验证码有效的情况下,该第二终端设备将该 x 个比特位与该 y 个比特位合并得到该第二密钥的标识。

25 具体的,该第二终端设备可以基于该 y 个比特位生成第三消息验证码,并与该第三消息中包含的该第三消息验证码进行比较,若比较一致的情况下,该第三消息验证码有效。

具体例如,该第三消息为安全模式结束消息(security mode complete)。

30 在一些实施例中,该第二终端设备通过该中继设备向该第一终端设备发送错误消息;其中,该错误消息包括以下至少之一:原因信息,第四消息验证码;其中,该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突,或者,该原因信息用于指示该第一消息验证码验证失败,或者,该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败,该第四消息验证码的输入参数包括以下至少之一:该原因信息。

具体的,对于该第一终端设备,在该第四消息验证码有效的情况下,该第一终端设备确定安全模式建立失败,和/或,该第一终端设备重新发起安全模式建立流程。

在一些实施例中,该错误消息也可以受完整性保护。

35 具体例如,该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突,例如,该第二终端设备不支持该第一消息中携带的该第一终端设备的安全策略信息。

具体例如,该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败,例如,该第二终端设备不支持该第一消息中携带的该第一终端设备的安全能力信息。

在一些实施例中,该第二终端设备通过该中继设备向该第一终端设备发送认证请求消息;

40 其中,该认证请求消息包括以下至少之一:该第二终端设备所属用户的信息,该第二终端设备生成的第一临时公钥,该第二终端设备的签名,该中继设备的相关信息;

其中,该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK;该第二终端设备的签名的输入参数包括以下至少之一:该第二终端设备所属用户的信息和该第一临时公钥;该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥。

45 在本申请实施例中,该第二终端设备的签名的输入参数包括以下至少之一:该第二终端设备所属用户的信息和该第一临时公钥。也即,该第二终端设备可以基于该第二终端设备所属用户的信息和该第一临时公钥中的至少之一,生成该第二终端设备的签名。

50 在本申请实施例中,该中继设备的签名的输入参数包括以下至少之一:该第二终端设备的签名和该中继设备所属用户的信息。也即,该中继设备可以基于该第二终端设备的签名和该中继设备所属用户的信息中的至少之一,生成该中继设备的签名。

在一些实施例中,在该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK 的情况下,该第二终端设备的签名由该第二终端设备的秘密签名密钥(SSK)生

成。可选地，该第二终端设备的 PVT 和 KPAK、以及秘密签名密钥 (SSK) 可以是可信中心 KMS 通过安全通道为该第二终端设备预先配置的。该安全通道可以基于 AKMA 机制或者 GBA 机制来建立该第二终端设备与 KMS 的安全连接，该 KMS 可以直接由运营商来负责管理或者是与运营商有商业关系的第三方服务提供商。

5 在一些实施例中，该第一密钥可以是 K_D ，该第一密钥的标识可以是 K_D ID；该第二密钥可以是 K_{D-SESS} ，该第二密钥的标识可以是 K_{D-SESS} ID。

在一些实施例中，该完整性保护密钥包括控制面的完整性保护密钥 ($K_{D-CPint}$) 和用户面的完整性保护密钥 ($K_{D-UPint}$)；和/或，该机密性保护密钥包括控制面的机密性保护密钥 ($K_{D-CPenc}$) 和用户面的机密性保护密钥 ($K_{D-UPenc}$)。

10 因此，在本申请实施例中，第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥，第二密钥用于派生完整性保护密钥和/或机密性保护密钥，能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

15 本申请实施例适用于 5G L2 UE-to-UE relay 架构下第一终端设备（源设备）和第二终端设备（目标设备）之间的安全通信建立流程。借助公钥签名技术，能够确保终端设备的身份真实性和消息不可否认性，能够抗重放攻击、中间人攻击、伪装等多种主动攻击，同时保证认证流程消息的完整性，并且利用 3GPP 标准中使用的 ECIES 算法，从而建立了源 UE 和目标 UE 之间的端到端安全，确保双方传输数据的机密性和完整性，防止外部敌手甚至中继 (relay) 的窃听；本申请实施例保证了安全通信建立机制的可扩展性，另外，本申请实施例能够实现源 UE 和目标 UE 之间用户面和控制面安全策略、以及双方所支持加密和完整性保护算法的安全协商，能够实现完整性保护，抵抗篡改和降级攻击。

20 上文结合图 7 至图 8，详细描述了本申请的第一终端设备侧实施例，下文结合图 13，详细描述本申请的中继设备侧实施例，应理解，中继设备侧实施例与第一终端设备侧实施例相互对应，类似的描述可以参照第一终端设备侧实施例。

25 图 13 是根据本申请实施例的中继通信的方法 700 的示意性流程图，如图 13 所示，该中继通信的方法 700 可以包括如下内容中的至少部分内容：

30 S710，中继设备接收第一终端设备发送的第一消息；其中，该第一消息包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的第二临时公钥，该第一终端设备生成的第一密钥的标识的 M 个比特位，该第一终端设备的签名，第一消息验证码；其中，该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK；该第一终端设备的签名的输入参数包括以下至少之一：该第一终端设备所属用户的信息，该第二临时公钥，该第一密钥的标识的 M 个比特位，该第二终端设备的签名；其中，该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护，且该第一消息验证码的输入参数包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一随机数，该第二临时公钥，该 M 个比特位，该第一终端设备的签名；

35 S720，在该第一终端设备的 KPAK 有效，且基于该第一终端设备的标识和该第一终端设备的 PVT 对该第一终端设备的签名验证成功的情况下，该中继设备向该第二终端设备发送验证之后的第一消息；其中，该验证之后的第一消息包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该中继设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的与该第二临时私钥配对的第二临时公钥，该第一终端设备生成的该第一密钥的标识的 M 个比特位，该第一终端设备的签名，该中继设备的签名，该中继设备的相关信息，该第一消息验证码；其中，该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK；该中继设备的签名的输入参数包括以下至少之一：该中继设备所属用户的信息，该第一终端设备的签名，该第二终端设备的签名，该验证之后的第一消息；其中，该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，该第二密钥用于派生完整性保护密钥和/或机密性保护密钥，该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

50 本实施例基于 ECCSI 签名方案，建立 L2 架构下的 UE-to-UE 中继场景下的安全连接。具体的，本申请实施例应用于 L2 架构下的 UE-to-UE 中继场景，也即，第一终端设备与第二终端设备之间通过中继设备进行通信。例如，第一终端设备与第二终端设备之间的中继连接可以是 PC5 链路。

在本申请实施例中，第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥。也即，第一终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥，以及第一终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥，从而第一终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。同理，第二终端设备至少根据第一随机数、第一密钥和第二随机数派生第二密钥，以及第二终端设备可以基于第二密钥派生完整性保护密钥和/或机密性保护密钥，从而第二终端设备可以基于完整性保护密钥和/或机密性保护密钥对发送的消息进行安全保护。

在本申请实施例中，该第一消息验证码的输入参数包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一随机数，该第二临时公钥，该 M 个比特位。也即，该第一终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位中的至少之一，生成该第一消息验证码。

具体例如，假设该第一消息验证码的输入参数包括：该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位。该第二终端设备可以基于该第一终端设备的安全能力信息、该第一终端设备的安全策略信息、该第一随机数、该第二临时公钥、该 M 个比特位生成第一消息验证码，并与该第一消息中包含的该第一消息验证码进行比较，若比较一致的情况下，该第一消息验证码有效。

在一些实施例中，该第一消息为认证响应消息，或者，该第一消息为安全模式命令消息。

在一些实施例中，该第一终端设备的安全能力信息可以是该第一终端设备支持的密码算法列表。

在一些实施例中，该第一终端设备的安全策略信息可以是该第一终端设备是否支持机密性保护或完整性保护。其中，该第一终端设备的安全策略信息包括：该第一终端设备在控制面的安全策略信息，和/或，该第一终端设备在用户面的安全策略信息。

在一些实施例中，该 M 个比特位可以是该第一密钥的标识的最高 M 个比特位，该 N 个比特位可以是该第一密钥的标识的最低 N 个比特位；或者，该 M 个比特位可以是该第一密钥的标识的前 M 个比特位，该 N 个比特位可以是该第一密钥的标识的后 N 个比特位；或者，该 M 个比特位可以是该第一密钥的标识的偶数位的比特位，该 N 个比特位可以是该第一密钥的标识的奇数位的比特位。

在一些实施例中，M 与 N 的取值可以相同，也可以不同，本申请对此并不限定。

在一些实施例中，该中继设备将该第二终端设备发送的第二消息转发至该第一终端设备；

其中，该第二消息包括以下至少之一：该第二终端设备生成的该第二随机数，该第二终端设备生成的该第一密钥的标识的 N 个比特位，该第二终端设备生成的该第二密钥的标识的 x 个比特位，该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，第二消息验证码；

其中，该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护，或者，该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护，且该第二消息验证码的输入参数包括以下至少之一：该第二随机数，该 N 个比特位，该 x 个比特位，该第二终端设备选取的安全算法，该第二终端设备选取的安全策略；

其中，该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到，x 和 y 均为正整数。

在一些实施例中，该 x 个比特位可以是该第二密钥的标识的最高 x 个比特位，该 y 个比特位可以是该第二密钥的标识的最低 y 个比特位；或者，该 x 个比特位可以是该第二密钥的标识的前 x 个比特位，该 y 个比特位可以是该第二密钥的标识的后 y 个比特位；或者，该 x 个比特位可以是该第二密钥的标识的偶数位的比特位，该 y 个比特位可以是该第二密钥的标识的奇数位的比特位。

在一些实施例中，x 与 y 的取值可以相同，也可以不同，本申请对此并不限定。

具体例如，假设该第二消息验证码的输入参数包括：该第二随机数、该 N 个比特位、该 x 个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略。该第一终端设备可以基于该第二随机数、该 N 个比特位、该 x 个比特位、该第二终端设备选取的安全算法、该第二终端设备选取的安全策略生成第二消息验证码，并与该第二消息中包含的该第二消息验证码进行比较，若比较一致的情况下，该第二消息验证码有效。

在一些实施例中，该第二消息通过该第一密钥进行加密。当然，该第二消息也可以不通过该第一密钥进行加密，或者，该第二消息也可以不加密。

具体的，该第二终端设备可以基于该第一终端设备的安全能力信息选取安全算法，和/或，该第二终端设备可以基于该第一终端设备的安全策略信息选取安全策略。

在一些实施例中，该第一终端设备可以根据该第一随机数、该第一密钥、该第二随机数，以及源标识、目标标识、该第一随机数的长度、该第二随机数的长度、该源标识的长度、该目标标识的长度

中的至少之一,生成该第二密钥。以及该第二终端设备可以根据该第一随机数、该第一密钥、该第二随机数,以及源标识、目标标识、该第一随机数的长度、该第二随机数的长度、该源标识的长度、该目标标识的长度中的至少之一,生成该第二密钥。

其中,该源标识用于标识该第一终端设备与该第二终端设备之间的中继连接的源端,该目标标识用于标识该第一终端设备与该第二终端设备之间的中继连接的目标端。另外,该第二密钥的输入参数还可以包括其他系统设定参数,如 3GPP 指定的一个或多个固定参数。

在一些实施例中,该第一消息为认证响应消息,该第二消息为安全模式命令(SMC)消息。

在一些实施例中,该第一消息为安全模式命令(SMC)消息,该第二消息为安全模式响应消息。

在一些实施例中,该中继设备将该第一终端设备发送的第三消息转发至该第二终端设备;

其中,该第三消息用于指示安全模式建立完成,该第三消息通过目标密钥进行加密,且该第三消息包括以下至少之一:该第一终端设备生成的该第二密钥的标识的 y 个比特位,第三消息验证码;

其中,该目标密钥包括以下之一:该第一密钥,该第二密钥,该第二密钥派生的机密性保护密钥;

其中,该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护,或者,该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护,该第三消息验证码的输入参数包括该 y 个比特位。

在一些实施例中,对于该第二终端设备,该第二终端设备通过该目标密钥对该第三消息进行解密;在该第三消息中携带的信息未遭受篡改的情况下,且该第三消息验证码有效的情况下,该第二终端设备将该 x 个比特位与该 y 个比特位合并得到该第二密钥的标识。

具体的,该第二终端设备可以基于该 y 个比特位生成第三消息验证码,并与该第三消息中包含的该第三消息验证码进行比较,若比较一致的情况下,该第三消息验证码有效。

具体例如,该第三消息为安全模式结束消息(security mode complete)。

在一些实施例中,该中继设备将该第二终端设备发送的错误消息转发至该第一终端设备;其中,该错误消息包括以下至少之一:原因信息,第四消息验证码;其中,该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突,或者,该原因信息用于指示该第一消息验证码验证失败,或者,该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败,该第四消息验证码的输入参数包括以下至少之一:该原因信息。

具体的,在该第四消息验证码有效的情况下,该第一终端设备确定安全模式建立失败,和/或,该第一终端设备重新发起安全模式建立流程。

在一些实施例中,该错误消息也可以受完整性保护。

具体例如,该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突,例如,该第二终端设备不支持该第一消息中携带的该第一终端设备的安全策略信息。

具体例如,该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败,例如,该第二终端设备不支持该第一消息中携带的该第一终端设备的安全能力信息。

在一些实施例中,该中继设备接收该第二终端设备发送的认证请求消息;其中,该认证请求消息包括以下至少之一:该第二终端设备所属用户的信息,该第二终端设备生成的第一临时公钥,该第二终端设备的签名;其中,该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK;该第二终端设备的签名的输入参数包括以下至少之一:该第二终端设备所属用户的信息和该第一临时公钥;该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥;

在该第二终端设备的 KPAK 有效,且基于该第二终端设备的标识和该第二终端设备的 PVT 对该第二终端设备的签名验证成功的情况下,该中继设备向该第一终端设备发送验证之后的认证请求消息;其中,该验证之后的认证请求消息包括以下至少之一:该第二终端设备所属用户的信息,该中继设备所属用户的信息,该第一临时公钥,该第二终端设备的签名,该中继设备的签名,该中继设备的相关信息;其中,该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK;该中继设备的签名的输入参数包括以下至少之一:该第二终端设备的签名和该中继设备所属用户的信息。

在本申请实施例中,该第二终端设备的签名的输入参数包括以下至少之一:该第二终端设备所属用户的信息和该第一临时公钥。也即,该第二终端设备可以基于该第二终端设备所属用户的信息和该第一临时公钥中的至少之一,生成该第二终端设备的签名。

在本申请实施例中,该中继设备的签名的输入参数包括以下至少之一:该第二终端设备的签名和该中继设备所属用户的信息。也即,该中继设备可以基于该第二终端设备的签名和该中继设备所属用户的信息中的至少之一,生成该中继设备的签名。

具体的,该中继设备可以基于其本地存储的一个或多个 KPAK,验证该第二终端设备的 KPAK 的有效性。例如,在中继设备本地存储的 KPAK 中存在与第二终端设备的 KPAK 一致的 KPAK 的情况下,该第二终端设备的 KPAK 有效。可选地,该第一终端设备本地存储的一个或多个 KPAK 可以由 KMS 预配置。

在本申请实施例中,第一终端设备可以根据第二终端设备生成的第一临时公钥、中继设备的相关信息和第一终端设备生成的第二临时私钥派生第一密钥。相应的,第二终端设备可以根据第一终端设备生成的第二临时公钥、中继设备的相关信息和第二终端设备生成的第一临时私钥派生第一密钥。其中,第二终端设备生成的第一临时公钥与第二终端设备生成的第一临时私钥配对,第一终端设备生成的第二临时公钥与第一终端设备生成的第二临时私钥配对。

具体例如,第一终端设备可以根据第一临时公钥和第二临时私钥,并使用 ECIES 算法计算出第一密钥;第二终端设备可以根据第二临时公钥和第一临时私钥,并使用 ECIES 算法计算出第一密钥。

在一些实施例中,在该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK 的情况下,该第二终端设备的签名由该第二终端设备的秘密签名密钥 (SSK) 生成。可选地,该第二终端设备的 PVT 和 KPAK、以及秘密签名密钥 (SSK) 可以是可信中心 KMS 通过安全通道为该第二终端设备预先配置的。该安全通道可以基于 AKMA 机制或者 GBA 机制来建立该第二终端设备与 KMS 的安全连接,该 KMS 可以直接由运营商来负责管理或者是与运营商有商业关系的第三方服务提供商。

在一些实施例中,在该中继设备所属用户的信息包括该中继设备的标识、该中继设备的 PVT 和 KPAK 的情况下,该中继设备的签名由该中继设备的秘密签名密钥 (SSK) 生成。可选地,该中继设备的 PVT 和 KPAK、以及秘密签名密钥 (SSK) 可以是可信中心 KMS 通过安全通道为该中继设备预先配置的。该安全通道可以基于 AKMA 机制或者 GBA 机制来建立该中继设备与 KMS 的安全连接,该 KMS 可以直接由运营商来负责管理或者是与运营商有商业关系的第三方服务提供商。

在一些实施例中,该第一密钥可以是 K_D ,该第一密钥的标识可以是 K_D ID;该第二密钥可以是 K_{D-SESS} ,该第二密钥的标识可以是 K_{D-SESS} ID。

在一些实施例中,该完整性保护密钥包括控制面的完整性保护密钥 ($K_{D-CPint}$) 和用户面的完整性保护密钥 ($K_{D-UPint}$);和/或,该机密性保护密钥包括控制面的机密性保护密钥 ($K_{D-CPenc}$) 和用户面的机密性保护密钥 ($K_{D-UPenc}$)。

因此,在本申请实施例中,第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥,第二密钥用于派生完整性保护密钥和/或机密性保护密钥,能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性,从而确保双方传输数据的机密性和完整性,防止其他设备甚至中继设备的窃听。

本申请实施例适用于 5G L2 UE-to-UE relay 架构下源设备 (第一终端设备) 和目标设备 (第二终端设备) 之间的安全通信建立流程。借助公钥签名技术,能够确保终端设备的身份真实性和消息不可否认性,能够抗重放攻击、中间人攻击、伪装等多种主动攻击,同时保证认证流程消息的完整性,并且利用 3GPP 标准中使用的 ECIES 算法,从而建立了源 UE 和目标 UE 之间的端到端安全,确保双方传输数据的机密性和完整性,防止外部敌手甚至中继 (relay) 的窃听;本申请实施例保证了安全通信建立机制的可扩展性,另外,本申请实施例能够实现源 UE 和目标 UE 之间用户面和控制面安全策略、以及双方所支持加密和完整性保护算法的安全协商,能够实现完整性保护,抵抗篡改和降级攻击。

以下通过实施例 1 至实施例 2 详述本申请 L2 架构下的 UE-to-UE 中继场景中基于签名的安全通信建立流程。

实施例 1,如图 14 所示,假设所有设备之间在此之前没有建立任何安全连接,可以通过 S1-0 至 S1-8 中的部分或全部步骤建立 L2 架构下的 UE-to-UE 中继场景下基于签名的安全通信连接。具体的,UE1 可以是第一终端设备,UE2 可以是第二终端设备,UE-to-UE relay 可以是中继设备, K_D 可以是第一密钥, K_{D-SESS} 可以是第二密钥。

S1-0. UE1、UE2、终端至终端中继设备 (UE-to-UE relay) 获得了密钥管理服务器 (KMS) 下发的签名公钥 (KPAK),以及一组与 UE 标识相关的凭证,即秘密签名密钥 (SSK) 和公共验证参数 (PVT),可使用 UE-to-UE relay 服务。UE-to-UE relay 向网络注册可提供 UE-to-UE Relay 功能,UE-to-UE Relay 配置了中继策略参数。

S1-1. UE2 确定 PC5 单播链路建立时信令接收的目的 L2 ID。

S1-2. UE1 通过广播方式发送端到端的直接通信请求消息,具体的,在源终端 (即 UE1) 上,应用层向 ProSe 层提供 PC5 单播通信的信息 (如广播 L2 ID、ProSe 应用层 ID、终端应用层 ID、目标终端应用层 ID、中继适用指示),ProSe 层通过发送端到端广播直接通信请求消息触发终端的发现机制。

消息使用源 L2 ID 和广播 L2 ID 作为目的发送，并包含其他与应用程序相关的参数。

S1-3. UE-to-UE Relay 接收广播的直接通信请求消息，并验证 UE-to-UE Relay 是否配置为转发这个应用程序，例如，UE-to-UE Relay 将宣布的 ProSe 应用 ID 与它所提供中继策略/参数进行比较。UE-to-UE Relay 转发端到端广播的直接通信请求消息时，使用自己的 L2 ID 作为源 (Source) L2 ID，并在消息中添加 UE-to-UE Relay 的 UE ID，在适配层指定标识 UE1 的信息。UE-to-UE Relay 在 ProSe 层处理此端到端广播消息，并根据适配层信息转发任何后续的端到端 PC5-S 消息。

S1-4a. UE2 对宣布的应用程序感兴趣，如果 UE2 和 UE-to-UE Relay 之间不存在每跳链路，UE2 会触发 UE-to-UE Relay 建立每跳链路。UE2 发送每跳链路建立过程消息，源地址是 UE2 L2 ID，目的地址是中继的 L2 ID。

S1-4b. 如果 UE-to-UE relay 和 UE1 之间不存在每跳链路，则执行 UE-to-UE relay 和 UE1 之间的每跳链路建立过程。UE1 将自己的 L2 ID 作为源地址，中继的 L2 ID 作为目的地址。

S1-5a. 当 UE-2 和 UE-to-UE relay 成功建立了每跳链路 (per hop link)，将进一步触发 UE2 和 UE1 间端到端安全的建立。若 UE2 已具备 K_D ID 及安全环境，同时 UE1 和 UE2 之间建立不同 (Source ID、Destination ID) 组之间的链接安全上下文时，那么可选的是，UE2 可以省略认证流程，直接执行安全模式命令消息，或者考虑更高安全性，重新继续执行认证流程，创建该 Source ID 与 Destination ID 组下的崭新安全环境；若 UE1 和 UE2 初次建立安全连接，那么 UE2 必须通过 UE-to-UE relay 和 UE1 执行认证流程。当执行认证流程时，UE2 首先产生一对临时公私钥，即第一临时公钥 (Ephemeral public key1) 和第一临时私钥 (Ephemeral private key1)，然后通过 UE-to-UE relay 与 UE1 进行通信。

具体的，UE2 发送认证请求消息，包括以下参数：

UE2 所属用户的信息，其中，UE2 所属用户的信息包括 UE2 的标识和 UE2 的 PVT 和 KPAK；
第一临时公钥 (Ephemeral public key1)；

UE2 的签名，其中，UE2 的签名的输入参数包括以下至少之一：“UE2 所属用户的信息”和“第一临时公钥”。

S1-5b. 在收到认证请求消息后，UE-to-UE relay 验证 UE2 所属用户的信息中的 UE2 的 KPAK 有效性 (具体的，UE-to-UE relay 根据本地存储信息验证 UE2 的 KPAK 有效性，例如，在 UE-to-UE relay 本地存储的 KPAK 中存在与 UE2 的 KPAK 一致的 KPAK，UE2 的 KPAK 有效)，UE-to-UE relay 基于 UE2 的标识和 UE2 的 PVT 对 UE2 的签名进行验证。

最后，如果 UE2 的签名验证有效，那么 UE-to-UE relay 向 UE1 发送验证之后的认证请求消息，验证之后的认证请求消息除了包括上述认证请求消息内的全部内容外，还包括以下参数：

UE-to-UE relay 所属用户的信息，其中，UE-to-UE relay 所属用户的信息包括 UE-to-UE relay 的标识和 UE-to-UE relay 的 PVT 和 KPAK；

UE-to-UE relay 的签名，其中，UE-to-UE relay 的签名中输入参数包括以下至少之一：“UE2 的签名”和“UE-to-UE relay 所属用户的信息”；

UE-to-UE relay 的相关信息，其中，该 UE-to-UE relay 的相关信息包括以下之一：该 UE-to-UE relay 的身份信息，该 UE-to-UE relay 生成的随机数，该 UE-to-UE relay 生成的计数器。

S1-6a. 在收到认证请求消息后，UE1 分别检查 UE2 的 KPAK 和 UE-to-UE relay 的 KPAK，在 UE2 的 KPAK 和 UE-to-UE relay 的 KPAK 有效的情况下，且基于 UE2 的标识和 UE2 的 PVT 对 UE2 的签名进行验证，以及基于 UE-to-UE relay 的标识和 UE-to-UE relay 的 PVT 对 UE-to-UE relay 的签名进行验证。如果 UE2 的签名和 UE-to-UE relay 的签名验证成功，那么 UE1 产生临时公私钥对，即第二临时公钥 (Ephemeral public key2) 和第二临时私钥 (Ephemeral private key2)，然后，UE1 根据第一临时公钥、UE-to-UE relay 的相关信息和第二临时私钥，使用 ECIES 算法，计算出共享密钥 K_D ，并且生成 K_D ID 的 M 个比特位， K_D ID 用于标识 K_D 。

最后，UE1 通过 UE-to-UE relay 发送认证响应消息，包括以下参数：

UE1 的安全能力信息 (可选)；

UE1 的安全策略信息 (可选)；

UE1 所属用户的信息，其中，UE1 所属用户的信息包括 UE1 的标识和 UE1 的 PVT 和 KPAK；

第一随机数 (Nonce_1)；

第二临时公钥 (Ephemeral public key2)；

K_D ID 的 M 个比特位；

UE1 的签名，其中，UE1 的签名输入参数包括但不限于以下至少之一：“UE1 所属用户的信息”、“第二临时公钥”、“第一随机数 (Nonce_1)”、“ K_D ID 的 M 个比特位”和“UE2 的签名”；
第一消息验证码。

具体的, 该认证响应消息通过基于 K_D 生成的该第一消息验证码进行完整性保护, 且该第一消息验证码的输入参数包括以下至少之一: UE1 的安全能力信息, UE1 的安全策略信息, UE1 所属用户的信息, 第一随机数 (Nonce_1), 该第二临时公钥, K_D ID 的 M 个比特位, UE1 的签名。

若 UE1 的安全能力和 UE1 的安全策略没有更新, 那么在认证响应消息中可以不发送 UE1 的安全能力信息和 UE1 的安全策略信息。

S1-6b. 收到认证响应消息后, UE-to-UE relay 验证 UE1 所属用户的信息中的 UE1 的 KPAK 的有效性 (具体的, UE-to-UE relay 根据本地存储信息验证 UE1 的 KPAK 有效性, 例如, 在 UE-to-UE relay 本地存储的 KPAK 中存在与 UE1 的 KPAK 一致的 KPAK, UE1 的 KPAK 有效), UE-to-UE relay 基于 UE1 的标识和 UE1 的 PVT 对 UE1 的签名进行验证。最后, 如果 UE1 的签名验证成功, UE-to-UE relay 向 UE2 发送验证之后的认证响应消息, 其中, 验证之后的认证响应消息包含以下参数:

UE1 的安全能力信息 (可选);

UE1 的安全策略信息 (可选);

第一随机数 (Nonce_1);

UE1 所属用户的信息, 其中, UE1 所属用户的信息包括 UE1 的标识和 UE1 的 PVT 和 KPAK;

第二临时公钥;

K_D ID 的 M 个比特位;

UE1 的签名;

UE-to-UE relay 所属用户的信息;

UE-to-UE relay 的签名 2, 其中, 该 UE-to-UE relay 的签名 2 输入参数包括以下至少之一: “UE-to-UE relay 所属用户的信息”、“UE1 的签名”、“UE2 的签名”和“验证之后的认证响应消息”;

第一消息验证码。

S1-7. 收到验证之后的认证响应消息后, UE2 分别检查 UE1 的 KPAK 和 UE-to-UE relay 的 KPAK, 在 UE1 的 KPAK 和 UE-to-UE relay 的 KPAK 有效的情况下, 且基于 UE1 的标识和 UE1 的 PVT 对 UE1 的签名进行验证, 以及基于 UE-to-UE relay 的标识和 UE-to-UE relay 的 PVT 对 UE-to-UE relay 的签名进行验证。如果 UE1 的签名和 UE-to-UE relay 的签名验证成功, UE2 验证认证响应消息中包含的信息的完整性, UE2 基于第一临时私钥、UE-to-UE relay 的相关信息和第二临时公钥, 利用 ECIES 算法计算出共享密钥 K_D 。在第一消息验证码合格的情况下, UE2 生成 K_D ID 的 N 个比特位, 并将 K_D ID 的 N 个比特位与接收到的 K_D ID 的 M 个比特位合并, 生成并存储完整的 K_D ID, 后续用于标识 K_D 。此时, UE1 和 UE2 双方进行了认证和根密钥协商, 之后 UE2 开始处理认证响应消息。若该认证响应消息中包含 UE1 的安全能力信息与 UE1 的安全策略信息, UE2 协商出安全策略与安全算法, 然后生成第二随机数 (Nonce_2), 并根据利用第一随机数、第二随机数和 K_D 计算 K_{D-SESS} 和其他密钥 (即 $K_{D-CPint}$ 、 $K_{D-CPenc}$ 、 $K_{D-UPint}$ 、 $K_{D-UPenc}$)。另外 UE2 生成 K_{D-SESS} 的 x 个比特位。

最后, UE2 通过 UE-to-UE relay 发送一个受完整性保护的安全模式命令消息给 UE1, 其中, 安全模式命令消息中包含以下参数:

第二随机数 (Nonce_2);

K_D ID 的 N 个比特位;

K_{D-SESS} ID 的 x 个比特位;

UE2 选取的安全算法;

UE2 选取的安全策略;

第二消息验证码, 其中, 该安全模式命令消息通过基于 K_{D-SESS} 生成的该第二消息验证码进行完整性保护, 或者, 该安全模式命令消息通过基于 K_{D-SESS} 派生的完整性保护密钥生成的该第二消息验证码进行完整性保护, 且该第二消息验证码的输入参数包括以下至少之一: 第二随机数 (Nonce_2)、 K_D ID 的 N 个比特位、 K_{D-SESS} ID 的 x 个比特位、UE2 选取的安全算法、UE2 选取的安全策略。

需要注意的是, 如果 UE2 与 UE1 的安全策略相互冲突, 或者, 第一消息验证码验证失败, 或者, UE2 与 UE1 的安全算法协商失败, UE2 将回复错误消息, 其中, 该错误消息包括原因信息和第四消息校验码; 其中, 该原因信息用于指示 UE2 与 UE1 的安全策略冲突, 或者, 该原因信息用于指示第一消息验证码验证失败, 或者, 该原因信息用于指示 UE2 与 UE1 的安全算法协商失败; 该第四消息验证码的输入参数至少包括: 该原因信息。在第四消息验证码有效的情况下, UE1 确定安全模式建立失败, 和/或, UE1 重新发起安全模式建立流程。

S1-8. 接收到安全模式命令消息后, UE1 判断安全模式命令消息中携带的信息是否遭受篡改, 若未篡改, 那么 UE1 将 K_D ID 的 M 个比特位和 K_D ID 的 N 个比特位合并得到 K_D ID, 以及 UE1 采用与 UE2 相同的方式计算 K_{D-SESS} 以及其他密钥 (即 $K_{D-CPint}$ 、 $K_{D-CPenc}$ 、 $K_{D-UPint}$ 、 $K_{D-UPenc}$), UE1 生成 K_{D-SESS}

ID 的 y 个比特位, 并且 UE1 将 K_{D-SESS} ID 的 x 个比特位和 K_{D-SESS} ID 的 y 个比特位合并得到 K_{D-SESS} ID, 并保存 K_{D-SESS} ID。然后, UE1 验证第二消息校验码是否有效, 若有效, UE1 准备以新安全环境来保护后续通信。

具体的, 在第二消息验证码有效的情况下, UE1 根据 UE2 选取的安全算法、 K_{D-SESS} 、基于 K_{D-SESS} 生成完整性保护密钥和/或机密性保护密钥、UE2 选取的安全策略, 与 UE2 进行通信。

进一步地, UE1 向 UE2 发送安全模式结束消息, 该安全模式结束消息通过目标密钥进行加密, 且该安全模式结束消息包括以下至少之一: K_{D-SESS} ID 的 y 个比特位, 第三消息验证码; 其中, 该目标密钥包括以下之一: K_D 、 K_{D-SESS} 、 $K_{D-CPenc}$ 、 $K_{D-UPenc}$; 其中, 该安全模式结束消息通过基于 K_{D-SESS} 生成的该第三消息验证码进行完整性保护, 或者, 该安全模式结束消息通过基于 K_{D-SESS} 派生的完整性保护密钥生成的该第三消息验证码进行完整性保护, 该第三消息验证码的输入参数包括 K_{D-SESS} ID 的 y 个比特位。

具体的, UE2 验证第三消息校验码是否有效, 若有效, UE2 将 K_{D-SESS} ID 的 x 个比特位和 K_{D-SESS} ID 的 y 个比特位合并得到 K_{D-SESS} ID, 并保存 K_{D-SESS} ID。UE2 根据 UE2 选取的安全算法、 K_{D-SESS} 、基于 K_{D-SESS} 生成完整性保护密钥和/或机密性保护密钥、UE2 选取的安全策略, 与 UE1 进行通信。

实施例 2, 如图 15 所示, 假设所有设备之间在此之前没有建立任何安全连接, 可以通过 S2-0 至 S2-8 中的部分或全部步骤建立 L2 架构下 UE-to-UE 中继场景下基于签名的安全通信连接。具体的, UE1 可以是第一终端设备, UE2 可以是第二终端设备, UE-to-UE relay 可以是中继设备, K_D 可以是第一密钥, K_{D-SESS} 可以是第二密钥。

S2-0. UE1、UE2、终端至终端中继设备 (UE-to-UE relay) 获得了密钥管理服务器 (KMS) 下发的签名公钥 (KPAK), 以及一组与 UE 标识相关的凭证, 即秘密签名密钥 (SSK) 和公共验证参数 (PVT), 可使用 UE-to-UE relay 服务。UE-to-UE relay 向网络注册可提供 UE-to-UE Relay 功能, UE-to-UE Relay 配置了中继策略参数。

S2-1. UE2 确定 PC5 单播链路建立时信令接收的目的 L2 ID。

S2-2. UE1 通过广播方式发送端到端的直接通信请求消息, 具体的, 在源终端 (即 UE1) 上, 应用层向 ProSe 层提供 PC5 单播通信的信息 (如广播 L2 ID、ProSe 应用层 ID、终端应用层 ID、目标终端应用层 ID、中继适用指示), ProSe 层通过发送端到端广播直接通信请求消息触发终端的发现机制。消息使用源 L2 ID 和广播 L2 ID 作为目的发送, 并包含其他与应用程序相关的参数。

S2-3. UE-to-UE Relay 接收广播的直接通信请求消息, 并验证 UE-to-UE Relay 是否配置为转发这个应用程序, 例如, UE-to-UE Relay 将宣布的 ProSe 应用 ID 与它所提供的中继策略/参数进行比较。UE-to-UE Relay 转发端到端广播的直接通信请求消息时, 使用自己的 L2 ID 作为源 (Source) L2 ID, 并在消息中添加 UE-to-UE Relay 的 UE ID, 在适配层指定标识 UE1 的信息。UE-to-UE Relay 在 ProSe 层处理此端到端广播消息, 并根据适配层信息转发任何后续的中继 PC5-S 消息。

S2-4a. UE2 对宣布的应用程序感兴趣, 如果 UE2 和 UE-to-UE Relay 之间不存在每跳链路, UE2 会触发 UE-to-UE Relay 建立每跳链路。UE2 发送每跳链路建立过程消息, 源地址是 UE2 L2 ID, 目的地址是中继的 L2 ID。

S2-4b. 如果 UE-to-UE relay 和 UE1 之间不存在每跳链路, 则执行 UE-to-UE relay 和 UE1 之间的每跳链路建立过程。UE1 将自己的 L2 ID 作为源地址, 中继的 L2 ID 作为目的地址。

S2-5a. 当 UE-2 和 UE-to-UE relay 成功建立了每跳链路 (per hop link), 将进一步触发 UE2 和 UE1 间端到端安全的建立。若 UE2 已具备 K_D ID 及安全环境, 同时 UE1 和 UE2 之间建立不同 (Source ID、Destination ID) 组之间的链接安全上下文时, 那么可选的是, UE2 可以省略认证流程, 直接执行安全模式命令消息, 或者考虑更高安全性, 重新继续执行认证流程, 创建该 Source ID 与 Destination ID 组下的崭新安全环境; 若 UE1 和 UE2 初次建立安全连接, 那么 UE2 必须通过 UE-to-UE relay 和 UE1 执行认证流程。当执行认证流程时, UE2 首先产生一对临时公私钥, 即第一临时公钥 (Ephemeral public key1) 和第一临时私钥 (Ephemeral private key1), 然后通过 UE-to-UE relay 与 UE1 进行通信。

具体的, UE2 发送认证请求消息, 包括以下参数:

UE2 所属用户的信息, 其中, UE2 所属用户的信息包括 UE2 的标识和 UE2 的 PVT 和 KPAK; 第一临时公钥 (Ephemeral public key1);

UE2 的签名, 其中, UE2 的签名的输入参数包括以下至少之一: “UE2 所属用户的信息” 和 “第一临时公钥”。

S2-5b. 在收到认证请求消息后, UE-to-UE relay 验证 UE2 所属用户的信息中的 UE2 的 KPAK 有效性 (具体的, UE-to-UE relay 根据本地存储信息验证 UE2 的 KPAK 有效性, 例如, 在 UE-to-UE relay 本地存储的 KPAK 中存在与 UE2 的 KPAK 一致的 KPAK, UE2 的 KPAK 有效), UE-to-UE relay 基

于 UE2 的标识和 UE2 的 PVT 对 UE2 的签名进行验证。

最后, 如果 UE2 的签名验证有效, 那么 UE-to-UE relay 转发认证请求消息, 除了上述认证请求消息内的全部内容外, 还包括以下参数:

UE-to-UE relay 所属用户的信息, 其中, UE-to-UE relay 所属用户的信息包括 UE-to-UE relay 的标识和 UE-to-UE relay 的 PVT 和 KPAK;

UE-to-UE relay 的签名, 其中, UE-to-UE relay 的签名中输入参数包括以下至少之一: “UE2 的签名” 和 “UE-to-UE relay 所属用户的信息”;

UE-to-UE relay 的相关信息, 其中, 该 UE-to-UE relay 的相关信息包括以下之一: 该 UE-to-UE relay 的身份信息, 该 UE-to-UE relay 生成的随机数, 该 UE-to-UE relay 生成的计数器。

S2-6a. 在收到认证请求消息后, UE1 分别检查 UE2 的 KPAK 和 UE-to-UE relay 的 KPAK, 在 UE2 的 KPAK 和 UE-to-UE relay 的 KPAK 有效的情况下, 且基于 UE2 的标识和 UE2 的 PVT 对 UE2 的签名进行验证, 以及基于 UE-to-UE relay 的标识和 UE-to-UE relay 的 PVT 对 UE-to-UE relay 的签名进行验证。如果 UE2 的签名和 UE-to-UE relay 的签名验证成功, 那么 UE1 产生临时公私钥对, 即第二临时公钥 (Ephemeral public key2) 和第二临时私钥 (Ephemeral private key2), 然后, UE1 根据第一临时公钥、UE-to-UE relay 的相关信息和第二临时私钥, 使用 ECIES 算法, 计算出共享密钥 K_D , 并且生成 K_D ID 的 M 个比特位, K_D ID 用于标识 K_D 。

最后, UE1 通过 UE-to-UE relay 发送安全模式命令, 包括以下参数:

UE1 的安全能力信息 (可选);

UE1 的安全策略信息 (可选);

UE1 所属用户的信息, 其中, UE1 所属用户的信息包括 UE1 的标识和 UE1 的 PVT 和 KPAK;

第一随机数 (Nonce_1);

第二临时公钥 (Ephemeral public key2);

K_D ID 的 M 个比特位;

UE1 的签名, 其中, UE1 的签名输入参数包括但不限于以下至少之一: “UE1 所属用户的信息”、“第二临时公钥”、“第一随机数 (Nonce_1)”、“ K_D ID 的 M 个比特位”和 “UE2 的签名”;

第一消息验证码。

具体的, 该安全模式命令通过基于 K_D 生成的该第一消息验证码进行完整性保护, 且该第一消息验证码的输入参数包括以下至少之一: UE1 的安全能力信息, UE1 的安全策略信息, UE1 所属用户的信息, 第一随机数 (Nonce_1), 该第二临时公钥, K_D ID 的 M 个比特位, UE1 的签名。

若 UE1 的安全能力和 UE1 的安全策略没有更新, 那么在安全模式命令中可以不发送 UE1 的安全能力信息和 UE1 的安全策略信息。

S2-6b. 收到安全模式命令后, UE-to-UE relay 验证 UE1 所属用户的信息中的 UE1 的 KPAK 的有效性 (具体的, UE-to-UE relay 根据本地存储信息验证 UE1 的 KPAK 有效性, 例如, 在 UE-to-UE relay 本地存储的 KPAK 中存在与 UE1 的 KPAK 一致的 KPAK, UE1 的 KPAK 有效), UE-to-UE relay 基于 UE1 的标识和 UE1 的 PVT 对 UE1 的签名进行验证。最后, 如果 UE1 的签名验证成功, UE-to-UE relay 向 UE2 发送验证之后的安全模式命令, 其中, 验证之后的安全模式命令包含以下参数:

UE1 的安全能力信息 (可选);

UE1 的安全策略信息 (可选);

第一随机数 (Nonce_1);

UE1 所属用户的信息, 其中, UE1 所属用户的信息包括 UE1 的标识和 UE1 的 PVT 和 KPAK;

第二临时公钥;

K_D ID 的 M 个比特位;

UE1 的签名;

UE-to-UE relay 所属用户的信息;

UE-to-UE relay 的签名 2, 其中, 该 UE-to-UE relay 的签名 2 输入参数包括以下至少之一: “UE-to-UE relay 所属用户的信息”、“UE1 的签名”、“UE2 的签名”和 “验证之后的安全模式命令”。

第一消息验证码。

S2-7. 收到验证之后的安全模式命令后, UE2 分别检查 UE1 的 KPAK 和 UE-to-UE relay 的 KPAK, 在 UE1 的 KPAK 和 UE-to-UE relay 的 KPAK 有效的情况下, 且基于 UE1 的标识和 UE1 的 PVT 对 UE1 的签名进行验证, 以及基于 UE-to-UE relay 的标识和 UE-to-UE relay 的 PVT 对 UE-to-UE relay 的签名进行验证。如果 UE1 的签名和 UE-to-UE relay 的签名验证成功, UE2 验证认证响应消息中包含的信息的完整性, UE2 基于第一临时私钥、UE-to-UE relay 的相关信息和第二临时公钥, 利用 ECIES 算法

计算出共享密钥 K_D 。在第一消息验证码合格的情况下，UE2 生成 K_D ID 的 N 个比特位，并将 K_D ID 的 N 个比特位与接收到的 K_D ID 的 M 个比特位合并，生成并存储完整的 K_D ID，后续用于标识 K_D 。此时，UE1 和 UE2 双方进行了认证和根密钥协商，之后 UE2 开始处理安全模式命令。若该安全模式命令中包含 UE1 的安全能力信息与 UE1 的安全策略信息，UE2 协商出安全策略与安全算法，然后生成第二随机数 (Nonce_2)，并根据利用第一随机数、第二随机数和 K_D 计算 K_{D-SESS} 和其他密钥 (即 $K_{D-CPint}$ 、 $K_{D-CPenc}$ 、 $K_{D-UPint}$ 、 $K_{D-UPenc}$)。另外 UE2 生成 K_{D-SESS} 的 x 个比特位。

最后，UE2 通过 UE-to-UE relay 发送一个受完整性保护的安全模式响应给 UE1，其中，安全模式响应通过 K_D 进行加密，以及该安全模式响应中包含以下参数：

第二随机数 (Nonce_2)；

K_D ID 的 N 个比特位；

K_{D-SESS} ID 的 x 个比特位；

UE2 选取的安全算法；

UE2 选取的安全策略；

第二消息验证码，其中，该安全模式响应通过基于 K_{D-SESS} 生成的该第二消息验证码进行完整性保护，或者，该安全模式响应通过基于 K_{D-SESS} 派生的完整性保护密钥生成的该第二消息验证码进行完整性保护，且该第二消息验证码的输入参数包括以下至少之一：第二随机数 (Nonce_2)、 K_D ID 的 N 个比特位、 K_{D-SESS} ID 的 x 个比特位、UE2 选取的安全算法、UE2 选取的安全策略。

需要注意的是，如果 UE2 与 UE1 的安全策略相互冲突，或者，第一消息验证码验证失败，或者，UE2 与 UE1 的安全算法协商失败，UE2 将回复错误消息，其中，该错误消息包括原因信息和第四消息校验码；其中，该原因信息用于指示 UE2 与 UE1 的安全策略冲突，或者，该原因信息用于指示第一消息验证码验证失败，或者，该原因信息用于指示 UE2 与 UE1 的安全算法协商失败；该第四消息验证码的输入参数至少包括：该原因信息。在第四消息验证码有效的情况下，UE1 确定安全模式建立失败，和/或，UE1 重新发起安全模式建立流程。

S2-8. 接收到安全模式响应后，UE1 基于 K_D 对安全模式响应进行解密，在解密之后，UE1 判断安全模式响应中携带的信息是否遭受篡改，若未篡改，那么 UE1 将 K_D ID 的 M 个比特位和 K_D ID 的 N 个比特位合并得到 K_D ID，以及 UE1 采用与 UE2 相同的方式计算 K_{D-SESS} 以及其他密钥 (即 $K_{D-CPint}$ 、 $K_{D-CPenc}$ 、 $K_{D-UPint}$ 、 $K_{D-UPenc}$)，UE1 生成 K_{D-SESS} ID 的 y 个比特位，并且 UE1 将 K_{D-SESS} ID 的 x 个比特位和 K_{D-SESS} ID 的 y 个比特位合并得到 K_{D-SESS} ID，并保存 K_{D-SESS} ID。然后，UE1 验证第二消息校验码是否有效，若有效，UE1 准备以新安全环境来保护后续通信。

具体的，在第二消息验证码有效的情况下，UE1 根据 UE2 选取的安全算法、 K_{D-SESS} 、基于 K_{D-SESS} 生成完整性保护密钥和/或机密性保护密钥、UE2 选取的安全策略，与 UE2 进行通信。

进一步地，UE1 向 UE2 发送安全模式结束消息，该安全模式结束消息通过目标密钥进行加密，且该安全模式结束消息包括以下至少之一： K_{D-SESS} ID 的 y 个比特位，第三消息验证码；其中，该目标密钥包括以下之一： K_D 、 K_{D-SESS} 、 $K_{D-CPenc}$ 、 $K_{D-UPenc}$ ；其中，该安全模式结束消息通过基于 K_{D-SESS} 生成的该第三消息验证码进行完整性保护，或者，该安全模式结束消息通过基于 K_{D-SESS} 派生的完整性保护密钥生成的该第三消息验证码进行完整性保护，该第三消息验证码的输入参数包括 K_{D-SESS} ID 的 y 个比特位。

具体的，UE2 验证第三消息校验码是否有效，若有效，UE2 将 K_{D-SESS} ID 的 x 个比特位和 K_{D-SESS} ID 的 y 个比特位合并得到 K_{D-SESS} ID，并保存 K_{D-SESS} ID。UE2 根据 UE2 选取的安全算法、 K_{D-SESS} 、基于 K_{D-SESS} 生成完整性保护密钥和/或机密性保护密钥、UE2 选取的安全策略，与 UE1 进行通信。

图 16 是根据本申请实施例的中继通信的方法 800 的示意性流程图，如图 16 所示，该中继通信的方法 800 可以包括如下内容中的至少部分内容：

S810，第一终端设备通过中继设备向第二终端设备发送直接通信请求；其中，该直接通信请求包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备生成的第一临时公钥，该第一终端设备生成的第一随机数；其中，该直接通信请求通过第一加密密钥进行加密，以及该直接通信请求通过第一完整性保护密钥进行完整性保护，该第一加密密钥为基于已注册并被授权使用终端至终端中继 (UE-to-UE relay) 通信的终端的对称密钥衍生的加密密钥，该第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥；其中，该第一临时公钥和该中继设备的相关信息用于该第二终端设备派生第一密钥；该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥；其中，该中继设备的相关信息包

括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

本实施例基于 5G PKMT 分配的对称密钥建立安全通信的方案，建立 L2 架构下的 UE-to-UE 中继场景下的安全连接。具体的，本申请实施例应用于 L2 架构下的 UE-to-UE 中继场景，也即，第一终端设备与第二终端设备之间通过中继设备进行通信。例如，第一终端设备与第二终端设备之间的中继连接可以是 PC5 链路。

在本申请实施例中，该第一终端设备可以是源设备或源终端，该第二终端设备可以是目标设备或目标终端。该中继设备可以是中继终端。

在一些实施例中，该第一加密密钥可以为邻近业务加密密钥（PEK），该第一完整性保护密钥可以为邻近业务完整性保护密钥（PIK）。当然，该第一加密密钥也可以是其他的加密密钥，该第一完整性保护密钥也可以是其他的完整性保护密钥，本申请对此并不限定。

在一些实施例中，已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥可以由 ProSe 密钥管理功能（ProSe Key Management Function, PKMF）或 5G PKMF 分配。具体例如，在 5G PKMF 中，可以不具体定义 5G PKMF 给 UE 分配并管理的对称密钥的名称和数量。具体例如，在 4G PKMF 中，在 4G ProSe 中，PKMF 使用 MIKEY 机制为 UE 下发共享密钥，即 ProSe 组密钥（Prose Group Key, PGK）。

具体的，5G PKMF 和 UE 之间基于 MIKEY 机制安全下发群组密钥（PGK），第一终端设备和第二终端设备之间基于 PGK 衍生出 ProSe 传输密钥（Prose Traffic Key, PTK），以及进一步衍生出的 ProSe 完整性保护密钥（Prose Integrity Key, PIK）和 ProSe 加密密钥（Prose Encrypt Key, PEK），保护第一终端设备和/或第二终端设备传输的信息，以便第一终端设备和第二终端设备之间生成端到端的安全上下文。

在一些实施例中，本实施例涉及的密钥类型可以如表 1 所示。

表 1

PGK	群组密钥	UE 向 PKMF 请求，由 PKMF 使用 MIKEY 机制安全下发
PTK	传输密钥	由 PGK 衍生
PEK	加密密钥	由 PTK 衍生
PIK	完整性保护密钥	由 PTK 衍生

在一些实施例中，PTK 衍生输入参数可以如表 2 所示。

表 2

KDF 输入参数	具体值
FC	0X4A
P0	组成员标识（Group Member Identity） （例如，发端 UE 的 Layer 2 源 ID）
L0	P0 长度
P1	PTK 标识（PTK Identity）
L1	P1 长度
P2	组标识（Group Identity）
L2	P2 长度
输入密钥 （Input Key）	256 位 PGK

在一些实施例中，PEK/PIK 衍生输入参数可以如表 3 所示。

表 3

KDF 输入参数	具体值
FC	0X4B
P0	0X00(PEK) 0X01(PIK)
L0	P0 长度
P1	算法 ID
L1	P1 长度
输入密钥（Input Key）	256 位 PTK

在本申请实施例中，该第二加密密钥用于对第一终端设备与第二终端设备之间交互的端到端消息进行加密，以及该第二完整性保护密钥用于对第一终端设备与第二终端设备之间交互的端到端消息进行完整性保护。其中，该第二加密密钥可以是机密性保护密钥（ K_{D-enc} ），该第二完整性保护密钥可以是完整性保护密钥（ K_{D-int} ）。

5 在一些实施例中，该第二完整性保护密钥包括控制面的完整性保护密钥（ $K_{D-CPint}$ ）和用户面的完整性保护密钥（ $K_{D-UPint}$ ）；和/或，该第二加密密钥包括控制面的机密性保护密钥（ $K_{D-CPenc}$ ）和用户面的机密性保护密钥（ $K_{D-UPenc}$ ）。

10 在一些实施例中，该第二完整性保护密钥的输入参数包括以下至少之一：该第二密钥，选定的算法类型标识符，选定的算法类型标识符的长度，完整性保护算法标识，完整性保护算法标识的长度。也即，可以基于该第二密钥、选定的算法类型标识符、选定的算法类型标识符的长度、完整性保护算法标识、完整性保护算法标识的长度中的至少之一，生成该第二完整性保护密钥。或者，该第二完整性保护密钥的输入参数包括以下至少之一：该第一随机数，该第一密钥，该第二随机数，选定的算法类型标识符，选定的算法类型标识符的长度，完整性保护算法标识，完整性保护算法标识的长度。

15 可选地，该第二完整性保护密钥的输入参数还可以包括一些系统设定参数。在该第二密钥自动刷新时，该第二完整性保护密钥自动更新。

20 在一些实施例中，该第二加密密钥的输入参数包括以下至少之一：该第二密钥，选定的算法类型标识符，选定的算法类型标识符的长度，机密性保护算法标识，机密性保护算法标识的长度。也即，可以基于该第二密钥、选定的算法类型标识符、选定的算法类型标识符的长度、机密性保护算法标识、机密性保护算法标识的长度中的至少之一，生成该第二加密密钥。或者，该第二加密密钥的输入参数包括以下至少之一：该第一随机数，该第一密钥，该第二随机数，选定的算法类型标识符，选定的算法类型标识符的长度，机密性保护算法标识，机密性保护算法标识的长度。

可选地，该第二加密密钥的输入参数还可以包括一些系统设定参数。在该第二密钥自动刷新时，该第二加密密钥自动更新。

25 在一些实施例中，对于控制面的完整性保护密钥（ $K_{D-CPint}$ ），选定的算法类型标识符可以通过“控制面完整性保护算法”或设置特定值来表示。

在一些实施例中，对于控制面的机密性保护密钥（ $K_{D-CPenc}$ ），选定的算法类型标识符可以通过“控制面机密性保护算法”或设置特定值来表示。

30 在一些实施例中，对于用户面的完整性保护密钥（ $K_{D-UPint}$ ），选定的算法类型标识符可以通过“用户面完整性保护算法”或设置特定值来表示。

在一些实施例中，对于用户面的机密性保护密钥（ $K_{D-UPenc}$ ），选定的算法类型标识符可以通过“用户面机密性保护算法”或设置特定值来表示。

在一些实施例中，该第一终端设备接收该第二终端设备通过该中继设备发送的安全模式命令；

35 其中，该安全模式命令包括以下至少之一：该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，该第二终端设备生成的第二临时公钥，该第二终端设备生成的该第二随机数，该第二终端设备生成的该第一密钥的标识的 M 个比特位，该中继设备的相关信息，第一消息验证码；

其中，该安全模式命令通过该第一加密密钥进行加密，该安全模式命令通过该第一完整性保护密钥进行完整性保护，该第一消息验证码基于该第二完整性保护密钥生成，且该第一消息验证码的输入参数包括以下至少之一：该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，该第二临时公钥，该第二随机数，该 M 个比特位，该中继设备的相关信息；

40 其中，该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥，该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数。

在一些实施例中，该第二终端设备可以基于该第一终端设备的安全能力信息选取安全算法，和/或，该第二终端设备可以基于该第一终端设备的安全策略信息选取安全策略。

在一些实施例中，该第一终端设备的安全能力信息可以是该第一终端设备支持的密码算法列表。

45 在一些实施例中，该第一终端设备的安全策略信息可以是该第一终端设备是否支持机密性保护或完整性保护。其中，该第一终端设备的安全策略信息包括：该第一终端设备在控制面的安全策略信息，和/或，该第一终端设备在用户面的安全策略信息。

50 在一些实施例中，该 M 个比特位可以是该第一密钥的标识的最高 M 个比特位，该 N 个比特位可以是该第一密钥的标识的最低 N 个比特位；或者，该 M 个比特位可以是该第一密钥的标识的前 M 个比特位，该 N 个比特位可以是该第一密钥的标识的后 N 个比特位；或者，该 M 个比特位可以是该第一密钥的标识的偶数位的比特位，该 N 个比特位可以是该第一密钥的标识的奇数位的比特位。

在一些实施例中，M 与 N 的取值可以相同，也可以不同，本申请对此并不限定。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该安全模式命令还包括该第二终端设备生成的该第二密钥的标识的 x 个比特位,以及该第一消息验证码的输入参数包括该 x 个比特位;其中,该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

5 在一些实施例中,该 x 个比特位可以是该第二密钥的标识的最高 x 个比特位,该 y 个比特位可以是该第二密钥的标识的最低 y 个比特位;或者,该 x 个比特位可以是该第二密钥的标识的前 x 个比特位,该 y 个比特位可以是该第二密钥的标识的后 y 个比特位;或者,该 x 个比特位可以是该第二密钥的标识的偶数位的比特位,该 y 个比特位可以是该第二密钥的标识的奇数位的比特位。

在一些实施例中, x 与 y 的取值可以相同,也可以不同,本申请对此并不限定。

10 在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该第一终端设备使用该第一加密密钥解密该安全模式命令,以及使用该第一完整性保护密钥判断该安全模式命令的完整性;

15 在该安全模式命令中携带的信息未遭受篡改的情况下,该第一终端设备根据与该第一临时公钥配对的第一临时私钥、该第二临时公钥、该中继设备的相关信息派生该第一密钥,且该第一终端设备生成该第一密钥的标识的该 N 个比特位,以及将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识;

该第一终端设备至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥,该第一终端设备根据该第二密钥生成该第二完整性保护密钥和/或该第二加密密钥,以及该第一终端设备生成该第二密钥的标识的该 y 个比特位,并将该 x 个比特位和该 y 个比特位合并得到该第二密钥的标识;

20 在该第一消息验证码有效的情况下,该第一终端设备根据该第二终端设备选取的安全算法、该第二完整性保护密钥和/或该第二加密密钥、该第二终端设备选取的安全策略,与该第二终端设备进行通信。

25 在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该第一终端设备通过该中继设备向该第二终端设备发送安全模式建立完成消息;其中,该安全模式建立完成消息通过该第二密钥或该第二加密密钥进行加密,该安全模式建立完成消息通过该第二密钥或该第二完整性保护密钥进行完整性保护;其中,该安全模式建立完成消息至少包括该第二密钥的标识的该 y 个比特位。

30 在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该第二完整性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,该第二加密密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

35 在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下,该第一终端设备使用该第一加密密钥解密该安全模式命令,以及使用该第一完整性保护密钥判断该安全模式命令的完整性;

在该安全模式命令中携带的信息未遭受篡改的情况下,该第一终端设备根据与该第一临时公钥配对的第一临时私钥、该第二临时公钥、该中继设备的相关信息派生该第一密钥,且该第一终端设备生成该第一密钥的该 N 个比特位,以及将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识;

40 该第一终端设备至少根据该第一随机数、该第一密钥和该第二随机数生成该第二完整性保护密钥和/或该第二加密密钥;

在该第一消息验证码有效的情况下,该第一终端设备根据该第二终端设备选取的安全算法、该第二完整性保护密钥和/或该第二加密密钥、该第二终端设备选取的安全策略,与该第二终端设备进行通信。

45 在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下,该第一终端设备通过该中继设备向该第二终端设备发送安全模式建立完成消息;其中,该安全模式建立完成消息通过该第二加密密钥进行加密,该安全模式建立完成消息通过该第二完整性保护密钥进行完整性保护。

50 在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下,该第二完整性保护密钥的输入参数包括以下至少之一:该第一随机数,该第一密钥,该第二随机数,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,该第二加密密钥的输入参数包括以下至少之一:该第一随机数,该第一密钥,该第二随机数,选定的算法类型标识符,选定的算法类型标识符的长度,

机密性保护算法标识, 机密性保护算法标识的长度。

在一些实施例中, 对于第一终端设备而言, 生成第一密钥时的输入参数包括: 第一终端设备生成的第二临时私钥 (Ephemeral private key2)、第二终端设备生成的第一临时公钥 (Ephemeral public key1), 以及中继设备的相关信息 (如中继设备的身份信息, 或者中继设备生成的随机数, 或者中继设备生成的计数器 (COUNT))。对于第二终端设备而言, 生成第一密钥时的输入参数包括: 第一终端设备生成的第二临时公钥 (Ephemeral public key2)、第二终端设备生成的第一临时私钥 (Ephemeral private key1), 以及中继设备的相关信息 (如中继设备的身份信息, 或者中继设备生成的随机数, 或者中继设备生成的计数器 (COUNT))。其中, 第一临时公钥与第一临时私钥配对, 第二临时公钥与第二临时私钥配对。

在一些实施例中, 该第一密钥可以是 K_D , 该第一密钥的标识可以是 K_D ID; 该第二密钥可以是 K_{D-SESS} , 该第二密钥的标识可以是 K_{D-SESS} ID。

K_D : 密钥长度至少为 256 比特 (bits), 由源设备和目标设备双方通过临时公私钥协商生成。基于根密钥, 通过重新运行认证流程来更新 K_D 。 K_D 用于生成下一层密钥 K_{D-SESS} 。即使源设备与目标设备之间没有活动的通信会话, 那么也可以保存该密钥。 K_D ID 可以用来标识 K_D 。

K_D : 对于 UE-1 而言, 生成时的输入参数包括: UE-1 的临时私钥 Ephemeral private key2、UE-2 的临时公钥 Ephemeral public key1、以及 UE-relay 的身份信息, 或者 UE-relay 生成的随机数, 或者 UE-relay 生成的计数器 COUNT; 对于 UE-2 而言, 生成时的输入参数包括: UE-1 的临时公钥 Ephemeral public key2、UE-2 的临时私钥 Ephemeral private key1、以及 UE-relay 的身份, 或者 UE-relay 生成的随机数, 或者 UE-relay 生成的计数器 COUNT。

K_{D-SESS} : 密钥长度至少为 256bits, K_{D-SESS} 用于派生下一层完整性保护或机密性保护密钥。可以基于 K_D , 通过重新运行安全连接建立流程或者相关的密钥更新流程来刷新 K_{D-SESS} 。 K_{D-SESS} ID 用于标识 K_{D-SESS} 。 K_{D-SESS} 由 K_D 使用 HMAC-SHA-256 或 HMAC-SM3 等密钥派生算法衍生而成。 K_{D-SESS} 的输入参数至少必须含有密钥 K_D 、随机数 Nonce_1 (即第一终端设备生成的第一随机数)、随机数 Nonce_2 (即第二终端设备生成的第二随机数)。可选地, K_{D-SESS} 的输入参数还可以包括但不限于以下至少之一: 源标识 (Source ID)、目标标识 (Destination ID)、随机数 Nonce_1 的长度、随机数 Nonce_2 的长度、源标识 (Source ID) 的长度、目标标识 (Destination ID) 的长度。另外, K_{D-SESS} 的输入参数还可以包括其他系统设定参数, 如 3GPP 指定的一个或多个固定参数。

$K_{D-CPint}$: 密钥长度至少为 128bits, 该密钥可以用于控制面数据完整性保护, 该密钥由 K_{D-SESS} 使用 HMAC-SHA-256 或 HMAC-SM3 等密钥派生算法衍生而来。 $K_{D-CPint}$ 的输入参数至少必须含有密钥 K_{D-SESS} 、所选定的算法类型标识符 (比如 “控制面完整性保护算法” 或设置特定值来表示) 及该选定的算法类型标识符的长度, 完整性保护算法标识以及该完整性保护算法标识的长度, 其他系统设定参数可以作为可选输入参数。在 K_{D-SESS} 自动刷新时, $K_{D-CPint}$ 自动更新。

$K_{D-CPenc}$: 密钥长度至少为 128bits, 该密钥可以用于控制面数据机密性保护, 该密钥由 K_{D-SESS} 使用 HMAC-SHA-256 或 HMAC-SM3 等密钥派生算法衍生而来。 $K_{D-CPenc}$ 的输入参数至少必须含有密钥 K_{D-SESS} 、所选定的算法类型标识符 (比如 “控制面机密性保护算法” 或设置特定值来表示) 及选定的算法类型标识符的长度, 机密性保护算法标识以及该机密性保护算法标识的长度, 其他系统设定参数可以作为可选输入参数。在 K_{D-SESS} 自动刷新时, $K_{D-CPenc}$ 自动更新。

$K_{D-UPint}$: 密钥长度至少为 128bits, 该密钥可以用于用户面数据完整性保护, 该密钥由 K_{D-SESS} 使用 HMAC-SHA-256 或 HMAC-SM3 等密钥派生算法衍生而来。 $K_{D-UPint}$ 的输入参数至少必须含有密钥 K_{D-SESS} 、所选定的算法类型标识符 (比如 “用户面完整性保护算法” 或设置特定值来表示) 及该选定的算法类型标识符的长度, 完整性保护算法标识以及该完整性保护算法标识的长度, 其他系统设定参数可以作为可选输入参数。在 K_{D-SESS} 自动刷新时, $K_{D-UPint}$ 自动更新。

$K_{D-UPenc}$: 密钥长度至少为 128bits, 该密钥可以用于用户面数据机密性保护, 该密钥由 K_{D-SESS} 使用 HMAC-SHA-256 或 HMAC-SM3 等密钥派生算法衍生而来。 $K_{D-UPenc}$ 的输入参数至少必须含有密钥 K_{D-SESS} 、所选定的算法类型标识符 (比如 “用户面机密性保护算法” 或设置特定值来表示) 及该选定的算法类型标识符的长度, 机密性保护算法标识以及该机密性保护算法标识的长度, 其他系统设定参数可以作为可选输入参数。在 K_{D-SESS} 自动刷新时, $K_{D-UPenc}$ 自动更新。

在一些实施例中, 本申请中的 ECCSI 仅为示例, 并不局限于该算法, 也可以使用其他基于身份的公钥签名和公钥加密算法来替换, 在替换公钥算法的同时, 所有请求消息中与公钥算法相关的参数需要作相应替换。

在一些实施例中, 本申请中第一终端设备和第二终端设备使用的密钥派生函数不局限于 HMAC-SHA-256 或 HMAC-SM3, 包括任何一种满足计算安全的密钥派生函数。

在一些实施例中，本申请中密钥派生函数的输入参数不局限于上述提到的必要参数，可以含有其他可选参数，比如应用系统设置固定参数。

在一些实施例中，本申请中的密钥管理中心不限于 KMS、PKMF、5GPKMF，运营商管理或被第三方业务提供商管理的合法密钥管理中心均适用于本申请的技术方案。

5 本方案中，PKMF 为已注册并被授权使用 UE-to-UE relay 功能的终端设备下发的对称密钥不局限于上述方案，具体配置可根据运营商或业务提供商对 PKMF 的设计而更改。

在一些实施例中，本申请中安全通信建立流程中所有交互消息中的信息元素并不局限于上述方案中提到的内容，也可以增加由于应用系统要求的可选信息元素。

10 因此，在本申请实施例中，第一终端设备可以基于第二终端设备通过中继设备发送的直接通信请求生成第一密钥，且该直接通信请求通过第一加密密钥进行加密，以及直接通信请求通过第一完整性保护密钥进行完整性保护。以及第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥，第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，第一终端设备生成的第一随机数、第一密钥和第二终端设备用于派生第二随机数生成第二加密密钥和/或第二完整性保护密钥，能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

15 本申请实施例适用于 5G L2 UE-to-UE relay 架构下第一终端设备（源设备）和第二终端设备（目标设备）之间的安全通信建立流程。通过使用 PKMF 的密钥生成和安全下发功能，通过 PKMF 下发给已注册并被授权使用 UE-to-UE relay 功能的终端设备对称密钥，保护算法和密钥协商，从而高效的建立源 UE 和目标 UE 间端到端的安全通道。本申请实施例在计算和通信上都有非常高的效率，同样的能够实现认证性，加密保护，完整性保护，抵抗篡改和降级攻击。

20 上文结合图 16，详细描述了本申请的第一终端设备侧实施例，下文结合图 17，详细描述本申请的第二终端设备侧实施例，应理解，第二终端设备侧实施例与第一终端设备侧实施例相互对应，类似的描述可以参照第一终端设备侧实施例。

25 图 17 是根据本申请实施例的中继通信的方法 900 的示意性流程图，如图 17 所示，该中继通信的方法 900 可以包括如下内容中的至少部分内容：

30 S910，第二终端设备接收第一终端设备通过中继设备发送的直接通信请求；其中，该直接通信请求包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备生成的第一临时公钥，该第一终端设备生成的第一随机数，该中继设备的标识，该中继设备的相关信息；其中，该直接通信请求通过第一加密密钥进行加密，以及该直接通信请求通过第一完整性保护密钥进行完整性保护，该第一加密密钥为基于已注册并被授权使用终端至终端中继（UE-to-UE relay）通信的终端的对称密钥衍生的加密密钥，该第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器；该第一临时公钥和该中继设备的相关信息用于该第二终端设备派生第一密钥；该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

35 本实施例基于 5G PKMT 分配的对称密钥建立安全通信的方案，建立 L2 架构下的 UE-to-UE 中继场景下的安全连接。具体的，本申请实施例应用于 L2 架构下的 UE-to-UE 中继场景，也即，第一终端设备与第二终端设备之间通过中继设备进行通信。例如，第一终端设备与第二终端设备之间的中继连接可以是 PC5 链路。

40 在本申请实施例中，该第一终端设备可以是源设备或源终端，该第二终端设备可以是目标设备或目标终端。该中继设备可以是中继终端。

45 在一些实施例中，该第一加密密钥可以为邻近业务加密密钥（PEK），该第一完整性保护密钥可以为邻近业务完整性保护密钥（PIK）。当然，该第一加密密钥也可以是其他的加密密钥，该第一完整性保护密钥也可以是其他的完整性保护密钥，本申请对此并不限定。

在一些实施例中，在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下，该第二终端设备使用该第一加密密钥解密该直接通信请求，以及使用该第一完整性保护密钥判断该直接通信请求的完整性；

50 在该直接通信请求中携带的信息未遭受篡改的情况下，该第二终端设备生成第二临时私钥，以及该第二终端设备根据该第一临时公钥、该第二临时私钥和该中继设备的相关信息派生该第一密钥，且该第二终端设备生成该第一密钥的标识的 M 个比特位；

该第二终端设备生成该第二随时数,以及该第二终端设备至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥,该第二终端设备根据该第二密钥生成该第二完整性保护密钥和/或该第二加密密钥,且该第二终端设备生成该第二密钥的标识的 x 个比特位;

其中,该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数,该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

在一些实施例中,该第二终端设备可以基于该第一终端设备的安全能力信息选取安全算法,和/或,该第二终端设备可以基于该第一终端设备的安全策略信息选取安全策略。

在一些实施例中,该第一终端设备的安全能力信息可以是该第一终端设备支持的密码算法列表。

在一些实施例中,该第一终端设备的安全策略信息可以是该第一终端设备是否支持机密性保护或完整性保护。其中,该第一终端设备的安全策略信息包括:该第一终端设备在控制面的安全策略信息,和/或,该第一终端设备在用户面的安全策略信息。

在一些实施例中,该 M 个比特位可以是该第一密钥的标识的最高 M 个比特位,该 N 个比特位可以是该第一密钥的标识的最低 N 个比特位;或者,该 M 个比特位可以是该第一密钥的标识的前 M 个比特位,该 N 个比特位可以是该第一密钥的标识的后 N 个比特位;或者,该 M 个比特位可以是该第一密钥的标识的偶数位的比特位,该 N 个比特位可以是该第一密钥的标识的奇数位的比特位。

在一些实施例中, M 与 N 的取值可以相同,也可以不同,本申请对此并不限定。

在一些实施例中,该 x 个比特位可以是该第二密钥的标识的最高 x 个比特位,该 y 个比特位可以是该第二密钥的标识的最低 y 个比特位;或者,该 x 个比特位可以是该第二密钥的标识的前 x 个比特位,该 y 个比特位可以是该第二密钥的标识的后 y 个比特位;或者,该 x 个比特位可以是该第二密钥的标识的偶数位的比特位,该 y 个比特位可以是该第二密钥的标识的奇数位的比特位。

在一些实施例中, x 与 y 的取值可以相同,也可以不同,本申请对此并不限定。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该第二终端设备通过该中继设备向该第一终端设备发送安全模式命令;

其中,该安全模式命令包括以下至少之一:该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,该第二终端设备生成的与该第二临时私钥配对的第二临时公钥,该第二随机数,该第一密钥的标识的该 M 个比特位,该第二密钥的标识的该 x 个比特位,第一消息验证码;

其中,该安全模式命令通过该第一加密密钥进行加密,该安全模式命令通过该第一完整性保护密钥进行完整性保护,该第一消息验证码基于该第二完整性保护密钥生成,且该第一消息验证码的输入参数包括以下至少之一:该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,该第二临时公钥,该第二随机数,该 M 个比特位,该 x 个比特位,该中继设备的相关信息;该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该第二终端设备接收该第一终端设备通过该中继设备发送的安全模式建立完成消息;

其中,该安全模式建立完成消息通过该第二密钥或该第二加密密钥进行加密,该安全模式建立完成消息通过该第二密钥或该第二完整性保护密钥进行完整性保护;

其中,该安全模式建立完成消息至少包括该第二密钥的标识的该 y 个比特位。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该第二完整性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,

该第二加密密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下,该第二终端设备使用该第一加密密钥解密该直接通信请求,以及使用该第一完整性保护密钥判断该直接通信请求的完整性;

在该直接通信请求中携带的信息未遭受篡改的情况下,该第二终端设备生成第二临时私钥,以及该第二终端设备根据该第一临时公钥、该第二临时私钥和该中继设备的相关信息派生该第一密钥,且该第二终端设备生成该第一密钥的标识的 M 个比特位;

该第二终端设备生成该第二随时数,以及该第二终端设备至少根据该第一随机数、该第一密钥和该第二随机数生成该第二完整性保护密钥和/或该第二加密密钥;

其中,该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数。

在一些实施例中，在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下，该第二终端设备通过该中继设备向该第一终端设备发送安全模式命令；

其中，该安全模式命令包括以下至少之一：该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，该第二终端设备生成的与该第二临时私钥配对的第二临时公钥，该第二随机数，该第一密钥的标识的该 M 个比特位，第一消息验证码；

其中，该安全模式命令通过该第一加密密钥进行加密，该安全模式命令通过该第一完整性保护密钥进行完整性保护，该第一消息验证码基于该第二完整性保护密钥生成，且该第一消息验证码的输入参数包括以下至少之一：该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，该第二临时公钥，该第二随机数，该 M 个比特位；该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥。

在一些实施例中，在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下，该第二终端设备接收该第一终端设备通过该中继设备发送的安全模式建立完成消息；

其中，该安全模式建立完成消息通过该第二加密密钥进行加密，该安全模式建立完成消息通过该第二完整性保护密钥进行完整性保护。

在一些实施例中，在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下，该第二完整性保护密钥的输入参数包括以下至少之一：该第一随机数，该第一密钥，该第二随机数，选定的算法类型标识符，选定的算法类型标识符的长度，完整性保护算法标识，完整性保护算法标识的长度；和/或，

该第二加密密钥的输入参数包括以下至少之一：该第一随机数，该第一密钥，该第二随机数，选定的算法类型标识符，选定的算法类型标识符的长度，机密性保护算法标识，机密性保护算法标识的长度。

在一些实施例中，该安全模式命令还包括该中继设备的相关信息，以及该第一消息验证码的输入参数还包括该中继设备的相关信息。

在一些实施例中，该第二终端设备根据该第二终端设备选取的安全算法、该第二完整性保护密钥和/或该第二加密密钥、该第二终端设备选取的安全策略，与该第一终端设备进行通信。

因此，在本申请实施例中，第一终端设备可以基于第二终端设备通过中继设备发送的直接通信请求生成第一密钥，且该直接通信请求通过第一加密密钥进行加密，以及直接通信请求通过第一完整性保护密钥进行完整性保护。以及第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥，第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，第一终端设备生成的第一随机数、第一密钥和第二终端设备用于派生第二随机数生成第二加密密钥和/或第二完整性保护密钥，能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

本申请实施例适用于 5G L2 UE-to-UE relay 架构下第一终端设备（源设备）和第二终端设备（目标设备）之间的安全通信建立流程。通过使用 PKMF 的密钥生成和安全下发功能，通过 PKMF 下发给已注册并被授权使用 UE-to-UE relay 功能的终端设备对称密钥，保护算法和密钥协商，从而高效的建立源 UE 和目标 UE 间端到端的安全通道。本申请实施例在计算和通信上都有非常高的效率，同样的能够实现认证性，加密保护，完整性保护，抵抗篡改和降级攻击。

上文结合图 16，详细描述了本申请的第一终端设备侧实施例，下文结合图 18，详细描述本申请的中继设备侧实施例，应理解，中继设备侧实施例与第一终端设备侧实施例相互对应，类似的描述可以参照第一终端设备侧实施例。

图 18 是根据本申请实施例的中继通信的方法 1000 的示意性流程图，如图 18 所示，该中继通信的方法 1000 可以包括如下内容中的至少部分内容：

S1010，中继设备接收第一终端设备发送的直接通信请求；其中，该直接通信请求包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备生成的第一临时公钥，该第一终端设备生成的第一随机数；其中，该直接通信请求通过第一加密密钥进行加密，以及该直接通信请求通过第一完整性保护密钥进行完整性保护，该第一加密密钥为基于已注册并被授权使用终端至终端中继（UE-to-UE relay）通信的终端的对称密钥衍生的加密密钥，该第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥；

S1010，该中继设备验证是否被配置为转发直接通信请求，在验证通过之后该中继设备使用该第一加密密钥解密该直接通信请求以获取 QoS 和计费信息，以及该中继设备使用该第一完整性保护密

5 钥验证该直接通信请求的完整性,在验证通过之后该中继设备在该直接通信请求中添加该中继设备的相关信息,并且该中继设备使用该第一加密密钥加密该直接通信请求,使用该第一完整性保护密钥保护该直接通信请求的完整性,并将所述直接通信请求转发至第二终端设备;其中,该中继设备的相关信息包括以下之一:该中继设备的身份信息,该中继设备生成的随机数,该中继设备生成的计数器;该第一临时公钥和该中继设备的相关信息用于该第二终端设备派生第一密钥;该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥,且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥,或者,该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

10 本实施例基于 5G PKMT 分配的对称密钥建立安全通信的方案,建立 L2 架构下的 UE-to-UE 中继场景下的安全连接。具体的,本申请实施例应用于 L2 架构下的 UE-to-UE 中继场景,也即,第一终端设备与第二终端设备之间通过中继设备进行通信。例如,第一终端设备与第二终端设备之间的中继连接可以是 PC5 链路。

在本申请实施例中,该第一终端设备可以是源设备或源终端,该第二终端设备可以是目标设备或目标终端。该中继设备可以是中继终端。

15 在一些实施例中,该第一加密密钥可以为邻近业务加密密钥(PEK),该第一完整性保护密钥可以为邻近业务完整性保护密钥(PIK)。当然,该第一加密密钥也可以是其他的加密密钥,该第一完整性保护密钥也可以是其他的完整性保护密钥,本申请对此并不限定。

20 在本申请实施例中,该第二加密密钥用于对第一终端设备与第二终端设备之间交互的端到端消息进行加密,以及该第二完整性保护密钥用于对第一终端设备与第二终端设备之间交互的端到端消息进行完整性保护。其中,该第二加密密钥可以是机密性保护密钥。

25 在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该中继设备接收该第二终端设备发送的安全模式命令;其中,该安全模式命令包括以下至少之一:该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,该第二终端设备生成的第二临时公钥,该第二终端设备生成的该第二随机数,该第二终端设备生成的该第一密钥的标识的 M 个比特位,该第二终端设备生成的该第二密钥的标识的 x 个比特位,第一消息验证码;其中,该安全模式命令通过该第一加密密钥进行加密,该安全模式命令通过该第一完整性保护密钥进行完整性保护,该第一消息验证码基于该第二完整性保护密钥生成,且该第一消息验证码的输入参数包括以下至少之一:该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,该第二临时公钥,该第二随机数,该 M 个比特位,该 x 个比特位,该中继设备的相关信息;该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥;

30 该中继设备使用该第一加密密钥解密该安全模式命令,以获取服务质量(Quality of Service, QoS)和计费信息,并在向该第一终端设备转发该安全模式命令;其中,该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥,该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数,该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

35 在一些实施例中,该第二终端设备可以基于该第一终端设备的安全能力信息选取安全算法,和/或,该第二终端设备可以基于该第一终端设备的安全策略信息选取安全策略。

在一些实施例中,该第一终端设备的安全能力信息可以是该第一终端设备支持的密码算法列表。

40 在一些实施例中,该第一终端设备的安全策略信息可以是该第一终端设备是否支持机密性保护或完整性保护。其中,该第一终端设备的安全策略信息包括:该第一终端设备在控制面的安全策略信息,和/或,该第一终端设备在用户面的安全策略信息。

45 在一些实施例中,该 M 个比特位可以是该第一密钥的标识的最高 M 个比特位,该 N 个比特位可以是该第一密钥的标识的最低 N 个比特位;或者,该 M 个比特位可以是该第一密钥的标识的前 M 个比特位,该 N 个比特位可以是该第一密钥的标识的后 N 个比特位;或者,该 M 个比特位可以是该第一密钥的标识的偶数位的比特位,该 N 个比特位可以是该第一密钥的标识的奇数位的比特位。

在一些实施例中, M 与 N 的取值可以相同,也可以不同,本申请对此并不限定。

50 在一些实施例中,该 x 个比特位可以是该第二密钥的标识的最高 x 个比特位,该 y 个比特位可以是该第二密钥的标识的最低 y 个比特位;或者,该 x 个比特位可以是该第二密钥的标识的前 x 个比特位,该 y 个比特位可以是该第二密钥的标识的后 y 个比特位;或者,该 x 个比特位可以是该第二密钥的标识的偶数位的比特位,该 y 个比特位可以是该第二密钥的标识的奇数位的比特位。

在一些实施例中, x 与 y 的取值可以相同,也可以不同,本申请对此并不限定。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,

该中继设备向该第二终端设备转发该第一终端设备发送的安全模式建立完成消息；

其中，该安全模式建立完成消息通过该第二密钥或该第二加密密钥进行加密，该安全模式建立完成消息通过该第二密钥或该第二完整性保护密钥进行完整性保护；

其中，该安全模式建立完成消息至少包括该第二密钥的标识的该 y 个比特位。

5 在一些实施例中，在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下，该中继设备接收该第二终端设备发送的安全模式命令；其中，该安全模式命令包括以下至少之一：该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，该第二终端设备生成的第二临时公钥，该第二终端设备生成的该第二随机数，该第二终端设备生成的该第一密钥的标识的 M 个比特位，第一消息验证码；其中，该安全模式命令通过该第一加密密钥进行加密，该安全模式命令通过该第一完整性保护密钥进行完整性保护，该第一消息验证码基于该第二完整性保护密钥生成，且该第一消息验证码的输入参数包括以下至少之一：该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，该第二临时公钥，该第二随机数，该 M 个比特位，该中继设备的相关信息；该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥；

10 该中继设备使用该第一加密密钥解密该安全模式命令，以获取 QoS 和计费信息，并在向该第一终端设备转发该安全模式命令；其中，该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥，该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到， M 和 N 均为正整数。

20 在一些实施例中，在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下，该中继设备向该第二终端设备转发该第一终端设备发送的安全模式建立完成消息；其中，该安全模式建立完成消息通过该第二加密密钥进行加密，该安全模式建立完成消息通过该第二完整性保护密钥进行完整性保护。

在一些实施例中，该安全模式命令包括该中继设备的相关信息，以及该第一消息验证码的输入参数还包括该中继设备的相关信息；或者，该中继设备在向该第一终端设备转发的该安全模式命令中添加了该中继设备的相关信息。

25 因此，在本申请实施例中，第一终端设备可以基于第二终端设备通过中继设备发送的直接通信请求生成第一密钥，且该直接通信请求通过第一加密密钥进行加密，以及直接通信请求通过第一完整性保护密钥进行完整性保护。以及第一终端设备生成的第一随机数、第一密钥和第二终端设备生成的第二随机数用于派生第二密钥，第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，第一终端设备生成的第一随机数、第一密钥和第二终端设备用于派生第二随机数生成第二加密密钥和/或第二完整性保护密钥，能够保证第一终端设备和第二终端设备的身份安全与通信数据的机密性与完整性，从而确保双方传输数据的机密性和完整性，防止其他设备甚至中继设备的窃听。

30 本申请实施例适用于 5G L2 UE-to-UE relay 架构下第一终端设备（源设备）和第二终端设备（目标设备）之间的安全通信建立流程。通过使用 PKMF 的密钥生成和安全下发功能，通过 PKMF 下发给已注册并被授权使用 UE-to-UE relay 功能的终端设备对称密钥，保护算法和密钥协商，从而高效的建立源 UE 和目标 UE 间端到端的安全通道。本申请实施例在计算和通信上都有非常高的效率，同样的能够实现认证性，加密保护，完整性保护，抵抗篡改和降级攻击。

以下通过实施例 3 至实施例 6 详述本申请 L2 架构下的 UE-to-UE 中继场景中基于 5G PKMT 分配的对称密钥建立安全通信的流程。

40 实施例 3，如图 19 所示，假设所有设备之间在此之前没有建立任何安全连接，可以通过 S3-0 至 S3-6 中的部分或全部步骤建立 L2 架构下的 UE-to-UE 中继场景下基于签名的安全通信连接。具体的，UE1 可以是第一终端设备，UE2 可以是第二终端设备，UE-to-UE relay 可以是中继设备， K_D 可以是第一密钥， K_{D-SESS} 可以是第二密钥，第一加密密钥为 PEK，第一完整性保护密钥为 PIK。

45 S3-0. UE 向网络注册，并被授权 UE-to-UE relay 服务。UE-to-UE relay 向网络注册可提供 UE-to-UE Relay 功能，UE-to-UE relay 配置了中继策略参数。PKMF 使用 MIKEY 机制，向上述已注册并得到授权的 UE 发送相关的 PGK、PGK ID 和到期时间。

S3-1. UE2 确定 PC5 单播链路建立时信令接收的目的 L2 ID。

50 S3-2. UE1 通过广播方式发送端到端的直接通信请求消息，具体的，UE1 在将直接通信请求广播给周围的终端设备之前，先需要根据 PGK 衍生出传输密钥 PTK，并进一步生成 PTK 的下级密钥，即 PEK 和 PIK。UE1 使用 PEK 加密广播消息，使用 PIK 计算直接通信请求消息的 MAC 即保护直接通信请求消息的完整性，也即，该直接通信请求通过 PEK 进行加密，以及该直接通信请求通过 PIK 进行完整性保护。其中，直接通信请求中包含以下至少之一：

UE1 的安全能力信息（UE1 security capabilities）；

UE1 的安全策略信息 (UE1 security policy) ;

UE1 生成的第一临时公钥 (Ephemeral public key1) ;

UE1 生成的第一随机数 (Nonce-1) 。

S3-3. UE-to-UE Relay 接收广播的直接通信请求消息, 并验证 UE-to-UE Relay 是否配置为转发直接通信请求消息, 例如, UE-to-UE Relay 将宣布的 ProSe 应用 ID 与它所提供的中继策略/参数进行比较。UE-to-UE Relay 转发端到端广播的直接通信请求消息时, 使用自己的 L2 ID 作为源 (Source) L2 ID, 并在消息中添加 UE-to-UE Relay 的 UE ID, 在适配层指定标识 UE1 的信息。UE-to-UE Relay 在 ProSe 层处理此端到端广播消息, 并根据适配层信息转发任何后续的端到端 PC5-S 消息。

具体的, 在验证通过之后 UE-to-UE Relay 使用 PEK 解密直接通信请求以获取 QoS 和计费信息, 以及 UE-to-UE Relay 使用 PIK 验证直接通信请求的完整性, 在验证通过之后 UE-to-UE Relay 在直接通信请求中添加 UE-to-UE Relay 的相关信息和 UE-to-UE Relay 的标识, 并且 UE-to-UE Relay 使用 PEK 加密直接通信请求, 使用 PIK 保护直接通信请求的完整性; 其中, UE-to-UE Relay 的相关信息包括以下之一: UE-to-UE Relay 的身份信息, UE-to-UE Relay 生成的随机数, UE-to-UE Relay 生成的计数器。

S3-4a. UE2 对宣布的应用程序感兴趣, 如果 UE2 和 UE-to-UE Relay 之间不存在每跳链路, UE2 会触发 UE-to-UE Relay 建立每跳链路。UE2 发送每跳链路建立过程消息, 源地址是 UE2 L2 ID, 目的地址是中继的 L2 ID。

S3-4b. 如果 UE-to-UE relay 和 UE1 之间不存在每跳链路, 则执行 UE-to-UE relay 和 UE1 之间的每跳链路建立过程。UE1 将自己的 L2 ID 作为源地址, 中继的 L2 ID 作为目的地址。

S3-5a. 当 UE-2 和 UE-to-UE relay 成功建立了每跳链路 (per hop link), 将进一步触发 UE2 和 UE1 间端到端安全的建立。UE2 首先使用 PGK 生成传输密钥 PTK, 并进一步生成 PEK 和 PIK, 解密收到的直接通信请求, 并验证直接通信请求的完整性。验证成功后, UE2 产生一对临时公私钥, 即第二临时公钥 (Ephemeral public key2) 和第二临时私钥 (Ephemeral private key2), 并使用第二临时私钥、第一临时公钥和 UE-to-UE relay 的相关信息, 计算出与 UE-1 的共享密钥 K_D 和 MSB of K_D ID。若直接通信请求中包含安全策略与安全算法, 那么 UE2 协商出安全策略与安全算法, 然后生成第二随机数 (Nonce_2), 并根据利用 K_D 计算 K_{D-sess} 和 K_{D-sess} 衍生的下级密钥 (即第二加密密钥 (K_{D-enc}) 和第二完整性保护密钥 (K_{D-int})), 另外 UE2 生成 MSB of K_{D-sess} ID。

具体的, UE2 通过 UE-to-UE relay 向 UE1 发送安全模式命令, 该安全模式命令通过 PEK 进行加密, 该安全模式命令通过 PIK 进行完整性保护, 该安全模式命令中包含以下参数:

UE2 选取的安全算法 (chosen_algs) ;

UE2 选取的安全策略 (chosen_security policy) ;

UE2 生成的第二临时公钥 (Ephemeral private key2) ;

UE2 生成的该第二随机数 (Nonce_2) ;

UE2 生成的 MSB of K_D ID;

UE2 生成的 MSB of K_{D-sess} ID;

UE-to-UE relay 的相关信息 (可选) ;

第一消息验证码, 其中, 该第一消息验证码基于 K_{D-sess} 衍生的下级完整性保护密钥 (即第二完整性保护密钥 (K_{D-int})) 生成, 且该第一消息验证码的输入参数包括以下至少之一: UE2 选取的安全算法, UE2 选取的安全策略, 第二临时公钥, 第二随机数, MSB of K_D ID, MSB of K_{D-sess} ID。

S3-5b. 在收到安全模式命令后, UE-to-UE relay 可使用 PEK 解密安全模式命令获得与 QoS 和计费相关的信息。进一步地, UE-to-UE relay 将安全模式命令发送给 UE1。可选地, 若安全模式命令中不包括 UE-to-UE relay 的相关信息, UE-to-UE relay 可以在转发给 UE1 的安全模式命令中加入 UE-to-UE relay 的相关信息。

S3-6. UE1 首先使用 PEK 解密安全模式命令, 使用 PIK 判断安全模式命令的完整性, 验证成功后, 进一步判断 UE1 的安全能力信息和 UE1 的安全策略信息是否遭受篡改, 若未篡改, 那么采用与 UE2 相同的方式计算 K_{D-sess} 以及 K_{D-sess} 衍生的下级密钥 (即第二加密密钥 (K_{D-enc}) 和第二完整性保护密钥 (K_{D-int})), 然后 UE1 验证第一消息验证码是否有效, 若有效, UE1 准备以新安全环境来保护后续通信。UE1 生成 LSB of K_D ID、LSB of K_{D-sess} ID, 并将 LSB of K_D ID 与收到的 MSB of K_D ID 合并得到 K_D ID, 以及将 LSB of K_{D-sess} ID 与收到的 MSB of K_{D-sess} ID 合并得到 K_{D-sess} ID, 并保存 K_D ID 和 K_{D-sess} ID, 后续用于标识 K_D 和 K_{D-sess} 。UE1 根据协商策略与协商算法, 通过 UE-to-UE relay 向 UE2 发送一个受安全性保护的安全模式完成消息, 该安全模式完成消息可使用 K_{D-sess} 进行完整性和加密保护, 或者, 该安全模式完成消息可使用 K_{D-sess} 生成的下级完整性保护密钥 (即第二完整性保护密钥 (K_{D-int})) 进行完整性保护, K_{D-sess} 生成的下级加密密钥 (即第二加密密钥 (K_{D-enc})) 进

行加密保护。其中,该安全模式完成消息可以包括 LSB of K_D -sess ID。UE2 可以将收到的 LSB of K_D -sess ID 与 UE2 生成的 MSB of K_D -sess ID 合并得到 K_D -sess ID,并保存 K_D -sess ID,后续用于标识 K_D -sess。

具体的,UE1 根据 UE2 选取的安全算法、 K_D -SESS、基于 K_D -SESS 生成完整性保护密钥和/或机密性保护密钥、UE2 选取的安全策略,与 UE2 进行通信。UE2 根据 UE2 选取的安全算法、 K_D -SESS、基于 K_D -SESS 生成完整性保护密钥和/或机密性保护密钥、UE2 选取的安全策略,与 UE1 进行通信。

实施例 4,如图 20 所示,假设所有设备之间在此之前没有建立任何安全连接,可以通过 S4-0 至 S4-6 中的部分或全部步骤建立 L2 架构下的 UE-to-UE 中继场景下基于签名的安全通信连接。具体的,UE1 可以是第一终端设备,UE2 可以是第二终端设备,UE-to-UE relay 可以是中继设备, K_D 可以是第一密钥, K_D -SESS 可以是第二密钥,第一加密密钥为 PEK,第一完整性保护密钥为 PIK。

S4-0. UE 向网络注册,并被授权 UE-to-UE relay 服务。UE-to-UE relay 向网络注册可提供 UE-to-UE Relay 功能,UE-to-UE relay 配置了中继策略参数。PKMF 使用 MIKEY 机制,向上述已注册并得到授权的 UE 发送相关的 PGK、PGK ID 和到期时间。

S4-1. UE2 确定 PC5 单播链路建立时信令接收的目的 L2 ID。

S4-2. UE1 通过广播方式发送端到端的直接通信请求消息,具体的,UE1 在将直接通信请求广播给周围的终端设备之前,先需要根据 PGK 衍生出传输密钥 PTK,并进一步生成 PTK 的下级密钥,即 PEK 和 PIK。UE1 使用 PEK 加密广播消息,使用 PIK 计算直接通信请求消息的 MAC 即保护直接通信请求消息的完整性,也即,该直接通信请求通过 PEK 进行加密,以及该直接通信请求通过 PIK 进行完整性保护。其中,直接通信请求中包含以下至少之一:

UE1 的安全能力信息 (UE1 security capabilities);

UE1 的安全策略信息 (UE1 security policy);

UE1 生成的第一临时公钥 (Ephemeral public key1);

UE1 生成的第一随机数 (Nonce-1)。

S4-3. UE-to-UE Relay 接收广播的直接通信请求消息,并验证 UE-to-UE Relay 是否配置为转发直接通信请求消息,例如,UE-to-UE Relay 将宣布的 ProSe 应用 ID 与它所提供的中继策略/参数进行比较。UE-to-UE Relay 转发端到端广播的直接通信请求消息时,使用自己的 L2 ID 作为源 (Source) L2 ID,并在消息中添加 UE-to-UE Relay 的 UE ID,在适配层指定标识 UE1 的信息。UE-to-UE Relay 在 ProSe 层处理此端到端广播消息,并根据适配层信息转发任何后续的中继 PC5-S 消息。

具体的,在验证通过之后 UE-to-UE Relay 使用 PEK 解密直接通信请求以获取 QoS 和计费信息,以及 UE-to-UE Relay 使用 PIK 验证直接通信请求的完整性,在验证通过之后 UE-to-UE Relay 在直接通信请求中添加 UE-to-UE Relay 的相关信息和 UE-to-UE Relay 的标识,并且 UE-to-UE Relay 使用 PEK 加密直接通信请求,使用 PIK 保护直接通信请求的完整性;其中,UE-to-UE Relay 的相关信息包括以下之一:UE-to-UE Relay 的身份信息,UE-to-UE Relay 生成的随机数,UE-to-UE Relay 生成的计数器。

S4-4a. UE2 对宣布的应用程序感兴趣,如果 UE2 和 UE-to-UE Relay 之间不存在每跳链路,UE2 会触发 UE-to-UE Relay 建立每跳链路。UE2 发送每跳链路建立过程消息,源地址是 UE2 L2 ID,目的地址是中继的 L2 ID。

S4-4b. 如果 UE-to-UE relay 和 UE1 之间不存在每跳链路,则执行 UE-to-UE relay 和 UE1 之间的每跳链路建立过程。UE1 将自己的 L2 ID 作为源地址,中继的 L2 ID 作为目的地址。

S4-5a. 当 UE-2 和 UE-to-UE relay 成功建立了每跳链路 (per hop link),将进一步触发 UE2 和 UE1 间端到端安全的建立。UE2 首先使用 PGK 生成传输密钥 PTK,并进一步生成 PEK 和 PIK,解密收到的直接通信请求,并验证直接通信请求的完整性。验证成功后,UE2 产生一对临时公私钥,即第二临时公钥 (Ephemeral public key2) 和第二临时私钥 (Ephemeral private key2),并使用第二临时私钥、第一临时公钥和 UE-to-UE relay 的相关信息,计算出与 UE1 的共享密钥 K_D 和 MSB of K_D ID。若直接通信请求中包含安全策略与安全算法,那么 UE2 协商出安全策略与安全算法,然后生成第二随机数 (Nonce_2),并根据利用 K_D 衍生的下级密钥 (即第二加密密钥 (K_{D-enc}) 和第二完整性保护密钥 (K_{D-int}))。

具体的,UE2 通过 UE-to-UE relay 向 UE1 发送安全模式命令,该安全模式命令通过 PEK 进行加密,该安全模式命令通过 PIK 进行完整性保护,该安全模式命令中包含以下参数:

UE2 选取的安全算法 (chosen_algs);

UE2 选取的安全策略 (chosen_security policy);

UE2 生成的第二临时公钥 (Ephemeral private key2);

UE2 生成的该第二随机数 (Nonce_2);

UE2 生成的 MSB of K_D ID;

UE-to-UE relay 的相关信息 (可选);

第一消息验证码, 其中, 该第一消息验证码基于第二完整性保护密钥 (K_{D-int}) 生成, 且该第一消息验证码的输入参数包括以下至少之一: UE2 选取的安全算法, UE2 选取的安全策略, 第二临时公钥, 第二随机数, MSB of K_D ID。

5 S4-5b. 在收到安全模式命令后, UE-to-UE relay 可使用 PEK 解密安全模式命令获得与 QoS 和计费相关的信息。进一步地, UE-to-UE relay 将安全模式命令发送给 UE1。可选地, 若安全模式命令中不包括 UE-to-UE relay 的相关信息, UE-to-UE relay 可以在转发给 UE1 的安全模式命令中加入 UE-to-UE relay 的相关信息。

10 S4-6. UE1 首先使用 PEK 解密安全模式命令, 使用 PIK 判断安全模式命令的完整性, 验证成功后, 进一步判断 UE1 的安全能力信息和 UE1 的安全策略信息是否遭受篡改, 若未篡改, 那么采用与 UE2 相同的方式计算第二加密密钥 (K_{D-enc}) 和第二完整性保护密钥 (K_{D-int}), 然后 UE1 验证第一消息验证码是否有效, 若有效, UE1 准备以新安全环境来保护后续通信。UE1 生成 LSB of K_D ID, 并将 LSB of K_D ID 与收到的 MSB of K_D ID 合并得到 K_D ID, 并保存 K_D ID, 后续用于标识 K_D 。UE1 根据协商策略与协商算法, 通过 UE-to-UE relay 向 UE2 发送一个受安全性保护的安全模式完成消息, 该安全模式完成消息可使用衍生的下级完整性保护密钥 (即第二完整性保护密钥 (K_{D-int})) 进行完整性保护, 衍生的下级加密密钥 (即第二加密密钥 (K_{D-enc})) 进行加密保护。

15 具体的, UE1 根据 UE2 选取的安全算法、第二完整性保护密钥 (K_{D-int}) 和/或第二加密密钥 (K_{D-enc})、UE2 选取的安全策略, 与 UE2 进行通信。UE2 根据 UE2 选取的安全算法、第二完整性保护密钥 (K_{D-int}) 和/或第二加密密钥 (K_{D-enc})、UE2 选取的安全策略, 与 UE1 进行通信。

20 实施例 5, 如图 21 所示, 假设所有设备之间在此之前没有建立任何安全连接, 可以通过 S5-0 至 S5-6 中的部分或全部步骤建立 L2 架构下的 UE-to-UE 中继场景下基于签名的安全通信连接。具体的, UE1 可以是第一终端设备, UE2 可以是第二终端设备, UE-to-UE relay 可以是中继设备, K_D 可以是第一密钥, K_{D-SESS} 可以是第二密钥。

25 S5-0. UE 向网络注册, 并被授权 UE-to-UE relay 服务。UE-to-UE relay 向网络注册可提供 UE-to-UE Relay 功能, UE-to-UE relay 配置了中继策略参数。PKMF 使用 MIKEY 机制, 向上述已注册并得到授权的 UE 发送相关的对称密钥, 可以基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生第一加密密钥和第一完整性保护密钥。

S5-1. UE2 确定 PC5 单播链路建立时信令接收的目的 L2 ID。

30 S5-2. UE1 通过广播方式发送端到端的直接通信请求消息, 具体的, UE1 在将直接通信请求广播给周围的终端设备之前, 基于已注册并被授权使用 UE-to-UE relay 通信的终端 (即 UE1 和 UE2) 的对称密钥衍生第一加密密钥和第一完整性保护密钥。UE1 使用第一加密密钥加密广播消息, 使用第一完整性保护密钥计算直接通信请求消息的 MAC 即保护直接通信请求消息的完整性, 也即, 该直接通信请求通过第一加密密钥进行加密, 以及该直接通信请求通过第一完整性保护密钥进行完整性保护。其中, 直接通信请求中包含以下至少之一:

- 35 UE1 的安全能力信息 (UE1 security capabilities);
- UE1 的安全策略信息 (UE1 security policy);
- UE1 生成的第一临时公钥 (Ephemeral public key1);
- UE1 生成的第一随机数 (Nonce-1)。

40 S5-3. UE-to-UE Relay 接收广播的直接通信请求消息, 并验证 UE-to-UE Relay 是否配置为转发直接通信请求消息, 例如, UE-to-UE Relay 将宣布的 ProSe 应用 ID 与它所提供的中继策略/参数进行比较。UE-to-UE Relay 转发端到端广播的直接通信请求消息时, 使用自己的 L2 ID 作为源 (Source) L2 ID, 并在消息中添加 UE-to-UE Relay 的 UE ID, 在适配层指定标识 UE1 的信息。UE-to-UE Relay 在 ProSe 层处理此端到端广播消息, 并根据适配层信息转发任何后续的中继 PC5-S 消息。

45 具体的, 在验证通过之后 UE-to-UE Relay 使用第一加密密钥解密直接通信请求以获取 QoS 和计费信息, 以及 UE-to-UE Relay 使用第一完整性保护密钥验证直接通信请求的完整性, 在验证通过之后 UE-to-UE Relay 在直接通信请求中添加 UE-to-UE Relay 的相关信息和 UE-to-UE Relay 的标识, 并且 UE-to-UE Relay 使用第一加密密钥加密直接通信请求, 使用第一完整性保护密钥保护直接通信请求的完整性; 其中, UE-to-UE Relay 的相关信息包括以下之一: UE-to-UE Relay 的身份信息, UE-to-UE Relay 生成的随机数, UE-to-UE Relay 生成的计数器。

50 S5-4a. UE2 对宣布的应用程序感兴趣, 如果 UE2 和 UE-to-UE Relay 之间不存在每跳链路, UE2 会触发 UE-to-UE Relay 建立每跳链路。UE2 发送每跳链路建立过程消息, 源地址是 UE2 L2 ID, 目的地址是中继的 L2 ID。

S5-4b. 如果 UE-to-UE relay 和 UE1 之间不存在每跳链路, 则执行 UE-to-UE relay 和 UE1 之间的每跳链路建立过程。UE1 将自己的 L2 ID 作为源地址, 中继的 L2 ID 作为目的地址。

S5-5a. 当 UE-2 和 UE-to-UE relay 成功建立了每跳链路 (per hop link), 将进一步触发 UE2 和 UE1 间端到端安全的建立。UE2 可以基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生第一加密密钥和第一完整性保护密钥, 解密收到的直接通信请求, 并验证直接通信请求的完整性。验证成功后, UE2 产生一对临时公私钥, 即第二临时公钥 (Ephemeral public key2) 和第二临时私钥 (Ephemeral private key2), 并使用第二临时私钥、第一临时公钥和 UE-to-UE relay 的相关信息, 计算出与 UE-1 的共享密钥 K_D 和 MSB of K_D ID。若直接通信请求中包含安全策略与安全算法, 那么 UE2 协商出安全策略与安全算法, 然后生成第二随机数 (Nonce_2), 并根据利用 K_D 计算 K_D -sess 和 K_D -sess 衍生的下级密钥 (即第二加密密钥 (K_{D-enc}) 和第二完整性保护密钥 (K_{D-int})), 另外 UE2 生成 MSB of K_D -sess ID。

具体的, UE2 通过 UE-to-UE relay 向 UE1 发送安全模式命令, 该安全模式命令通过第一加密密钥进行加密, 该安全模式命令通过第一完整性保护密钥进行完整性保护, 该安全模式命令中包含以下参数:

- UE2 选取的安全算法 (chosen_algs);
- UE2 选取的安全策略 (chosen_security policy);
- UE2 生成的第二临时公钥 (Ephemeral private key2);
- UE2 生成的该第二随机数 (Nonce_2);
- UE2 生成的 MSB of K_D ID;
- UE2 生成的 MSB of K_D -sess ID;
- UE-to-UE relay 的相关信息 (可选);

第一消息验证码, 其中, 该第一消息验证码基于 K_D -sess 衍生的下级完整性保护密钥 (即第二完整性保护密钥 (K_{D-int})) 生成, 且该第一消息验证码的输入参数包括以下至少之一: UE2 选取的安全算法, UE2 选取的安全策略, 第二临时公钥, 第二随机数, MSB of K_D ID, MSB of K_D -sess ID。

S5-5b. 在收到安全模式命令后, UE-to-UE relay 可使用第一加密密钥解密安全模式命令获得与 QoS 和计费相关的信息。进一步地, UE-to-UE relay 将安全模式命令发送给 UE1。可选地, 若安全模式命令中不包括 UE-to-UE relay 的相关信息, UE-to-UE relay 可以在转发给 UE1 的安全模式命令中加入 UE-to-UE relay 的相关信息。

S5-6. UE1 首先使用第一加密密钥解密安全模式命令, 使用第一完整性保护密钥判断安全模式命令的完整性, 验证成功后, 进一步判断 UE1 的安全能力信息和 UE1 的安全策略信息是否遭受篡改, 若未篡改, 那么采用与 UE2 相同的方式计算 K_D -sess 以及 K_D -sess 衍生的下级密钥 (即第二加密密钥 (K_{D-enc}) 和第二完整性保护密钥 (K_{D-int})), 然后 UE1 验证第一消息验证码是否有效, 若有效, UE1 准备以新安全环境来保护后续通信。UE1 生成 LSB of K_D ID、LSB of K_D -sess ID, 并将 LSB of K_D ID 与收到的 MSB of K_D ID 合并得到 K_D ID, 以及将 LSB of K_D -sess ID 与收到的 MSB of K_D -sess ID 合并得到 K_D -sess ID, 并保存 K_D ID 和 K_D -sess ID, 后续用于标识 K_D 和 K_D -sess。UE1 根据协商策略与协商算法, 通过 UE-to-UE relay 向 UE2 发送一个受安全性保护的安全模式完成消息, 该安全模式完成消息可使用 K_D -sess 进行完整性和加密保护, 或者, 该安全模式完成消息可使用 K_D -sess 生成的下级完整性保护密钥 (即第二完整性保护密钥 (K_{D-int})) 进行完整性保护, K_D -sess 生成的下级加密密钥 (即第二加密密钥 (K_{D-enc})) 进行加密保护。其中, 该安全模式完成消息可以包括 LSB of K_D -sess ID。UE2 可以将收到的 LSB of K_D -sess ID 与 UE2 生成的 MSB of K_D -sess ID 合并得到 K_D -sess ID, 并保存 K_D -sess ID, 后续用于标识 K_D -sess。

具体的, UE1 根据 UE2 选取的安全算法、 K_D -sess、基于 K_D -sess 生成完整性保护密钥和/或机密性保护密钥、UE2 选取的安全策略, 与 UE2 进行通信。UE2 根据 UE2 选取的安全算法、 K_D -sess、基于 K_D -sess 生成完整性保护密钥和/或机密性保护密钥、UE2 选取的安全策略, 与 UE1 进行通信。

实施例 6, 如图 22 所示, 假设所有设备之间在此之前没有建立任何安全连接, 可以通过 S6-0 至 S6-6 中的部分或全部步骤建立 L2 架构下的 UE-to-UE 中继场景下基于签名的安全通信连接。具体的, UE1 可以是第一终端设备, UE2 可以是第二终端设备, UE-to-UE relay 可以是中继设备, K_D 可以是第一密钥, K_D -sess 可以是第二密钥。

S6-0. UE 向网络注册, 并被授权使用 UE-to-UE relay 服务。UE-to-UE relay 向网络注册可提供 UE-to-UE Relay 功能, UE-to-UE relay 配置了中继策略参数。PKMF 使用 MIKEY 机制, 向上述已注册并得到授权的 UE 发送相关的对称密钥, 可以基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生第一加密密钥和第一完整性保护密钥。

S6-1. UE2 确定 PC5 单播链路建立时信令接收的目的 L2 ID。

S6-2. UE1 通过广播方式发送端到端的直接通信请求消息，具体的，UE1 在将直接通信请求广播给周围的终端设备之前，基于已注册并被授权使用 UE-to-UE relay 通信的终端（即 UE1 和 UE2）的对称密钥衍生第一加密密钥和第一完整性保护密钥。UE1 使用第一加密密钥加密广播消息，使用第一完整性保护密钥计算直接通信请求消息的 MAC 即保护直接通信请求消息的完整性，也即，该直接通信请求通过第一加密密钥进行加密，以及该直接通信请求通过第一完整性保护密钥进行完整性保护。其中，直接通信请求中包含以下至少之一：

UE1 的安全能力信息（UE1 security capabilities）；

UE1 的安全策略信息（UE1 security policy）；

UE1 生成的第一临时公钥（Ephemeral public key1）；

UE1 生成的第一随机数（Nonce-1）。

S6-3. UE-to-UE Relay 接收广播的直接通信请求消息，并验证 UE-to-UE Relay 是否配置为转发直接通信请求消息，例如，UE-to-UE Relay 将宣布的 ProSe 应用 ID 与它所提供的中继策略/参数进行比较。UE-to-UE Relay 转发端到端广播的直接通信请求消息时，使用自己的 L2 ID 作为源（Source）L2 ID，并在消息中添加 UE-to-UE Relay 的 UE ID，在适配层指定标识 UE1 的信息。UE-to-UE Relay 在 ProSe 层处理此端到端广播消息，并根据适配层信息转发任何后续的中继到端 PC5-S 消息。

具体的，在验证通过之后 UE-to-UE Relay 使用第一加密密钥解密直接通信请求以获取 QoS 和计费信息，以及 UE-to-UE Relay 使用第一完整性保护密钥验证直接通信请求的完整性，在验证通过之后 UE-to-UE Relay 在直接通信请求中添加 UE-to-UE Relay 的相关信息和 UE-to-UE Relay 的标识，并且 UE-to-UE Relay 使用第一加密密钥加密直接通信请求，使用第一完整性保护密钥保护直接通信请求的完整性；其中，UE-to-UE Relay 的相关信息包括以下之一：UE-to-UE Relay 的身份信息，UE-to-UE Relay 生成的随机数，UE-to-UE Relay 生成的计数器。

S6-4a. UE2 对宣布的应用程序感兴趣，如果 UE2 和 UE-to-UE Relay 之间不存在每跳链路，UE2 会触发 UE-to-UE Relay 建立每跳链路。UE2 发送每跳链路建立过程消息，源地址是 UE2 L2 ID，目的地址是中继的 L2 ID。

S6-4b. 如果 UE-to-UE relay 和 UE1 之间不存在每跳链路，则执行 UE-to-UE relay 和 UE1 之间的每跳链路建立过程。UE1 将自己的 L2 ID 作为源地址，中继的 L2 ID 作为目的地址。

S6-5a. 当 UE-2 和 UE-to-UE relay 成功建立了每跳链路（per hop link），将进一步触发 UE2 和 UE1 间端到端安全的建立。UE2 可以基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生第一加密密钥和第一完整性保护密钥，解密收到的直接通信请求，并验证直接通信请求的完整性。验证成功后，UE2 产生一对临时公私钥，即第二临时公钥（Ephemeral public key2）和第二临时私钥（Ephemeral private key2），并使用第二临时私钥、第一临时公钥和 UE-to-UE relay 的相关信息，计算出与 UE1 的共享密钥 K_D 和 MSB of K_D ID。若直接通信请求中包含安全策略与安全算法，那么 UE2 协商出安全策略与安全算法，然后生成第二随机数（Nonce_2），并根据利用 K_D 衍生的下级密钥（即第二加密密钥（ K_{D-enc} ）和第二完整性保护密钥（ K_{D-int} ））。

具体的，UE2 通过 UE-to-UE relay 向 UE1 发送安全模式命令，该安全模式命令通过第一加密密钥进行加密，该安全模式命令通过第一完整性保护密钥进行完整性保护，该安全模式命令中包含以下参数：

UE2 选取的安全算法（chosen_algs）；

UE2 选取的安全策略（chosen_security policy）；

UE2 生成的第二临时公钥（Ephemeral private key2）；

UE2 生成的该第二随机数（Nonce_2）；

UE2 生成的 MSB of K_D ID；

UE-to-UE relay 的相关信息（可选）；

第一消息验证码，其中，该第一消息验证码基于第二完整性保护密钥（ K_{D-int} ）生成，且该第一消息验证码的输入参数包括以下至少之一：UE2 选取的安全算法，UE2 选取的安全策略，第二临时公钥，第二随机数，MSB of K_D ID。

S6-5b. 在收到安全模式命令后，UE-to-UE relay 可使用第一加密密钥解密安全模式命令获得与 QoS 和计费相关的信息。进一步地，UE-to-UE relay 将安全模式命令发送给 UE1。可选地，若安全模式命令中不包括 UE-to-UE relay 的相关信息，UE-to-UE relay 可以在转发给 UE1 的安全模式命令中加入 UE-to-UE relay 的相关信息。

S6-6. UE1 首先使用第一加密密钥解密安全模式命令，使用第一完整性保护密钥判断安全模式命

令的完整性,验证成功后,进一步判断 UE1 的安全能力信息和 UE1 的安全策略信息是否遭受篡改,若未篡改,那么采用与 UE2 相同的方式计算第二加密密钥 (K_{D-enc}) 和第二完整性保护密钥 (K_{D-int}),然后 UE1 验证第一消息验证码是否有效,若有效,UE1 准备以新安全环境来保护后续通信。UE1 生成 LSB of K_D ID,并将 LSB of K_D ID 与收到的 MSB of K_D ID 合并得到 K_D ID,并保存 K_D ID,后续用于标识 K_D 。UE1 根据协商策略与协商算法,通过 UE-to-UE relay 向 UE2 发送一个受安全性保护的安全模式完成消息,该安全模式完成消息可使用衍生的下级完整性保护密钥(即第二完整性保护密钥 (K_{D-int}))进行完整性保护,衍生的下级加密密钥(即第二加密密钥 (K_{D-enc}))进行加密保护。

具体的,UE1 根据 UE2 选取的安全算法、第二完整性保护密钥(K_{D-int})和/或第二加密密钥(K_{D-enc})、UE2 选取的安全策略,与 UE2 进行通信。UE2 根据 UE2 选取的安全算法、第二完整性保护密钥(K_{D-int})和/或第二加密密钥 (K_{D-enc})、UE2 选取的安全策略,与 UE1 进行通信。

上文结合图 7 至图 22,详细描述了本申请的方法实施例,下文结合图 23 至图 31,详细描述本申请的装置实施例,应理解,装置实施例与方法实施例相互对应,类似的描述可以参照方法实施例。

图 23 示出了根据本申请实施例的终端设备 1100 的示意性框图。该终端设备 1100 为第一终端设备,如图 23 所示,该终端设备 1100 包括:

通信单元 1110,用于接收第二终端设备通过中继设备发送的认证请求消息;

其中,该认证请求消息包括以下至少之一:该第二终端设备所属用户的信息,该中继设备所属用户的信息,该第二终端设备生成的第一临时公钥,该第二终端设备的签名,该中继设备的签名,该中继设备的相关信息;

其中,该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK;该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK;该第二终端设备的签名的输入参数包括以下至少之一:该第二终端设备所属用户的信息和该第一临时公钥;该中继设备的签名的输入参数包括以下至少之一:该第二终端设备的签名和该中继设备所属用户的信息;该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥;该中继设备的相关信息包括以下之一:该中继设备的身份信息,该中继设备生成的随机数,该中继设备生成的计数器。

在一些实施例中,该第二终端设备的签名由该第二终端设备的秘密签名密钥生成,和/或,该中继设备的签名由该中继设备的秘密签名密钥生成。

在一些实施例中,该终端设备 1100 还包括:处理单元 1120;

在该第二终端设备的 KPAK 和该中继设备的 KPAK 有效,且基于该第二终端设备的标识和该第二终端设备的 PVT 对该第二终端设备的签名验证成功,以及基于该中继设备的标识和该中继设备的 PVT 对该中继设备的签名验证成功的情况下,该处理单元 1120 用于生成第二临时私钥,以及该处理单元 1120 用于根据该第一临时公钥、该中继设备的相关信息和该第二临时私钥派生该第一密钥。

在一些实施例中,该通信单元 1110 还用于通过该中继设备向该第二终端设备发送第一消息;

其中,该第一消息包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该第一终端设备生成的第一随机数,该第一终端设备生成的与该第二临时私钥配对的第二临时公钥,该第一终端设备生成的该第一密钥的标识的 M 个比特位,该第一终端设备的签名,第一消息验证码;

其中,该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK;该第一终端设备的签名的输入参数包括以下至少之一:该第一终端设备所属用户的信息,该第二临时公钥,该 M 个比特位,该第二终端设备的签名;

其中,该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护,且该第一消息验证码的输入参数包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该第一随机数,该第二临时公钥,该 M 个比特位,该第一终端设备的签名;

其中,该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥,该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥,该第二密钥用于派生完整性保护密钥和/或机密性保护密钥,该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数。

在一些实施例中,该通信单元 1110 还用于接收该第二终端设备通过该中继设备发送的第二消息;

其中,该第二消息包括以下至少之一:该第二终端设备生成的该第二随机数,该第二终端设备生成的该第一密钥的标识的 N 个比特位,该第二终端设备生成的该第二密钥的标识的 x 个比特位,该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,第二消息验证码;

其中,该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护,或者,该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护,且该第二消息验证码的输入参数包括以下至少之一:该第二随机数,该N个比特位,该x个比特位,该第二终端设备选取的安全算法,该第二终端设备选取的安全策略;其中,该第二密钥的标识由该x个比特位与
5 该第二密钥的标识的另外y个比特位合并得到,x和y均为正整数。

在一些实施例中,该第二消息通过该第一密钥进行加密。

在一些实施例中,在该第二消息中携带的信息未遭受篡改的情况下,该处理单元1120还用于至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥,该处理单元1120还用于根据该第二密钥生成完整性保护密钥和/或机密性保护密钥,以及该处理单元1120还用于将该M个比特位和
10 该N个比特位合并得到该第一密钥的标识,该处理单元1120还用于生成该第二密钥的标识的y个比特位,并将该x个比特位和该y个比特位合并得到该第二密钥的标识;

在该第二消息验证码有效的情况下,该处理单元1120还用于根据该第二终端设备选取的安全算法、该第二密钥、基于该第二密钥生成完整性保护密钥和/或机密性保护密钥、该第二终端设备选取的安全策略,与该第二终端设备进行通信。

在一些实施例中,该处理单元1120还用于根据该第一密钥解密该第二消息;

在该第二消息中携带的信息未遭受篡改的情况下,该处理单元1120还用于至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥,该处理单元1120还用于根据该第二密钥生成完整性保护密钥和/或机密性保护密钥,以及该处理单元1120还用于将该M个比特位和该N个比特位合并得到该第一密钥的标识,该处理单元1120还用于生成该第二密钥的标识的y个比特位,并将该x
20 个比特位和该y个比特位合并得到该第二密钥的标识;

在该第二消息验证码有效的情况下,该处理单元1120还用于根据该第二终端设备选取的安全算法、该第二密钥、基于该第二密钥生成完整性保护密钥和/或机密性保护密钥、该第二终端设备选取的安全策略,与该第二终端设备进行通信。

在一些实施例中,该完整性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,该机密性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

在一些实施例中,该第一消息为认证响应消息,该第二消息为安全模式命令消息。

在一些实施例中,该第一消息为安全模式命令消息,该第二消息为安全模式响应消息。

在一些实施例中,该通信单元1110还用于通过该中继设备向该第二终端设备发送第三消息;

其中,该第三消息用于指示安全模式建立完成,该第三消息通过目标密钥进行加密,且该第三消息包括以下至少之一:该第二密钥的标识的该y个比特位,第三消息验证码;

其中,该目标密钥包括以下之一:该第一密钥,该第二密钥,该第二密钥派生的机密性保护密钥;

其中,该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护,或者,该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护,该第三消息验证码的输入参数包括该y个比特位。
35

在一些实施例中,该通信单元1110还用于接收该第二终端设备通过该中继设备发送的错误消息;其中,该错误消息包括以下至少之一:原因信息,第四消息验证码;其中,该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突,或者,该原因信息用于指示该第一消息验证码验证失败,或者,该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败;该第四消息验证码的输入参数包括以下至少之一:该原因信息;
40

在该第四消息验证码有效的情况下,该处理单元1120还用于确定安全模式建立失败,和/或,该处理单元1120还用于重新发起安全模式建立流程。

在一些实施例中,该完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥;和/或,该机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

在一些实施例中,上述通信单元可以是通信接口或收发器,或者是通信芯片或者片上系统的输入输出接口。上述处理单元可以是一个或多个处理器。

应理解,根据本申请实施例的终端设备1100可对应于本申请方法实施例中的第一终端设备,并且终端设备1100中的各个单元的上述和其它操作和/或功能分别为了实现图7所示方法200中第一终端设备的相应流程,为了简洁,在此不再赘述。
50

图24示出了根据本申请实施例的终端设备1200的示意性框图。该终端设备1200为第二终端设备,如图24所示,该终端设备1200包括:

通信单元 1210, 用于通过中继设备向第一终端设备发送认证请求消息;

其中, 该认证请求消息包括以下至少之一: 该第二终端设备所属用户的信息, 该第二终端设备生成的第一临时公钥, 该第二终端设备的签名, 该中继设备的相关信息;

其中, 该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的公共验证令牌 PVT 和密钥管理服务服务器的公共认证密钥 KPAK; 该第二终端设备的签名的输入参数包括以下至少之一: 该第二终端设备所属用户的信息和该第一临时公钥; 该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥; 该中继设备的相关信息包括以下之一: 该中继设备的身份信息, 该中继设备生成的随机数, 该中继设备生成的计数器。

在一些实施例中, 该第二终端设备的签名由该第二终端设备的秘密签名密钥生成。

在一些实施例中, 该通信单元 1210 还用于接收该第一终端设备通过该中继设备发送的第一消息;

其中, 该第一消息包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该中继设备所属用户的信息, 该第一终端设备生成的第一随机数, 该第一终端设备生成的与该第二临时私钥配对的第二临时公钥, 该第一终端设备生成的该第一密钥的标识的 M 个比特位, 该第一终端设备的签名, 该中继设备的签名, 第一消息验证码;

其中, 该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK; 该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK; 该第一终端设备的签名的输入参数包括以下至少之一: 该第一终端设备所属用户的信息, 该第二临时公钥, 该 M 个比特位, 该第二终端设备的签名; 该中继设备的签名的输入参数包括以下至少之一: 该中继设备所属用户的信息, 该第一终端设备的签名, 该第二终端设备的签名, 该第一消息;

其中, 该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护, 且该第一消息验证码的输入参数包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该第一随机数, 该第二临时公钥, 该 M 个比特位, 该第一终端设备的签名;

其中, 该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥, 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥, 该第二密钥用于派生完整性保护密钥和/或机密性保护密钥, 该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数。

在一些实施例中, 该第一终端设备的签名由该第一终端设备的秘密签名密钥生成, 和/或, 该中继设备的签名由该中继设备的秘密签名密钥生成。

在一些实施例中, 该终端设备 1200 还包括: 处理单元 1220;

该处理单元 1220 用于分别检查该第一终端设备的 KPAK 和该中继设备的 KPAK, 在该第一终端设备的 KPAK 和该中继设备的 KPAK 有效的情况下, 且该处理单元 1220 用于基于该第一终端设备的标识和该第一终端设备的 PVT 对该第一终端设备的签名进行验证, 以及该处理单元 1220 用于基于该中继设备的标识和该中继设备的 PVT 对该中继设备的签名进行验证;

在该第一终端设备的签名和该中继设备的签名验证成功, 且该第一消息中携带的信息未遭受篡改的情况下, 该处理单元 1220 用于生成第二随机数, 该处理单元 1220 用于至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥, 该处理单元 1220 用于根据该第二密钥生成完整性保护密钥和/或机密性保护密钥, 以及该处理单元 1220 用于生成该第一密钥的标识的 N 个比特位, 并将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识;

在该第一消息验证码有效的情况下, 该通信单元 1210 还用于通过该中继设备向该第一终端设备发送第二消息; 其中, 该第二消息包括以下至少之一: 该第二随机数, 该 N 个比特位, 该第二终端设备生成的该第二密钥的标识的 x 个比特位, 该第二终端设备选取的安全算法, 该第二终端设备选取的安全策略, 第二消息验证码;

其中, 该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护, 或者, 该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护, 且该第二消息验证码的输入参数包括以下至少之一: 该第二随机数, 该 N 个比特位, 该 x 个比特位, 该第二终端设备选取的安全算法, 该第二终端设备选取的安全策略; 其中, 该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

在一些实施例中, 该第二消息通过该第一密钥进行加密。

在一些实施例中, 该第一消息为认证响应消息, 该第二消息为安全模式命令消息。

在一些实施例中, 该第一消息为安全模式命令消息, 该第二消息为安全模式响应消息。

在一些实施例中, 该完整性保护密钥的输入参数包括以下至少之一: 该第二密钥, 选定的算法类

型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,该机密性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

在一些实施例中,该通信单元 1210 还用于接收该第一终端设备通过该中继设备发送的第三消息;

其中,该第三消息用于指示安全模式建立完成,该第三消息通过目标密钥进行加密,且该第三消息包括以下至少之一:该第一终端设备生成的该第二密钥的标识的 y 个比特位,第三消息验证码;

其中,该目标密钥包括以下之一:该第一密钥,该第二密钥,该第二密钥派生的机密性保护密钥;

其中,该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护,或者,该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护,该第三消息验证码的输入参数包括该 y 个比特位。

在一些实施例中,该处理单元 1220 用于通过该目标密钥对该第三消息进行解密;

在该第三消息中携带的信息未遭受篡改的情况下,且该第三消息验证码有效的情况下,该第二终端设备将该 x 个比特位与该 y 个比特位合并得到该第二密钥的标识。

在一些实施例中,该通信单元 1210 还用于通过该中继设备向该第一终端设备发送错误消息;其中,该错误消息包括以下至少之一:原因信息,第四消息验证码;其中,该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突,或者,该原因信息用于指示该第一消息验证码验证失败,或者,该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败;该第四消息验证码的输入参数包括以下至少之一:该原因信息。

在一些实施例中,该完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥;和/或,该机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

在一些实施例中,上述通信单元可以是通信接口或收发器,或者是通信芯片或者片上系统的输入输出接口。上述处理单元可以是一个或多个处理器。

应理解,根据本申请实施例的终端设备 1200 可对应于本申请方法实施例中的第二终端设备,并且终端设备 1200 中的各个单元的上述和其它操作和/或功能分别为了实现图 9 所示方法 300 中第二终端设备的相应流程,为了简洁,在此不再赘述。

图 25 示出了根据本申请实施例的终端设备 1300 的示意性框图。该终端设备 1300 为中继设备,如图 25 所示,该终端设备 1300 包括:

通信单元 1310,用于接收第二终端设备发送的认证请求消息;其中,该认证请求消息包括以下至少之一:该第二终端设备所属用户的信息,该第二终端设备生成的第一临时公钥,该第二终端设备的签名;其中,该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK;该第二终端设备的签名的输入参数包括以下至少之一:该第二终端设备所属用户的信息和该第一临时公钥;

在该第二终端设备的 KPAK 有效,且基于该第二终端设备的标识和该第二终端设备的 PVT 对该第二终端设备的签名验证成功的情况下,该通信单元 1310 还用于向该第一终端设备发送验证之后的认证请求消息;其中,该验证之后的认证请求消息包括以下至少之一:该第二终端设备所属用户的信息,该中继设备所属用户的信息,该第一临时公钥,该第二终端设备的签名,该中继设备的签名,该中继设备的相关信息;其中,该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK;该中继设备的签名的输入参数包括以下至少之一:该第二终端设备的签名和该中继设备所属用户的信息;其中,该第一临时公钥和该中继设备的相关信息用于第一终端设备派生第一密钥;该中继设备的相关信息包括以下之一:该中继设备的身份信息,该中继设备生成的随机数,该中继设备生成的计数器。

在一些实施例中,该第二终端设备的签名由该第二终端设备的秘密签名密钥生成,和/或,该中继设备的签名由该中继设备的秘密签名密钥生成。

在一些实施例中,该通信单元 1310 还用于接收该第一终端设备发送的第一消息;其中,该第一消息包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该第一终端设备生成的第一随机数,该第一终端设备生成的第二临时公钥,该第一终端设备生成的该第一密钥的标识的 M 个比特位,该第一终端设备的签名,第一消息验证码;其中,该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的 PVT 和 KPAK;该第一终端设备的签名的输入参数包括以下至少之一:该第一终端设备所属用户的信息,该第二临时公钥,该 M 个比特位,该第二终端设备的签名;其中,该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护,且该第一消息验证码的输入参数包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该第

一随机数, 该第二临时公钥, 该 M 个比特位, 该第一终端设备的签名;

在该第一终端设备的 KPAK 有效, 且基于该第一终端设备的标识和该第一终端设备的 PVT 对该第一终端设备的签名验证成功的情况下, 该通信单元 1310 还用于向该第二终端设备发送验证之后的第一消息; 其中, 该验证之后的第一消息包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该中继设备所属用户的信息, 该第一终端设备生成的第一随机数, 该第一终端设备生成的与该第二临时私钥配对的第二临时公钥, 该第一终端设备生成的该第一密钥的标识的 M 个比特位, 该第一终端设备的签名, 该中继设备的签名, 该第一消息验证码; 其中, 该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK; 该中继设备的签名的输入参数包括以下至少之一: 该中继设备所属用户的信息, 该第一终端设备的签名, 该第二终端设备的签名, 该验证之后的第一消息;

其中, 该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥, 该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥, 该第二密钥用于派生完整性保护密钥和/或机密性保护密钥, 该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数。

在一些实施例中, 该通信单元 1310 还用于将该第二终端设备发送的第二消息转发至该第一终端设备;

其中, 该第二消息包括以下至少之一: 该第二终端设备生成的该第二随机数, 该第二终端设备生成的该第一密钥的标识的 N 个比特位, 该第二终端设备生成的该第二密钥的标识的 x 个比特位, 该第二终端设备选取的安全算法, 该第二终端设备选取的安全策略, 第二消息验证码;

其中, 该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护, 或者, 该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护, 且该第二消息验证码的输入参数包括以下至少之一: 该第二随机数, 该 N 个比特位, 该 x 个比特位, 该第二终端设备选取的安全算法, 该第二终端设备选取的安全策略; 其中, 该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

在一些实施例中, 该第二消息通过该第一密钥进行加密, 或者, 该第二消息不用于该第一密钥进行加密。

在一些实施例中, 该第一消息为认证响应消息, 该第二消息为安全模式命令消息。

在一些实施例中, 该第一消息为安全模式命令消息, 该第二消息为安全模式响应消息。

在一些实施例中, 该通信单元 1310 还用于将该第一终端设备发送的第三消息转发至该第二终端设备;

其中, 该第三消息用于指示安全模式建立完成, 该第三消息通过目标密钥进行加密, 且该第三消息包括以下至少之一: 该第一终端设备生成的该第二密钥的标识的 y 个比特位, 第三消息验证码;

其中, 该目标密钥包括以下之一: 该第一密钥, 该第二密钥, 该第二密钥派生的机密性保护密钥;

其中, 该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护, 或者, 该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护, 该第三消息验证码的输入参数包括该 y 个比特位。

在一些实施例中, 该通信单元 1310 还用于将该第二终端设备发送的错误消息转发至该第一终端设备; 其中, 该错误消息包括以下至少之一: 原因信息, 第四消息验证码; 其中, 该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突, 或者, 该原因信息用于指示该第一消息验证码验证失败, 或者, 该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败; 该第四消息验证码的输入参数包括以下至少之一: 该原因信息。

在一些实施例中, 该完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥; 和/或, 该机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

在一些实施例中, 上述通信单元可以是通信接口或收发器, 或者是通信芯片或者片上系统的输入输出接口。

应理解, 根据本申请实施例的终端设备 1300 可对应于本申请方法实施例中的中继设备, 并且终端设备 1300 中的各个单元的上述和其它操作和/或功能分别为了实现图 10 所示方法 400 中中继设备的相应流程, 为了简洁, 在此不再赘述。

图 26 示出了根据本申请实施例的终端设备 1400 的示意性框图。该终端设备 1400 为第一终端设备, 如图 26 所示, 该终端设备 1400 包括:

通信单元 1410, 用于通过中继设备向第二终端设备发送第一消息;

其中, 该第一消息包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全

策略信息,该第一终端设备所属用户的信息,该第一终端设备生成的第一随机数,该第一终端设备生成的第二临时公钥,该第一终端设备生成的第一密钥的标识的 M 个比特位,该第一终端设备的签名,第一消息验证码;

其中,该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的公共验证令牌 PVT 和密钥管理服务服务器的公共认证密钥 KPAK;该第一终端设备的签名的输入参数包括以下至少之一:该第一终端设备所属用户的信息,该第二临时公钥,该 M 个比特位,该第二终端设备的签名;

其中,该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护,且该第一消息验证码的输入参数包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该第一随机数,该第二临时公钥,该 M 个比特位,该第一终端设备的签名;

其中,该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥,该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥,该第二密钥用于派生完整性保护密钥和/或机密性保护密钥,该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数;

其中,该中继设备的相关信息包括以下之一:该中继设备的身份信息,该中继设备生成的随机数,该中继设备生成的计数器。

在一些实施例中,该通信单元 1410 还用于接收该第二终端设备通过该中继设备发送的第二消息;

其中,该第二消息包括以下至少之一:该第二终端设备生成的该第二随机数,该第二终端设备生成的该第一密钥的标识的 N 个比特位,该第二终端设备生成的该第二密钥的标识的 x 个比特位,该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,第二消息验证码;

其中,该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护,或者,该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护,且该第二消息验证码的输入参数包括以下至少之一:该第二随机数,该 N 个比特位,该 x 个比特位,该第二终端设备选取的安全算法,该第二终端设备选取的安全策略;其中,该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

在一些实施例中,该第二消息通过该第一密钥进行加密,或者,该第二消息不用于该第一密钥进行加密。

在一些实施例中,该终端设备 1400 还包括:处理单元 1420;

在该第二消息中携带的信息未遭受篡改的情况下,该处理单元 1420 用于至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥,该处理单元 1420 还用于根据该第二密钥生成完整性保护密钥和/或机密性保护密钥,以及该处理单元 1420 还用于将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识,该处理单元 1420 还用于生成该第二密钥的标识的 y 个比特位,并将该 x 个比特位和该 y 个比特位合并得到该第二密钥的标识;

在该第二消息验证码有效的情况下,该处理单元 1420 还用于根据该第二终端设备选取的安全算法、该第二密钥、基于该第二密钥生成完整性保护密钥和/或机密性保护密钥、该第二终端设备选取的安全策略,与该第二终端设备进行通信。

在一些实施例中,该处理单元 1420 还用于根据该第一密钥解密该第二消息;

在该第二消息中携带的信息未遭受篡改的情况下,该处理单元 1420 还用于至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥,该处理单元 1420 还用于根据该第二密钥生成完整性保护密钥和/或机密性保护密钥,以及该处理单元 1420 还用于将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识,该处理单元 1420 还用于生成该第二密钥的标识的 y 个比特位,并将该 x 个比特位和该 y 个比特位合并得到该第二密钥的标识;

在该第二消息验证码有效的情况下,该处理单元 1420 还用于根据该第二终端设备选取的安全算法、该第二密钥、基于该第二密钥生成完整性保护密钥和/或机密性保护密钥、该第二终端设备选取的安全策略,与该第二终端设备进行通信。

在一些实施例中,该完整性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,该机密性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

在一些实施例中,该第一消息为认证响应消息,该第二消息为安全模式命令消息。

在一些实施例中,该第一消息为安全模式命令消息,该第二消息为安全模式响应消息。

在一些实施例中, 该通信单元 1410 还用于通过该中继设备向该第二终端设备发送第三消息;

其中, 该第三消息用于指示安全模式建立完成, 该第三消息通过目标密钥进行加密, 且该第三消息包括以下至少之一: 该第二密钥的标识的该 y 个比特位, 第三消息验证码;

其中, 该目标密钥包括以下之一: 该第一密钥, 该第二密钥, 该第二密钥派生的机密性保护密钥;

其中, 该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护, 或者, 该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护, 该第三消息验证码的输入参数包括该 y 个比特位。

在一些实施例中, 该通信单元 1410 还用于接收该第二终端设备通过该中继设备发送的错误消息; 其中, 该错误消息包括以下至少之一: 原因信息, 第四消息验证码; 其中, 该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突, 或者, 该原因信息用于指示该第一消息验证码验证失败, 或者, 该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败, 该第四消息验证码的输入参数包括以下至少之一: 该原因信息;

在该第四消息验证码有效的情况下, 该处理单元 1420 还用于确定安全模式建立失败, 和/或, 该处理单元 1420 还用于重新发起安全模式建立流程。

在一些实施例中, 该完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥; 和/或, 该机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

在一些实施例中, 该通信单元 1410 还用于接收该第二终端设备通过该中继设备发送的认证请求消息;

其中, 该认证请求消息包括以下至少之一: 该第二终端设备所属用户的信息, 该中继设备所属用户的信息, 该第二终端设备生成的第一临时公钥, 该第二终端设备的签名, 该中继设备的签名, 该中继设备的相关信息;

其中, 该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK; 该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK; 该第二终端设备的签名的输入参数包括以下至少之一: 该第二终端设备所属用户的信息和该第一临时公钥; 该中继设备的签名的输入参数包括以下至少之一: 该第二终端设备的签名和该中继设备所属用户的信息; 该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥。

在一些实施例中, 该第二终端设备的签名由该第二终端设备的秘密签名密钥生成, 和/或, 该中继设备的签名由该中继设备的秘密签名密钥生成。

在一些实施例中, 在该第二终端设备的 KPAK 和该中继设备的 KPAK 有效, 且基于该第二终端设备的标识和该第二终端设备的 PVT 对该第二终端设备的签名验证成功, 以及基于该中继设备的标识和该中继设备的 PVT 对该中继设备的签名验证成功的情况下, 该处理单元 1420 还用于生成与该第二临时公钥配对的第二临时私钥, 以及该处理单元 1420 还用于根据该第一临时公钥、该中继设备的相关信息和该第二临时私钥派生该第一密钥。

在一些实施例中, 上述通信单元可以是通信接口或收发器, 或者是通信芯片或者片上系统的输入输出接口。上述处理单元可以是一个或多个处理器。

应理解, 根据本申请实施例的终端设备 1400 可对应于本申请方法实施例中的第一终端设备, 并且终端设备 1400 中的各个单元的上述和其它操作和/或功能分别为了实现图 11 所示方法 500 中第一终端设备的相应流程, 为了简洁, 在此不再赘述。

图 27 示出了根据本申请实施例的终端设备 1500 的示意性框图。该终端设备 1500 为第二终端设备, 如图 27 所示, 该终端设备 1500 包括:

通信单元 1510, 用于接收第一终端设备通过中继设备发送的第一消息;

其中, 该第一消息包括以下至少之一: 该第一终端设备的安全能力信息, 该第一终端设备的安全策略信息, 该第一终端设备所属用户的信息, 该中继设备所属用户的信息, 该第一终端设备生成的第一随机数, 该第一终端设备生成的第二临时公钥, 该第一终端设备生成的第一密钥的标识的 M 个比特位, 该第一终端设备的签名, 该中继设备的签名, 第一消息验证码;

其中, 该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK; 该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK; 该第一终端设备的签名的输入参数包括以下至少之一: 该第一终端设备所属用户的信息, 该第二临时公钥, 该 M 个比特位, 该第二终端设备的签名; 该中继设备的签名的输入参数包括以下至少之一: 该中继设备所属用户的信息, 该第一终端设备的签名, 该第二终端设备的签名, 该第一消息;

其中,该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护,且该第一消息验证码的输入参数包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该第一随机数,该第二临时公钥,该M个比特位,该第一终端设备的签名;

其中,该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥,该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥,该第二密钥用于派生完整性保护密钥和/或机密性保护密钥,该第一密钥的标识由该M个比特位与该第一密钥的标识的另外N个比特位合并得到,M和N均为正整数;

其中,该中继设备的相关信息包括以下之一:该中继设备的身份信息,该中继设备生成的随机数,该中继设备生成的计数器。

在一些实施例中,该第一终端设备的签名由该第一终端设备的秘密签名密钥生成,和/或,该中继设备的签名由该中继设备的秘密签名密钥生成。

在一些实施例中,该终端设备1500还包括:处理单元1520;

该处理单元1520用于分别检查该第一终端设备的KPAK和该中继设备的KPAK,在该第一终端设备的KPAK和该中继设备的KPAK有效的情况下,且该处理单元1520还用于基于该第一终端设备的标识和该第一终端设备的PVT对该第一终端设备的签名进行验证,以及该处理单元1520还用于基于该中继设备的标识和该中继设备的PVT对该中继设备的签名进行验证;

在该第一终端设备的签名和该中继设备的签名验证成功,且该第一消息中携带的信息未遭受篡改的情况下,该处理单元1520还用于生成第二随机数,该处理单元1520还用于至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥,该处理单元1520还用于根据该第二密钥生成完整性保护密钥和/或机密性保护密钥,以及该处理单元1520还用于生成该第一密钥的标识的N个比特位,并将该M个比特位和该N个比特位合并得到该第一密钥的标识;

在该第一消息验证码有效的情况下,该通信单元1510还用于通过该中继设备向该第一终端设备发送第二消息;其中,该第二消息包括以下至少之一:该第二随机数,该N个比特位,该第二终端设备生成的该第二密钥的标识的x个比特位,该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,第二消息验证码;

其中,该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护,或者,该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护,且该第二消息验证码的输入参数包括以下至少之一:该第二随机数,该N个比特位,该x个比特位,该第二终端设备选取的安全算法,该第二终端设备选取的安全策略;其中,该第二密钥的标识由该x个比特位与该第二密钥的标识的另外y个比特位合并得到,x和y均为正整数。

在一些实施例中,该第二消息通过该第一密钥进行加密,或者,该第二消息不用于该第一密钥进行加密。

在一些实施例中,该第一消息为认证响应消息,该第二消息为安全模式命令消息。

在一些实施例中,该第一消息为安全模式命令消息,该第二消息为安全模式响应消息。

在一些实施例中,该完整性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,该机密性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

在一些实施例中,该通信单元1510还用于接收该第一终端设备通过该中继设备发送的第三消息;

其中,该第三消息用于指示安全模式建立完成,该第三消息通过目标密钥进行加密,且该第三消息包括以下至少之一:该第一终端设备生成的该第二密钥的标识的y个比特位,第三消息验证码;

其中,该目标密钥包括以下之一:该第一密钥,该第二密钥,该第二密钥派生的机密性保护密钥;

其中,该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护,或者,该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护,该第三消息验证码的输入参数包括该y个比特位。

在一些实施例中,该处理单元1520还用于通过该目标密钥对该第三消息进行解密;

在该第三消息中携带的信息未遭受篡改的情况下,且该第三消息验证码有效的情况下,该处理单元1520还用于将该x个比特位与该y个比特位合并得到该第二密钥的标识。

在一些实施例中,该通信单元1510还用于通过该中继设备向该第一终端设备发送错误消息;其中,该错误消息包括以下至少之一:原因信息,第四消息验证码;其中,该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突,或者,该原因信息用于指示该第一消息验证码验证失败,

或者,该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败,该第四消息验证码的输入参数包括以下至少之一:该原因信息。

在一些实施例中,该完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥;和/或,该机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

5 在一些实施例中,该通信单元 1510 还用于通过该中继设备向该第一终端设备发送认证请求消息;其中,该认证请求消息包括以下至少之一:该第二终端设备所属用户的信息,该第二终端设备生成的第一临时公钥,该第二终端设备的签名,该中继设备的相关信息;

10 其中,该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK;该第二终端设备的签名的输入参数包括以下至少之一:该第二终端设备所属用户的信息和该第一临时公钥;该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥。

在一些实施例中,该第二终端设备的签名由该第二终端设备的秘密签名密钥生成。

在一些实施例中,上述通信单元可以是通信接口或收发器,或者是通信芯片或者片上系统的输入输出接口。上述处理单元可以是一个或多个处理器。

15 应理解,根据本申请实施例的终端设备 1500 可对应于本申请方法实施例中的第二终端设备,并且终端设备 1500 中的各个单元的上述和其它操作和/或功能分别为了实现图 12 所示方法 600 中第二终端设备的相应流程,为了简洁,在此不再赘述。

图 28 示出了根据本申请实施例的终端设备 1600 的示意性框图。该终端设备 1600 为中继设备,如图 28 所示,该终端设备 1600 包括:

20 通信单元 1610,用于接收第一终端设备发送的第一消息;其中,该第一消息包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该第一终端设备生成的第一随机数,该第一终端设备生成的第二临时公钥,该第一终端设备生成的第一密钥的标识的 M 个比特位,该第一终端设备的签名,第一消息验证码;其中,该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK;该第一终端设备的签名的输入参数包括以下至少之一:该第一终端设备所属用户的信息,该第二临时公钥,该 M 个比特位,该第二终端设备的签名;其中,该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护,且该第一消息验证码的输入参数包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该第一随机数,该第二临时公钥,该 M 个比特位,该第一终端设备的签名;

25 在该第一终端设备的 KPAK 有效,且基于该第一终端设备的标识和该第一终端设备的 PVT 对该第一终端设备的签名验证成功的情况下,该通信单元 1610 还用于向该第二终端设备发送验证之后的第一消息;其中,该验证之后的第一消息包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备所属用户的信息,该中继设备所属用户的信息,该第一终端设备生成的第一随机数,该第一终端设备生成的与该第二临时私钥配对的第二临时公钥,该第一终端设备生成的该第一密钥的标识的 M 个比特位,该第一终端设备的签名,该中继设备的签名,该中继设备的相关信息,该第一消息验证码;其中,该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK;该中继设备的签名的输入参数包括以下至少之一:该中继设备所属用户的信息,该第一终端设备的签名,该第二终端设备的签名,该验证之后的第一消息;

30 其中,该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥,该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥,该第二密钥用于派生完整性保护密钥和/或机密性保护密钥,该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到,M 和 N 均为正整数;其中,该中继设备的相关信息包括以下之一:该中继设备的身份信息,该中继设备生成的随机数,该中继设备生成的计数器。

35 在一些实施例中,该通信单元 1610 还用于将该第二终端设备发送的第二消息转发至该第一终端设备;

40 其中,该第二消息包括以下至少之一:该第二终端设备生成的该第二随机数,该第二终端设备生成的该第一密钥的标识的 N 个比特位,该第二终端设备生成的该第二密钥的标识的 x 个比特位,该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,第二消息验证码;

45 其中,该第二消息通过基于该第二密钥生成的该第二消息验证码进行完整性保护,或者,该第二消息通过基于该第二密钥派生的完整性保护密钥生成的该第二消息验证码进行完整性保护,且该第二消息验证码的输入参数包括以下至少之一:该第二随机数,该 N 个比特位,该 x 个比特位,该第二终端设备选取的安全算法,该第二终端设备选取的安全策略;其中,该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到,x 和 y 均为正整数。

在一些实施例中，该第二消息通过该第一密钥进行加密，或者，该第二消息不用于该第一密钥进行加密。

在一些实施例中，该第一消息为认证响应消息，该第二消息为安全模式命令消息。

在一些实施例中，该第一消息为安全模式命令消息，该第二消息为安全模式响应消息。

5 在一些实施例中，该通信单元 1610 还用于将该第一终端设备发送的第三消息转发至该第二终端设备；

其中，该第三消息用于指示安全模式建立完成，该第三消息通过目标密钥进行加密，且该第三消息包括以下至少之一：该第一终端设备生成的该第二密钥的标识的 y 个比特位，第三消息验证码；

其中，该目标密钥包括以下之一：该第一密钥，该第二密钥，该第二密钥派生的机密性保护密钥；

10 其中，该第三消息通过基于该第二密钥生成的该第三消息验证码进行完整性保护，或者，该第三消息通过基于该第二密钥派生的完整性保护密钥生成的该第三消息验证码进行完整性保护，该第三消息验证码的输入参数包括该 y 个比特位。

15 在一些实施例中，该通信单元 1610 还用于将该第二终端设备发送的错误消息转发至该第一终端设备；其中，该错误消息包括以下至少之一：原因信息，第四消息验证码；其中，该原因信息用于指示该第二终端设备与该第一终端设备的安全策略冲突，或者，该原因信息用于指示该第一消息验证码验证失败，或者，该原因信息用于指示该第二终端设备与该第一终端设备的安全算法协商失败，该第四消息验证码的输入参数包括以下至少之一：该原因信息。

在一些实施例中，该完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥；和/或，该机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

20 在一些实施例中，该通信单元 1610 还用于接收该第二终端设备发送的认证请求消息；其中，该认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该第二终端设备生成的第一临时公钥，该第二终端设备的签名；其中，该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的 PVT 和 KPAK；该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥；该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥；

25 在该第二终端设备的 KPAK 有效，且基于该第二终端设备的标识和该第二终端设备的 PVT 对该第二终端设备的签名验证成功的情况下，该通信单元 1610 还用于向该第一终端设备发送验证之后的认证请求消息；其中，该验证之后的认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该中继设备所属用户的信息，该第一临时公钥，该第二终端设备的签名，该中继设备的签名，该中继设备的相关信息；其中，该中继设备所属用户的信息包括该中继设备的标识和该中继设备的 PVT 和 KPAK；该中继设备的签名的输入参数包括以下至少之一：该第二终端设备的签名和该中继设备所属用户的信息。

30 在一些实施例中，该第二终端设备的签名由该第二终端设备的秘密签名密钥生成，和/或，该中继设备的签名由该中继设备的秘密签名密钥生成。

35 在一些实施例中，上述通信单元可以是通信接口或收发器，或者是通信芯片或者片上系统的输入输出接口。

应理解，根据本申请实施例的终端设备 1600 可对应于本申请方法实施例中的中继设备，并且终端设备 1600 中的各个单元的上述和其它操作和/或功能分别为了实现图 13 所示方法 700 中中继设备的相应流程，为了简洁，在此不再赘述。

40 图 29 示出了根据本申请实施例的终端设备 1700 的示意性框图。该终端设备 1700 为第一终端设备，如图 29 所示，该终端设备 1700 包括：

通信单元 1710，用于通过中继设备向第二终端设备发送直接通信请求；

其中，该直接通信请求包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备生成的第一临时公钥，该第一终端设备生成的第一随机数；

45 其中，该直接通信请求通过第一加密密钥进行加密，以及该直接通信请求通过第一完整性保护密钥进行完整性保护，该第一加密密钥为基于已注册并被授权使用终端至终端中继 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥，该第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥；

50 其中，该第一临时公钥和该中继设备的相关信息用于该第二终端设备派生第一密钥；该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥；

其中,该中继设备的相关信息包括以下之一:该中继设备的身份信息,该中继设备生成的随机数,该中继设备生成的计数器。

在一些实施例中,该通信单元 1710 还用于接收该第二终端设备通过该中继设备发送的安全模式命令;

其中,该安全模式命令包括以下至少之一:该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,该第二终端设备生成的第二临时公钥,该第二终端设备生成的该第二随机数,该第二终端设备生成的该第一密钥的标识的 M 个比特位,该中继设备的相关信息,第一消息验证码;

其中,该安全模式命令通过该第一加密密钥进行加密,该安全模式命令通过该第一完整性保护密钥进行完整性保护,该第一消息验证码基于该第二完整性保护密钥生成,且该第一消息验证码的输入参数包括以下至少之一:该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,该第二临时公钥,该第二随机数,该 M 个比特位,该中继设备的相关信息;

其中,该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥,该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该安全模式命令还包括该第二终端设备生成的该第二密钥的标识的 x 个比特位,以及该第一消息验证码的输入参数包括该 x 个比特位;

其中,该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该终端设备 1700 还包括:处理单元 1720;

该处理单元 1720 用于使用该第一加密密钥解密该安全模式命令,以及使用该第一完整性保护密钥判断该安全模式命令的完整性;

在该安全模式命令中携带的信息未遭受篡改的情况下,该处理单元 1720 还用于根据与该第一临时公钥配对的第一临时私钥、该第二临时公钥、该中继设备的相关信息派生该第一密钥,且该处理单元 1720 还用于生成该第一密钥的标识的该 N 个比特位,以及将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识;

该处理单元 1720 还用于至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥,该第一终端设备根据该第二密钥生成该第二完整性保护密钥和/或该第二加密密钥,以及该处理单元 1720 还用于生成该第二密钥的标识的该 y 个比特位,并将该 x 个比特位和该 y 个比特位合并得到该第二密钥的标识;

在该第一消息验证码有效的情况下,该处理单元 1720 还用于根据该第二终端设备选取的安全算法、该第二完整性保护密钥和/或该第二加密密钥、该第二终端设备选取的安全策略,与该第二终端设备进行通信。

在一些实施例中,该通信单元 1710 还用于通过该中继设备向该第二终端设备发送安全模式建立完成消息;

其中,该安全模式建立完成消息通过该第二密钥或该第二加密密钥进行加密,该安全模式建立完成消息通过该第二密钥或该第二完整性保护密钥进行完整性保护;

其中,该安全模式建立完成消息至少包括该第二密钥的标识的该 y 个比特位。

在一些实施例中,该第二完整性保护密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,该第二加密密钥的输入参数包括以下至少之一:该第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下,该处理单元 1720 还用于使用该第一加密密钥解密该安全模式命令,以及使用该第一完整性保护密钥判断该安全模式命令的完整性;

在该安全模式命令中携带的信息未遭受篡改的情况下,该处理单元 1720 还用于根据与该第一临时公钥配对的第一临时私钥、该第二临时公钥、该中继设备的相关信息派生该第一密钥,且该处理单元 1720 还用于生成该第一密钥的该 N 个比特位,以及将该 M 个比特位和该 N 个比特位合并得到该第一密钥的标识;

该处理单元 1720 还用于至少根据该第一随机数、该第一密钥和该第二随机数生成该第二完整性保护密钥和/或该第二加密密钥;

在该第一消息验证码有效的情况下,该处理单元 1720 还用于根据该第二终端设备选取的安全算

法、该第二完整性保护密钥和/或该第二加密密钥、该第二终端设备选取的安全策略，与该第二终端设备进行通信。

在一些实施例中，该通信单元 1710 还用于通过该中继设备向该第二终端设备发送安全模式建立完成消息；

其中，该安全模式建立完成消息通过该第二加密密钥进行加密，该安全模式建立完成消息通过该第二完整性保护密钥进行完整性保护。

在一些实施例中，该第二完整性保护密钥的输入参数包括以下至少之一：该第一随机数，该第一密钥，该第二随机数，选定的算法类型标识符，选定的算法类型标识符的长度，完整性保护算法标识，完整性保护算法标识的长度；和/或，

该第二加密密钥的输入参数包括以下至少之一：该第一随机数，该第一密钥，该第二随机数，选定的算法类型标识符，选定的算法类型标识符的长度，机密性保护算法标识，机密性保护算法标识的长度。

在一些实施例中，该第一加密密钥为邻近业务加密密钥 PEK，该第一完整性保护密钥为邻近业务完整性保护密钥 PIK。

在一些实施例中，上述通信单元可以是通信接口或收发器，或者是通信芯片或者片上系统的输入输出接口。上述处理单元可以是一个或多个处理器。

应理解，根据本申请实施例的终端设备 1700 可对应于本申请方法实施例中的第一终端设备，并且终端设备 1700 中的各个单元的上述和其它操作和/或功能分别为了实现图 16 所示方法 800 中第一终端设备的相应流程，为了简洁，在此不再赘述。

图 30 示出了根据本申请实施例的终端设备 1800 的示意性框图。该终端设备 1800 为第二终端设备，如图 30 所示，该终端设备 1800 包括：

通信单元 1810，用于接收第一终端设备通过中继设备发送的直接通信请求；

其中，该直接通信请求包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备生成的第一临时公钥，该第一终端设备生成的第一随机数，该中继设备的标识，该中继设备的相关信息；

其中，该直接通信请求通过第一加密密钥进行加密，以及该直接通信请求通过第一完整性保护密钥进行完整性保护，该第一加密密钥为基于已注册并被授权使用终端至终端中继 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥，该第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥；

其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器；该第一临时公钥和该中继设备的相关信息用于该第二终端设备派生第一密钥；该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥；

其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

在一些实施例中，在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下，该终端设备 1800 还包括：处理单元 1820；

该处理单元 1820 用于使用该第一加密密钥解密该直接通信请求，以及使用该第一完整性保护密钥判断该直接通信请求的完整性；

在该直接通信请求中携带的信息未遭受篡改的情况下，该处理单元 1820 还用于生成第二临时私钥，以及该处理单元 1820 还用于根据该第一临时公钥、该第二临时私钥和该中继设备的相关信息派生该第一密钥，且该第二终端设备生成该第一密钥的标识的 M 个比特位；

该处理单元 1820 还用于生成该第二随机数，以及该处理单元 1820 还用于至少根据该第一随机数、该第一密钥和该第二随机数生成该第二密钥，该处理单元 1820 还用于根据该第二密钥生成该第二完整性保护密钥和/或该第二加密密钥，且该处理单元 1820 还用于生成该第二密钥的标识的 x 个比特位；

其中，该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数，该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到，x 和 y 均为正整数。

在一些实施例中，该通信单元 1810 还用于通过该中继设备向该第一终端设备发送安全模式命令；

其中，该安全模式命令包括以下至少之一：该第二终端设备选取的安全算法，该第二终端设备选取的安全策略，该第二终端设备生成的与该第二临时私钥配对的第二临时公钥，该第二随机数，该第

一密钥的标识的该 M 个比特位, 该第二密钥的标识的该 x 个比特位, 第一消息验证码;

其中, 该安全模式命令通过该第一加密密钥进行加密, 该安全模式命令通过该第一完整性保护密钥进行完整性保护, 该第一消息验证码基于该第二完整性保护密钥生成, 且该第一消息验证码的输入参数包括以下至少之一: 该第二终端设备选取的安全算法, 该第二终端设备选取的安全策略, 该第二临时公钥, 该第二随机数, 该 M 个比特位, 该 x 个比特位, 该中继设备的相关信息; 该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥。

在一些实施例中, 该通信单元 1810 还用于接收该第一终端设备通过该中继设备发送的安全模式建立完成消息;

其中, 该安全模式建立完成消息通过该第二密钥或该第二加密密钥进行加密, 该安全模式建立完成消息通过该第二密钥或该第二完整性保护密钥进行完整性保护;

其中, 该安全模式建立完成消息至少包括该第二密钥的标识的该 y 个比特位。

在一些实施例中, 该第二完整性保护密钥的输入参数包括以下至少之一: 该第二密钥, 选定的算法类型标识符, 选定的算法类型标识符的长度, 完整性保护算法标识, 完整性保护算法标识的长度; 和/或, 该第二加密密钥的输入参数包括以下至少之一: 该第二密钥, 选定的算法类型标识符, 选定的算法类型标识符的长度, 机密性保护算法标识, 机密性保护算法标识的长度。

在一些实施例中, 在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下, 该终端设备 1800 还包括: 处理单元 1820;

该处理单元 1820 用于使用该第一加密密钥解密该直接通信请求, 以及使用该第一完整性保护密钥判断该直接通信请求的完整性;

在该直接通信请求中携带的信息未遭受篡改的情况下, 该处理单元 1820 还用于生成第二临时私钥, 以及该处理单元 1820 还用于根据该第一临时公钥、该第二临时私钥和该中继设备的相关信息派生该第一密钥, 且该处理单元 1820 还用于生成该第一密钥的标识的 M 个比特位;

该处理单元 1820 还用于生成该第二随机数, 以及该处理单元 1820 还用于至少根据该第一随机数、该第一密钥和该第二随机数生成该第二完整性保护密钥和/或该第二加密密钥; 其中, 该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数。

在一些实施例中, 该通信单元 1810 还用于通过该中继设备向该第一终端设备发送安全模式命令;

其中, 该安全模式命令包括以下至少之一: 该第二终端设备选取的安全算法, 该第二终端设备选取的安全策略, 该第二终端设备生成的与该第二临时私钥配对的第二临时公钥, 该第二随机数, 该第一密钥的标识的该 M 个比特位, 第一消息验证码;

其中, 该安全模式命令通过该第一加密密钥进行加密, 该安全模式命令通过该第一完整性保护密钥进行完整性保护, 该第一消息验证码基于该第二完整性保护密钥生成, 且该第一消息验证码的输入参数包括以下至少之一: 该第二终端设备选取的安全算法, 该第二终端设备选取的安全策略, 该第二临时公钥, 该第二随机数, 该 M 个比特位; 该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥。

在一些实施例中, 该通信单元 1810 还用于接收该第一终端设备通过该中继设备发送的安全模式建立完成消息;

其中, 该安全模式建立完成消息通过该第二加密密钥进行加密, 该安全模式建立完成消息通过该第二完整性保护密钥进行完整性保护。

在一些实施例中, 该第二完整性保护密钥的输入参数包括以下至少之一: 该第一随机数, 该第一密钥, 该第二随机数, 选定的算法类型标识符, 选定的算法类型标识符的长度, 完整性保护算法标识, 完整性保护算法标识的长度; 和/或,

该第二加密密钥的输入参数包括以下至少之一: 该第一随机数, 该第一密钥, 该第二随机数, 选定的算法类型标识符, 选定的算法类型标识符的长度, 机密性保护算法标识, 机密性保护算法标识的长度。

在一些实施例中, 该安全模式命令还包括该中继设备的相关信息, 以及该第一消息验证码的输入参数还包括该中继设备的相关信息。

在一些实施例中, 该处理单元 1820 还用于根据该第二终端设备选取的安全算法、该第二完整性保护密钥和/或该第二加密密钥、该第二终端设备选取的安全策略, 与该第一终端设备进行通信。

在一些实施例中, 该第一加密密钥为邻近业务加密密钥 PEK, 该第一完整性保护密钥为邻近业务完整性保护密钥 PIK。

在一些实施例中, 上述通信单元可以是通信接口或收发器, 或者是通信芯片或者片上系统的输入输出接口。上述处理单元可以是一个或多个处理器。

应理解,根据本申请实施例的终端设备 1800 可对应于本申请方法实施例中的第二终端设备,并且终端设备 1800 中的各个单元的上述和其它操作和/或功能分别为了实现图 17 所示方法 900 中第二终端设备的相应流程,为了简洁,在此不再赘述。

图 31 示出了根据本申请实施例的终端设备 1900 的示意性框图。该终端设备 1900 为中继设备,如图 31 所示,该终端设备 1900 包括:

通信单元 1910,用于接收第一终端设备发送的直接通信请求;其中,该直接通信请求包括以下至少之一:该第一终端设备的安全能力信息,该第一终端设备的安全策略信息,该第一终端设备生成的第一临时公钥,该第一终端设备生成的第一随机数;其中,该直接通信请求通过第一加密密钥进行加密,以及该直接通信请求通过第一完整性保护密钥进行完整性保护,该第一加密密钥为基于已注册并被授权使用终端至终端中继 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥,该第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥;

处理单元 1920,用于验证是否被配置为转发直接通信请求,在验证通过之后该处理单元 1920 用于使用该第一加密密钥解密该直接通信请求以获取服务质量 QoS 和计费信息,以及该处理单元 1920 用于使用该第一完整性保护密钥验证该直接通信请求的完整性,在验证通过之后该中继设备在该直接通信请求中添加该中继设备的相关信息和该中继设备的标识,并且该处理单元 1920 用于使用该第一加密密钥加密该直接通信请求,使用该第一完整性保护密钥保护该直接通信请求的完整性,该通信单元 1910 还用于并将该直接通信请求转发至第二终端设备;

其中,该中继设备的相关信息包括以下之一:该中继设备的身份信息,该中继设备生成的随机数,该中继设备生成的计数器;该第一临时公钥和该中继设备的相关信息用于第二终端设备派生第一密钥;该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥,且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥,或者,该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二密钥的情况下,该通信单元 1910 还用于接收该第二终端设备发送的安全模式命令;其中,该安全模式命令包括以下至少之一:该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,该第二终端设备生成的第二临时公钥,该第二终端设备生成的该第二随机数,该第二终端设备生成的该第一密钥的标识的 M 个比特位,该第二终端设备生成的该第二密钥的标识的 x 个比特位,第一消息验证码;其中,该安全模式命令通过该第一加密密钥进行加密,该安全模式命令通过该第一完整性保护密钥进行完整性保护,该第一消息验证码基于该第二完整性保护密钥生成,且该第一消息验证码的输入参数包括以下至少之一:该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,该第二临时公钥,该第二随机数,该 M 个比特位,该 x 个比特位,该中继设备的相关信息;该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥;

该处理单元 1920 还用于使用该第一加密密钥解密该安全模式命令,以获取 QoS 和计费信息,该通信单元 1910 还用于在向该第一终端设备转发该安全模式命令;

其中,该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥,该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数,该第二密钥的标识由该 x 个比特位与该第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

在一些实施例中,该通信单元 1910 还用于向该第二终端设备转发该第一终端设备发送的安全模式建立完成消息;

其中,该安全模式建立完成消息通过该第二密钥或该第二加密密钥进行加密,该安全模式建立完成消息通过该第二密钥或该第二完整性保护密钥进行完整性保护;

其中,该安全模式建立完成消息至少包括该第二密钥的标识的该 y 个比特位。

在一些实施例中,在该第一随机数、该第一密钥和该第二随机数用于派生该第二加密密钥和/或该第二完整性保护密钥的情况下,该通信单元 1910 还用于接收该第二终端设备发送的安全模式命令;其中,该安全模式命令包括以下至少之一:该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,该第二终端设备生成的第二临时公钥,该第二终端设备生成的该第二随机数,该第二终端设备生成的该第一密钥的标识的 M 个比特位,第一消息验证码;其中,该安全模式命令通过该第一加密密钥进行加密,该安全模式命令通过该第一完整性保护密钥进行完整性保护,该第一消息验证码基于该第二完整性保护密钥生成,且该第一消息验证码的输入参数包括以下至少之一:该第二终端设备选取的安全算法,该第二终端设备选取的安全策略,该第二临时公钥,该第二随机数,该 M 个比特位,该中继设备的相关信息;该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥;

该处理单元 1920 还用于使用该第一加密密钥解密该安全模式命令，以获取 QoS 和计费信息，该通信单元 1910 还用于在向该第一终端设备转发该安全模式命令；

其中，该第二临时公钥和该中继设备的相关信息用于该第一终端设备派生该第一密钥，该第一密钥的标识由该 M 个比特位与该第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数。

5 在一些实施例中，该通信单元 1910 还用于向该第二终端设备转发该第一终端设备发送的安全模式建立完成消息；

其中，该安全模式建立完成消息通过该第二加密密钥进行加密，该安全模式建立完成消息通过该第二完整性保护密钥进行完整性保护。

10 在一些实施例中，该安全模式命令包括该中继设备的相关信息，以及该第一消息验证码的输入参数还包括该中继设备的相关信息；或者，该中继设备在向该第一终端设备转发的该安全模式命令中添加了该中继设备的相关信息。

在一些实施例中，该第一加密密钥为邻近业务加密密钥 PEK，该第一完整性保护密钥为邻近业务完整性保护密钥 PIK。

15 在一些实施例中，上述通信单元可以是通信接口或收发器，或者是通信芯片或者片上系统的输入输出接口。上述处理单元可以是一个或多个处理器。

应理解，根据本申请实施例的终端设备 1900 可对应于本申请方法实施例中的中继设备，并且终端设备 1900 中的各个单元的上述和其它操作和/或功能分别为了实现图 18 所示方法 1000 中中继设备的相应流程，为了简洁，在此不再赘述。

20 图 32 是本申请实施例提供的一种通信设备 2000 示意性结构图。图 32 所示的通信设备 2000 包括处理器 2010，处理器 2010 可以从存储器中调用并运行计算机程序，以实现本申请实施例中的方法。

在一些实施例中，如图 32 所示，通信设备 2000 还可以包括存储器 2020。其中，处理器 2010 可以从存储器 2020 中调用并运行计算机程序，以实现本申请实施例中的方法。

其中，存储器 2020 可以是独立于处理器 2010 的一个单独的器件，也可以集成在处理器 2010 中。

25 在一些实施例中，如图 32 所示，通信设备 2000 还可以包括收发器 2030，处理器 2010 可以控制该收发器 2030 与其他设备进行通信，具体地，可以向其他设备发送信息或数据，或接收其他设备发送的信息或数据。

其中，收发器 2030 可以包括发射机和接收机。收发器 2030 还可以进一步包括天线，天线的数量可以是一个或多个。

30 在一些实施例中，该通信设备 2000 具体可为本申请实施例的终端设备，并且该通信设备 2000 可以实现本申请实施例的各个方法中由第一终端设备和/或第二终端实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该通信设备 2000 具体可为本申请实施例的终端设备，并且该通信设备 2000 可以实现本申请实施例的各个方法中由中继设备实现的相应流程，为了简洁，在此不再赘述。

35 图 33 是本申请实施例的装置的示意性结构图。图 33 所示的装置 2100 包括处理器 2110，处理器 2110 可以从存储器中调用并运行计算机程序，以实现本申请实施例中的方法。

在一些实施例中，如图 33 所示，装置 2100 还可以包括存储器 2120。其中，处理器 2110 可以从存储器 2120 中调用并运行计算机程序，以实现本申请实施例中的方法。

其中，存储器 2120 可以是独立于处理器 2110 的一个单独的器件，也可以集成在处理器 2110 中。

40 在一些实施例中，该装置 2100 还可以包括输入接口 2130。其中，处理器 2110 可以控制该输入接口 2130 与其他设备或芯片进行通信，具体地，可以获取其他设备或芯片发送的信息或数据。

在一些实施例中，该装置 2100 还可以包括输出接口 2140。其中，处理器 2110 可以控制该输出接口 2140 与其他设备或芯片进行通信，具体地，可以向其他设备或芯片输出信息或数据。

45 在一些实施例中，该装置可应用于本申请实施例中的终端设备，并且该装置可以实现本申请实施例的各个方法中由第一终端设备和/或第二终端实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该装置可应用于本申请实施例中的终端设备，并且该装置可以实现本申请实施例的各个方法中由中继设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，本申请实施例提到的装置也可以是芯片。例如可以是系统级芯片，系统芯片，芯片系统或片上系统芯片等。

50 图 34 是本申请实施例提供的一种通信系统 2200 的示意性框图。如图 34 所示，该通信系统 2200 包括第一终端设备 2210、第二终端设备 2220 和中继设备 2230。

其中，该第一终端设备 2210 可以用于实现上述方法中由第一终端设备实现的相应的功能，该第二终端设备 2220 可以用于实现上述方法中由第二终端设备实现的相应的功能，以及该中继设备 2230

可以用于实现上述方法中由中继设备实现的相应的功能，为了简洁，在此不再赘述。

应理解，本申请实施例的处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、数字信号处理器(Digital Signal Processor, DSP)、专用集成电路(Application Specific Integrated Circuit, ASIC)、现成可编程门阵列(Field Programmable Gate Array, FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

可以理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(Read-Only Memory, ROM)、可编程只读存储器(Programmable ROM, PROM)、可擦除可编程只读存储器(Erasable PROM, EPROM)、电可擦除可编程只读存储器(Electrically EPROM, EEPROM)或闪存。易失性存储器可以是随机存取存储器(Random Access Memory, RAM)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的RAM可用，例如静态随机存取存储器(Static RAM, SRAM)、动态随机存取存储器(Dynamic RAM, DRAM)、同步动态随机存取存储器(Synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器(Double Data Rate SDRAM, DDR SDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器(Synchlink DRAM, SLDRAM)和直接内存总线随机存取存储器(Direct Rambus RAM, DR RAM)。应注意，本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

应理解，上述存储器为示例性但不是限制性说明，例如，本申请实施例中的存储器还可以是静态随机存取存储器(static RAM, SRAM)、动态随机存取存储器(dynamic RAM, DRAM)、同步动态随机存取存储器(synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器(double data rate SDRAM, DDR SDRAM)、增强型同步动态随机存取存储器(enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器(synch link DRAM, SLDRAM)以及直接内存总线随机存取存储器(Direct Rambus RAM, DR RAM)等等。也就是说，本申请实施例中的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

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。

在一些实施例中，该计算机可读存储介质可应用于本申请实施例中的终端设备，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第一终端设备和/或第二终端设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该计算机可读存储介质可应用于本申请实施例中的终端设备，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中继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计算机程序产品，包括计算机程序指令。

在一些实施例中，该计算机程序产品可应用于本申请实施例中的终端设备，并且该计算机程序指令使得计算机执行本申请实施例的各个方法中由第一终端设备和/或第二终端设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该计算机程序产品可应用于本申请实施例中的终端设备，并且该计算机程序指令使得计算机执行本申请实施例的各个方法中由中继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计算机程序。

在一些实施例中，该计算机程序可应用于本申请实施例中的终端设备，当该计算机程序在计算机上运行时，使得计算机执行本申请实施例的各个方法中由第一终端设备和/或第二终端设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该计算机程序可应用于本申请实施例中的终端设备，当该计算机程序在计算机上运行时，使得计算机执行本申请实施例的各个方法中由中继设备实现的相应流程，为了简洁，在此不再赘述。

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，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

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

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

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，可以存储在一个计算机可读存储介质中。针对这样的理解，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。

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

1、一种中继通信的方法，其特征在于，包括：

第一终端设备接收第二终端设备通过中继设备发送的认证请求消息；

其中，所述认证请求消息包括以下至少之一：所述第二终端设备所属用户的信息，所述中继设备所属用户的信息，所述第二终端设备生成的第一临时公钥，所述第二终端设备的签名，所述中继设备的签名，所述中继设备的相关信息；

其中，所述第二终端设备所属用户的信息包括所述第二终端设备的标识和所述第二终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK；所述中继设备所属用户的信息包括所述中继设备的标识和所述中继设备的 PVT 和 KPAK；所述第二终端设备的签名的输入参数包括以下至少之一：所述第二终端设备所属用户的信息和所述第一临时公钥；所述中继设备的签名的输入参数包括以下至少之一：所述第二终端设备的签名和所述中继设备所属用户的信息；所述第一临时公钥和所述中继设备的相关信息用于所述第一终端设备派生第一密钥；所述中继设备的相关信息包括以下之一：所述中继设备的身份信息，所述中继设备生成的随机数，所述中继设备生成的计数器。

2、如权利要求 1 所述的方法，其特征在于，

所述第二终端设备的签名由所述第二终端设备的秘密签名密钥生成，和/或，所述中继设备的签名由所述中继设备的秘密签名密钥生成。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述方法还包括：

在所述第二终端设备的 KPAK 和所述中继设备的 KPAK 有效，且基于所述第二终端设备的标识和所述第二终端设备的 PVT 对所述第二终端设备的签名验证成功，以及基于所述中继设备的标识和所述中继设备的 PVT 对所述中继设备的签名验证成功的情况下，所述第一终端设备生成第二临时私钥，以及所述第一终端设备根据所述第一临时公钥、所述中继设备的相关信息和所述第二临时私钥派生所述第一密钥。

4、如权利要求 3 所述的方法，其特征在于，所述方法还包括：

所述第一终端设备通过所述中继设备向所述第二终端设备发送第一消息；

其中，所述第一消息包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安全策略信息，所述第一终端设备所属用户的信息，所述第一终端设备生成的第一随机数，所述第一终端设备生成的与所述第二临时私钥配对的所述第二临时公钥，所述第一终端设备生成的所述第一密钥的标识的 M 个比特位，所述第一终端设备的签名，第一消息验证码；

其中，所述第一终端设备所属用户的信息包括所述第一终端设备的标识和所述第一终端设备的 PVT 和 KPAK；所述第一终端设备的签名的输入参数包括以下至少之一：所述第一终端设备所属用户的信息，所述第二临时公钥，所述 M 个比特位，所述第二终端设备的签名；

其中，所述第一消息通过基于所述第一密钥生成的所述第一消息验证码进行完整性保护，且所述第一消息验证码的输入参数包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安全策略信息，所述第一终端设备所属用户的信息，所述第一随机数，所述第二临时公钥，所述 M 个比特位，所述第一终端设备的签名；

其中，所述第二临时公钥和所述中继设备的相关信息用于所述第二终端设备派生所述第一密钥，所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥，所述第二密钥用于派生完整性保护密钥和/或机密性保护密钥，所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数。

5、如权利要求 4 所述的方法，其特征在于，所述方法还包括：

所述第一终端设备接收所述第二终端设备通过所述中继设备发送的第二消息；

其中，所述第二消息包括以下至少之一：所述第二终端设备生成的所述第二随机数，所述第二终端设备生成的所述第一密钥的标识的 N 个比特位，所述第二终端设备生成的所述第二密钥的标识的 x 个比特位，所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略，第二消息验证码；

其中，所述第二消息通过基于所述第二密钥生成的所述第二消息验证码进行完整性保护，或者，所述第二消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第二消息验证码进行完整性保护，且所述第二消息验证码的输入参数包括以下至少之一：所述第二随机数，所述 N 个比特位，所述 x 个比特位，所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略；其中，所述第二密钥的标识由所述 x 个比特位与所述第二密钥的标识的另外 y 个比特位合并得到，x 和 y 均为正整数。

6、如权利要求 5 所述的方法，其特征在于，

所述第二消息通过所述第一密钥进行加密。

7、如权利要求5所述的方法，其特征在于，所述方法还包括：

在所述第二消息中携带的信息未遭受篡改的情况下，所述第一终端设备至少根据所述第一随机数、所述第一密钥和所述第二随机数生成所述第二密钥，所述第一终端设备根据所述第二密钥生成完整性保护密钥和/或机密性保护密钥，以及所述第一终端设备将所述M个比特位和所述N个比特位合并得到所述第一密钥的标识，所述第一终端设备生成所述第二密钥的标识的y个比特位，并将所述x个比特位和所述y个比特位合并得到所述第二密钥的标识；

在所述第二消息验证码有效的情况下，所述第一终端设备根据所述第二终端设备选取的安全算法、所述第二密钥、基于所述第二密钥生成完整性保护密钥和/或机密性保护密钥、所述第二终端设备选取的安全策略，与所述第二终端设备进行通信。

8、如权利要求6所述的方法，其特征在于，所述方法还包括：

所述第一终端设备根据所述第一密钥解密所述第二消息；

在所述第二消息中携带的信息未遭受篡改的情况下，所述第一终端设备至少根据所述第一随机数、所述第一密钥和所述第二随机数生成所述第二密钥，所述第一终端设备根据所述第二密钥生成完整性保护密钥和/或机密性保护密钥，以及所述第一终端设备将所述M个比特位和所述N个比特位合并得到所述第一密钥的标识，所述第一终端设备生成所述第二密钥的标识的y个比特位，并将所述x个比特位和所述y个比特位合并得到所述第二密钥的标识；

在所述第二消息验证码有效的情况下，所述第一终端设备根据所述第二终端设备选取的安全算法、所述第二密钥、基于所述第二密钥生成完整性保护密钥和/或机密性保护密钥、所述第二终端设备选取的安全策略，与所述第二终端设备进行通信。

9、如权利要求7或8所述的方法，其特征在于，

所述完整性保护密钥的输入参数包括以下至少之一：所述第二密钥，选定的算法类型标识符，选定的算法类型标识符的长度，完整性保护算法标识，完整性保护算法标识的长度；和/或，

所述机密性保护密钥的输入参数包括以下至少之一：所述第二密钥，选定的算法类型标识符，选定的算法类型标识符的长度，机密性保护算法标识，机密性保护算法标识的长度。

10、如权利要求5或7所述的方法，其特征在于，

所述第一消息为认证响应消息，所述第二消息为安全模式命令消息。

11、如权利要求6或8所述的方法，其特征在于，

所述第一消息为安全模式命令消息，所述第二消息为安全模式响应消息。

12、如权利要求7至9中任一项所述的方法，其特征在于，所述方法还包括：

所述第一终端设备通过所述中继设备向所述第二终端设备发送第三消息；

其中，所述第三消息用于指示安全模式建立完成，所述第三消息通过目标密钥进行加密，且所述第三消息包括以下至少之一：所述第二密钥的标识的所述y个比特位，第三消息验证码；

其中，所述目标密钥包括以下之一：所述第一密钥，所述第二密钥，所述第二密钥派生的机密性保护密钥；

其中，所述第三消息通过基于所述第二密钥生成的所述第三消息验证码进行完整性保护，或者，所述第三消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第三消息验证码进行完整性保护，所述第三消息验证码的输入参数包括所述y个比特位。

13、如权利要求4所述的方法，其特征在于，所述方法还包括：

所述第一终端设备接收所述第二终端设备通过所述中继设备发送的错误消息；其中，所述错误消息包括以下至少之一：原因信息，第四消息验证码；其中，所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全策略冲突，或者，所述原因信息用于指示所述第一消息验证码验证失败，或者，所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全算法协商失败；所述第四消息验证码的输入参数包括以下至少之一：所述原因信息；

在所述第四消息验证码有效的情况下，所述第一终端设备确定安全模式建立失败，和/或，所述第一终端设备重新发起安全模式建立流程。

14、如权利要求4至13中任一项所述的方法，其特征在于，

所述完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥；和/或，

所述机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

15、一种中继通信的方法，其特征在于，包括：

第二终端设备通过中继设备向第一终端设备发送认证请求消息；

其中，所述认证请求消息包括以下至少之一：所述第二终端设备所属用户的信息，所述第二终端设备生成的第一临时公钥，所述第二终端设备的签名，所述中继设备的相关信息；

其中,所述第二终端设备所属用户的信息包括所述第二终端设备的标识和所述第二终端设备的公共验证令牌 PVT 和密钥管理服务服务器的公共认证密钥 KPAK;所述第二终端设备的签名的输入参数包括以下至少之一:所述第二终端设备所属用户的信息和所述第一临时公钥;所述第一临时公钥和所述中继设备的相关信息用于所述第一终端设备派生第一密钥;所述中继设备的相关信息包括以下之一:所述中继设备的身份信息,所述中继设备生成的随机数,所述中继设备生成的计数器。

16、如权利要求 15 所述的方法,其特征在于,

所述第二终端设备的签名由所述第二终端设备的秘密签名密钥生成。

17、如权利要求 15 或 16 所述的方法,其特征在于,所述方法还包括:

所述第二终端设备接收所述第一终端设备通过所述中继设备发送的第一消息;

其中,所述第一消息包括以下至少之一:所述第一终端设备的安全能力信息,所述第一终端设备的安全策略信息,所述第一终端设备所属用户的信息,所述中继设备所属用户的信息,所述第一终端设备生成的第一随机数,所述第一终端设备生成的第二临时公钥,所述第一终端设备生成的所述第一密钥的标识的 M 个比特位,所述第一终端设备的签名,所述中继设备的签名,第一消息验证码;

其中,所述第一终端设备所属用户的信息包括所述第一终端设备的标识和所述第一终端设备的 PVT 和 KPAK;所述中继设备所属用户的信息包括所述中继设备的标识和所述中继设备的 PVT 和 KPAK;所述第一终端设备的签名的输入参数包括以下至少之一:所述第一终端设备所属用户的信息,所述第二临时公钥,所述 M 个比特位,所述第二终端设备的签名;所述中继设备的签名的输入参数包括以下至少之一:所述中继设备所属用户的信息,所述第一终端设备的签名,所述第二终端设备的签名,所述第一消息;

其中,所述第一消息通过基于所述第一密钥生成的所述第一消息验证码进行完整性保护,且所述第一消息验证码的输入参数包括以下至少之一:所述第一终端设备的安全能力信息,所述第一终端设备的安全策略信息,所述第一终端设备所属用户的信息,所述第一随机数,所述第二临时公钥,所述 M 个比特位,所述第一终端设备的签名;

其中,所述第二临时公钥和所述中继设备的相关信息用于所述第二终端设备派生所述第一密钥,所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥,所述第二密钥用于派生完整性保护密钥和/或机密性保护密钥,所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数。

18、如权利要求 17 所述的方法,其特征在于,

所述第一终端设备的签名由所述第一终端设备的秘密签名密钥生成,和/或,所述中继设备的签名由所述中继设备的秘密签名密钥生成。

19、如权利要求 17 或 18 所述的方法,其特征在于,所述方法还包括:

所述第二终端设备分别检查所述第一终端设备的 KPAK 和所述中继设备的 KPAK,在所述第一终端设备的 KPAK 和所述中继设备的 KPAK 有效的情况下,且基于所述第一终端设备的标识和所述第一终端设备的 PVT 对所述第一终端设备的签名进行验证,以及基于所述中继设备的标识和所述中继设备的 PVT 对所述中继设备的签名进行验证;

在所述第一终端设备的签名和所述中继设备的签名验证成功,且所述第一消息中携带的信息未遭受篡改的情况下,所述第二终端设备生成第二随机数,所述第二终端设备至少根据所述第一随机数、所述第一密钥和所述第二随机数生成所述第二密钥,所述第二终端设备根据所述第二密钥生成完整性保护密钥和/或机密性保护密钥,以及所述第二终端设备生成所述第一密钥的标识的 N 个比特位,并将所述 M 个比特位和所述 N 个比特位合并得到所述第一密钥的标识;

在所述第一消息验证码有效的情况下,所述第二终端设备通过所述中继设备向所述第一终端设备发送第二消息;其中,所述第二消息包括以下至少之一:所述第二随机数,所述 N 个比特位,所述第二终端设备生成的所述第二密钥的标识的 x 个比特位,所述第二终端设备选取的安全算法,所述第二终端设备选取的安全策略,第二消息验证码;

其中,所述第二消息通过基于所述第二密钥生成的所述第二消息验证码进行完整性保护,或者,所述第二消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第二消息验证码进行完整性保护,且所述第二消息验证码的输入参数包括以下至少之一:所述第二随机数,所述 N 个比特位,所述 x 个比特位,所述第二终端设备选取的安全算法,所述第二终端设备选取的安全策略;其中,所述第二密钥的标识由所述 x 个比特位与所述第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

20、如权利要求 19 所述的方法,其特征在于,

所述第二消息通过所述第一密钥进行加密。

21、如权利要求 19 所述的方法，其特征在于，
所述第一消息为认证响应消息，所述第二消息为安全模式命令消息。

22、如权利要求 20 所述的方法，其特征在于，
所述第一消息为安全模式命令消息，所述第二消息为安全模式响应消息。

23、如权利要求 19 至 22 中任一项所述的方法，其特征在于，
所述完整性保护密钥的输入参数包括以下至少之一：所述第二密钥，选定的算法类型标识符，选定的算法类型标识符的长度，完整性保护算法标识，完整性保护算法标识的长度；和/或，
所述机密性保护密钥的输入参数包括以下至少之一：所述第二密钥，选定的算法类型标识符，选定的算法类型标识符的长度，机密性保护算法标识，机密性保护算法标识的长度。

24、如权利要求 19 至 23 中任一项所述的方法，其特征在于，所述方法还包括：
所述第二终端设备接收所述第一终端设备通过所述中继设备发送的第三消息；
其中，所述第三消息用于指示安全模式建立完成，所述第三消息通过目标密钥进行加密，且所述第三消息包括以下至少之一：所述第一终端设备生成的所述第二密钥的标识的 y 个比特位，第三消息验证码；

其中，所述目标密钥包括以下之一：所述第一密钥，所述第二密钥，所述第二密钥派生的机密性保护密钥；

其中，所述第三消息通过基于所述第二密钥生成的所述第三消息验证码进行完整性保护，或者，所述第三消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第三消息验证码进行完整性保护，所述第三消息验证码的输入参数包括所述 y 个比特位。

25、如权利要求 24 所述的方法，其特征在于，所述方法还包括：
所述第二终端设备通过所述目标密钥对所述第三消息进行解密；
在所述第三消息中携带的信息未遭受篡改的情况下，且所述第三消息验证码有效的情况下，所述第二终端设备将所述 x 个比特位与所述 y 个比特位合并得到所述第二密钥的标识。

26、如权利要求 17 或 18 所述的方法，其特征在于，所述方法还包括：
所述第二终端设备通过所述中继设备向所述第一终端设备发送错误消息；其中，所述错误消息包括以下至少之一：原因信息，第四消息验证码；其中，所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全策略冲突，或者，所述原因信息用于指示所述第一消息验证码验证失败，或者，所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全算法协商失败；所述第四消息验证码的输入参数包括以下至少之一：所述原因信息。

27、如权利要求 17 至 26 中任一项所述的方法，其特征在于，
所述完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥；和/或，
所述机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

28、一种中继通信的方法，其特征在于，包括：
中继设备接收第二终端设备发送的认证请求消息；其中，所述认证请求消息包括以下至少之一：
所述第二终端设备所属用户的信息，所述第二终端设备生成的第一临时公钥，所述第二终端设备的签名；其中，所述第二终端设备所属用户的信息包括所述第二终端设备的标识和所述第二终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK；所述第二终端设备的签名的输入参数包括以下至少之一：所述第二终端设备所属用户的信息和所述第一临时公钥；

在所述第二终端设备的 KPAK 有效，且基于所述第二终端设备的标识和所述第二终端设备的 PVT 对所述第二终端设备的签名验证成功的情况下，所述中继设备向第一终端设备发送验证之后的认证请求消息；其中，所述验证之后的认证请求消息包括以下至少之一：所述第二终端设备所属用户的信息，所述中继设备所属用户的信息，所述第一临时公钥，所述第二终端设备的签名，所述中继设备的签名，所述中继设备的相关信息；其中，所述中继设备所属用户的信息包括所述中继设备的标识和所述中继设备的 PVT 和 KPAK；所述中继设备的签名的输入参数包括以下至少之一：所述第二终端设备的签名和所述中继设备所属用户的信息；其中，所述第一临时公钥和所述中继设备的相关信息用于所述第一终端设备派生第一密钥；所述中继设备的相关信息包括以下之一：所述中继设备的身份信息，所述中继设备生成的随机数，所述中继设备生成的计数器。

29、如权利要求 28 所述的方法，其特征在于，
所述第二终端设备的签名由所述第二终端设备的秘密签名密钥生成，和/或，所述中继设备的签名由所述中继设备的秘密签名密钥生成。

30、如权利要求 28 或 29 所述的方法，其特征在于，所述方法还包括：
所述中继设备接收所述第一终端设备发送的第一消息；其中，所述第一消息包括以下至少之一：

所述第一终端设备的安全能力信息,所述第一终端设备的安全策略信息,所述第一终端设备所属用户的信息,所述第一终端设备生成的第一随机数,所述第一终端设备生成的第二临时公钥,所述第一终端设备生成的所述第一密钥的标识的 M 个比特位,所述第一终端设备的签名,第一消息验证码;其中,所述第一终端设备所属用户的信息包括所述第一终端设备的标识和所述第一终端设备的 PVT 和 KPAK;所述第一终端设备的签名的输入参数包括以下至少之一:所述第一终端设备所属用户的信息,所述第二临时公钥,所述 M 个比特位,所述第二终端设备的签名;其中,所述第一消息通过基于所述第一密钥生成的所述第一消息验证码进行完整性保护,且所述第一消息验证码的输入参数包括以下至少之一:所述第一终端设备的安全能力信息,所述第一终端设备的安全策略信息,所述第一终端设备所属用户的信息,所述第一随机数,所述第二临时公钥,所述 M 个比特位,所述第一终端设备的签名;

在所述第一终端设备的 KPAK 有效,且基于所述第一终端设备的标识和所述第一终端设备的 PVT 对所述第一终端设备的签名验证成功的情况下,所述中继设备向所述第二终端设备发送验证之后的第一消息;其中,所述验证之后的第一消息包括以下至少之一:所述第一终端设备的安全能力信息,所述第一终端设备的安全策略信息,所述第一终端设备所属用户的信息,所述中继设备所属用户的信息,所述第一终端设备生成的第一随机数,所述第一终端设备生成的与所述第二临时私钥配对的第二临时公钥,所述第一终端设备生成的所述第一密钥的标识的 M 个比特位,所述第一终端设备的签名,所述中继设备的签名,所述第一消息验证码;其中,所述中继设备所属用户的信息包括所述中继设备的标识和所述中继设备的 PVT 和 KPAK;所述中继设备的签名的输入参数包括以下至少之一:所述中继设备所属用户的信息,所述第一终端设备的签名,所述第二终端设备的签名,所述验证之后的第一消息;

其中,所述第二临时公钥和所述中继设备的相关信息用于所述第二终端设备派生所述第一密钥,所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥,所述第二密钥用于派生完整性保护密钥和/或机密性保护密钥,所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数。

31、如权利要求 30 所述的方法,其特征在于,所述方法还包括:

所述中继设备将所述第二终端设备发送的第二消息转发至所述第一终端设备;

其中,所述第二消息包括以下至少之一:所述第二终端设备生成的所述第二随机数,所述第二终端设备生成的所述第一密钥的标识的 N 个比特位,所述第二终端设备生成的所述第二密钥的标识的 x 个比特位,所述第二终端设备选取的安全算法,所述第二终端设备选取的安全策略,第二消息验证码;

其中,所述第二消息通过基于所述第二密钥生成的所述第二消息验证码进行完整性保护,或者,所述第二消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第二消息验证码进行完整性保护,且所述第二消息验证码的输入参数包括以下至少之一:所述第二随机数,所述 N 个比特位,所述 x 个比特位,所述第二终端设备选取的安全算法,所述第二终端设备选取的安全策略;其中,所述第二密钥的标识由所述 x 个比特位与所述第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

32、如权利要求 31 所述的方法,其特征在于,

所述第二消息通过所述第一密钥进行加密,或者,所述第二消息不用于所述第一密钥进行加密。

33、如权利要求 31 所述的方法,其特征在于,

所述第一消息为认证响应消息,所述第二消息为安全模式命令消息。

34、如权利要求 32 所述的方法,其特征在于,

所述第一消息为安全模式命令消息,所述第二消息为安全模式响应消息。

35、如权利要求 30 至 34 中任一项所述的方法,其特征在于,所述方法还包括:

所述中继设备将所述第一终端设备发送的第三消息转发至所述第二终端设备;

其中,所述第三消息用于指示安全模式建立完成,所述第三消息通过目标密钥进行加密,且所述第三消息包括以下至少之一:所述第一终端设备生成的所述第二密钥的标识的 y 个比特位,第三消息验证码;

其中,所述目标密钥包括以下之一:所述第一密钥,所述第二密钥,所述第二密钥派生的机密性保护密钥;

其中,所述第三消息通过基于所述第二密钥生成的所述第三消息验证码进行完整性保护,或者,所述第三消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第三消息验证码进行完整性保护,所述第三消息验证码的输入参数包括所述 y 个比特位。

36、如权利要求 30 所述的方法,其特征在于,所述方法还包括:

所述中继设备将所述第二终端设备发送的错误消息转发至所述第一终端设备；其中，所述错误消息包括以下至少之一：原因信息，第四消息验证码；其中，所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全策略冲突，或者，所述原因信息用于指示所述第一消息验证码验证失败，或者，所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全算法协商失败；所述第四消息验证码的输入参数包括以下至少之一：所述原因信息。

37、如权利要求 30 至 35 中任一项所述的方法，其特征在于，
所述完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥；和/或，
所述机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

38、一种中继通信的方法，其特征在于，包括：

第一终端设备通过中继设备向第二终端设备发送第一消息；

其中，所述第一消息包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安全策略信息，所述第一终端设备所属用户的信息，所述第一终端设备生成的第一随机数，所述第一终端设备生成的第二临时公钥，所述第一终端设备生成的第一密钥的标识的 M 个比特位，所述第一终端设备的签名，第一消息验证码；

其中，所述第一终端设备所属用户的信息包括所述第一终端设备的标识和所述第一终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK；所述第一终端设备的签名的输入参数包括以下至少之一：所述第一终端设备所属用户的信息，所述第二临时公钥，所述 M 个比特位，所述第二终端设备的签名；

其中，所述第一消息通过基于所述第一密钥生成的所述第一消息验证码进行完整性保护，且所述第一消息验证码的输入参数包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安全策略信息，所述第一终端设备所属用户的信息，所述第一随机数，所述第二临时公钥，所述 M 个比特位，所述第一终端设备的签名；

其中，所述第二临时公钥和所述中继设备的相关信息用于所述第二终端设备派生所述第一密钥，所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥，所述第二密钥用于派生完整性保护密钥和/或机密性保护密钥，所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数；

其中，所述中继设备的相关信息包括以下之一：所述中继设备的身份信息，所述中继设备生成的随机数，所述中继设备生成的计数器。

39、如权利要求 38 所述的方法，其特征在于，所述方法还包括：

所述第一终端设备接收所述第二终端设备通过所述中继设备发送的第二消息；

其中，所述第二消息包括以下至少之一：所述第二终端设备生成的所述第二随机数，所述第二终端设备生成的所述第一密钥的标识的 N 个比特位，所述第二终端设备生成的所述第二密钥的标识的 x 个比特位，所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略，第二消息验证码；

其中，所述第二消息通过基于所述第二密钥生成的所述第二消息验证码进行完整性保护，或者，所述第二消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第二消息验证码进行完整性保护，且所述第二消息验证码的输入参数包括以下至少之一：所述第二随机数，所述 N 个比特位，所述 x 个比特位，所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略；其中，所述第二密钥的标识由所述 x 个比特位与所述第二密钥的标识的另外 y 个比特位合并得到，x 和 y 均为正整数。

40、如权利要求 39 所述的方法，其特征在于，

所述第二消息通过所述第一密钥进行加密，或者，所述第二消息不用于所述第一密钥进行加密。

41、如权利要求 39 所述的方法，其特征在于，所述方法还包括：

在所述第二消息中携带的信息未遭受篡改的情况下，所述第一终端设备至少根据所述第一随机数、所述第一密钥和所述第二随机数生成所述第二密钥，所述第一终端设备根据所述第二密钥生成完整性保护密钥和/或机密性保护密钥，以及所述第一终端设备将所述 M 个比特位和所述 N 个比特位合并得到所述第一密钥的标识，所述第一终端设备生成所述第二密钥的标识的 y 个比特位，并将所述 x 个比特位和所述 y 个比特位合并得到所述第二密钥的标识；

在所述第二消息验证码有效的情况下，所述第一终端设备根据所述第二终端设备选取的安全算法、所述第二密钥、基于所述第二密钥生成完整性保护密钥和/或机密性保护密钥、所述第二终端设备选取的安全策略，与所述第二终端设备进行通信。

42、如权利要求 40 所述的方法，其特征在于，所述方法还包括：

所述第一终端设备根据所述第一密钥解密所述第二消息；

在所述第二消息中携带的信息未遭受篡改的情况下,所述第一终端设备至少根据所述第一随机数、所述第一密钥和所述第二随机数生成所述第二密钥,所述第一终端设备根据所述第二密钥生成完整性保护密钥和/或机密性保护密钥,以及所述第一终端设备将所述M个比特位和所述N个比特位合并得到所述第一密钥的标识,所述第一终端设备生成所述第二密钥的标识的y个比特位,并将所述x个比特位和所述y个比特位合并得到所述第二密钥的标识;

在所述第二消息验证码有效的情况下,所述第一终端设备根据所述第二终端设备选取的安全算法、所述第二密钥、基于所述第二密钥生成完整性保护密钥和/或机密性保护密钥、所述第二终端设备选取的安全策略,与所述第二终端设备进行通信。

43、如权利要求41或42所述的方法,其特征在于,

所述完整性保护密钥的输入参数包括以下至少之一:所述第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,

所述机密性保护密钥的输入参数包括以下至少之一:所述第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

44、如权利要求39或41所述的方法,其特征在于,

所述第一消息为认证响应消息,所述第二消息为安全模式命令消息。

45、如权利要求40或42所述的方法,其特征在于,

所述第一消息为安全模式命令消息,所述第二消息为安全模式响应消息。

46、如权利要求41至43中任一项所述的方法,其特征在于,所述方法还包括:

所述第一终端设备通过所述中继设备向所述第二终端设备发送第三消息;

其中,所述第三消息用于指示安全模式建立完成,所述第三消息通过目标密钥进行加密,且所述第三消息包括以下至少之一:所述第二密钥的标识的所述y个比特位,第三消息验证码;

其中,所述目标密钥包括以下之一:所述第一密钥,所述第二密钥,所述第二密钥派生的机密性保护密钥;

其中,所述第三消息通过基于所述第二密钥生成的所述第三消息验证码进行完整性保护,或者,所述第三消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第三消息验证码进行完整性保护,所述第三消息验证码的输入参数包括所述y个比特位。

47、如权利要求38所述的方法,其特征在于,所述方法还包括:

所述第一终端设备接收所述第二终端设备通过所述中继设备发送的错误消息;其中,所述错误消息包括以下至少之一:原因信息,第四消息验证码;其中,所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全策略冲突,或者,所述原因信息用于指示所述第一消息验证码验证失败,或者,所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全算法协商失败,所述第四消息验证码的输入参数包括以下至少之一:所述原因信息;

在所述第四消息验证码有效的情况下,所述第一终端设备确定安全模式建立失败,和/或,所述第一终端设备重新发起安全模式建立流程。

48、如权利要求38至47中任一项所述的方法,其特征在于,

所述完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥;和/或,

所述机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

49、如权利要求38至48中任一项所述的方法,其特征在于,所述方法还包括:

所述第一终端设备接收所述第二终端设备通过所述中继设备发送的认证请求消息;

其中,所述认证请求消息包括以下至少之一:所述第二终端设备所属用户的信息,所述中继设备所属用户的信息,所述第二终端设备生成的第一临时公钥,所述第二终端设备的签名,所述中继设备的签名,所述中继设备的相关信息;

其中,所述第二终端设备所属用户的信息包括所述第二终端设备的标识和所述第二终端设备的公共验证令牌PVT和密钥管理服务服务器的公共认证密钥KPAK;所述中继设备所属用户的信息包括所述中继设备的标识和所述中继设备的PVT和KPAK;所述第二终端设备的签名的输入参数包括以下至少之一:所述第二终端设备所属用户的信息和所述第一临时公钥;所述中继设备的签名的输入参数包括以下至少之一:所述第二终端设备的签名和所述中继设备所属用户的信息;所述第一临时公钥和所述中继设备的相关信息用于所述第一终端设备派生所述第一密钥。

50、如权利要求49所述的方法,其特征在于,

所述第二终端设备的签名由所述第二终端设备的秘密签名密钥生成,和/或,所述中继设备的签名由所述中继设备的秘密签名密钥生成。

51、如权利要求49或50所述的方法,其特征在于,所述方法还包括:

在所述第二终端设备的 KPAK 和所述中继设备的 KPAK 有效, 且基于所述第二终端设备的标识和所述第二终端设备的 PVT 对所述第二终端设备的签名验证成功, 以及基于所述中继设备的标识和所述中继设备的 PVT 对所述中继设备的签名验证成功的情况下, 所述第一终端设备生成与所述第二临时公钥配对的第二临时私钥, 以及所述第一终端设备根据所述第一临时公钥、所述中继设备的相关信息和所述第二临时私钥派生所述第一密钥。

52、一种中继通信的方法, 其特征在于, 包括:

第二终端设备接收第一终端设备通过中继设备发送的第一消息;

其中, 所述第一消息包括以下至少之一: 所述第一终端设备的安全能力信息, 所述第一终端设备的安全策略信息, 所述第一终端设备所属用户的信息, 所述中继设备所属用户的信息, 所述第一终端设备生成的第一随机数, 所述第一终端设备生成的第二临时公钥, 所述第一终端设备生成的第一密钥的标识的 M 个比特位, 所述第一终端设备的签名, 所述中继设备的签名, 第一消息验证码;

其中, 所述第一终端设备所属用户的信息包括所述第一终端设备的标识和所述第一终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK; 所述中继设备所属用户的信息包括所述中继设备的标识和所述中继设备的 PVT 和 KPAK; 所述第一终端设备的签名的输入参数包括以下至少之一: 所述第一终端设备所属用户的信息, 所述第二临时公钥, 所述 M 个比特位, 所述第二终端设备的签名; 所述中继设备的签名的输入参数包括以下至少之一: 所述中继设备所属用户的信息, 所述第一终端设备的签名, 所述第二终端设备的签名, 所述第一消息;

其中, 所述第一消息通过基于所述第一密钥生成的所述第一消息验证码进行完整性保护, 且所述第一消息验证码的输入参数包括以下至少之一: 所述第一终端设备的安全能力信息, 所述第一终端设备的安全策略信息, 所述第一终端设备所属用户的信息, 所述第一随机数, 所述第二临时公钥, 所述 M 个比特位, 所述第一终端设备的签名;

其中, 所述第二临时公钥和所述中继设备的相关信息用于所述第二终端设备派生所述第一密钥, 所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥, 所述第二密钥用于派生完整性保护密钥和/或机密性保护密钥, 所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数;

其中, 所述中继设备的相关信息包括以下之一: 所述中继设备的身份信息, 所述中继设备生成的随机数, 所述中继设备生成的计数器。

53、如权利要求 52 所述的方法, 其特征在于,

所述第一终端设备的签名由所述第一终端设备的秘密签名密钥生成, 和/或, 所述中继设备的签名由所述中继设备的秘密签名密钥生成。

54、如权利要求 52 或 53 所述的方法, 其特征在于, 所述方法还包括:

所述第二终端设备分别检查所述第一终端设备的 KPAK 和所述中继设备的 KPAK, 在所述第一终端设备的 KPAK 和所述中继设备的 KPAK 有效的情况下, 且基于所述第一终端设备的标识和所述第一终端设备的 PVT 对所述第一终端设备的签名进行验证, 以及基于所述中继设备的标识和所述中继设备的 PVT 对所述中继设备的签名进行验证;

在所述第一终端设备的签名和所述中继设备的签名验证成功, 且所述第一消息中携带的信息未遭受篡改的情况下, 所述第二终端设备生成第二随机数, 所述第二终端设备至少根据所述第一随机数、所述第一密钥和所述第二随机数生成所述第二密钥, 所述第二终端设备根据所述第二密钥生成完整性保护密钥和/或机密性保护密钥, 以及所述第二终端设备生成所述第一密钥的标识的 N 个比特位, 并将所述 M 个比特位和所述 N 个比特位合并得到所述第一密钥的标识;

在所述第一消息验证码有效的情况下, 所述第二终端设备通过所述中继设备向所述第一终端设备发送第二消息; 其中, 所述第二消息包括以下至少之一: 所述第二随机数, 所述 N 个比特位, 所述第二终端设备生成的所述第二密钥的标识的 x 个比特位, 所述第二终端设备选取的安全算法, 所述第二终端设备选取的安全策略, 第二消息验证码;

其中, 所述第二消息通过基于所述第二密钥生成的所述第二消息验证码进行完整性保护, 或者, 所述第二消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第二消息验证码进行完整性保护, 且所述第二消息验证码的输入参数包括以下至少之一: 所述第二随机数, 所述 N 个比特位, 所述 x 个比特位, 所述第二终端设备选取的安全算法, 所述第二终端设备选取的安全策略; 其中, 所述第二密钥的标识由所述 x 个比特位与所述第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

55、如权利要求 54 所述的方法, 其特征在于,

所述第二消息通过所述第一密钥进行加密, 或者, 所述第二消息不用于所述第一密钥进行加密。

56、如权利要求 54 所述的方法，其特征在于，
所述第一消息为认证响应消息，所述第二消息为安全模式命令消息。

57、如权利要求 55 所述的方法，其特征在于，
所述第一消息为安全模式命令消息，所述第二消息为安全模式响应消息。

58、如权利要求 54 至 57 中任一项所述的方法，其特征在于，
所述完整性保护密钥的输入参数包括以下至少之一：所述第二密钥，选定的算法类型标识符，选定的算法类型标识符的长度，完整性保护算法标识，完整性保护算法标识的长度；和/或，
所述机密性保护密钥的输入参数包括以下至少之一：所述第二密钥，选定的算法类型标识符，选定的算法类型标识符的长度，机密性保护算法标识，机密性保护算法标识的长度。

59、如权利要求 54 至 58 中任一项所述的方法，其特征在于，所述方法还包括：
所述第二终端设备接收所述第一终端设备通过所述中继设备发送的第三消息；
其中，所述第三消息用于指示安全模式建立完成，所述第三消息通过目标密钥进行加密，且所述第三消息包括以下至少之一：所述第一终端设备生成的所述第二密钥的标识的 y 个比特位，第三消息验证码；

其中，所述目标密钥包括以下之一：所述第一密钥，所述第二密钥，所述第二密钥派生的机密性保护密钥；

其中，所述第三消息通过基于所述第二密钥生成的所述第三消息验证码进行完整性保护，或者，所述第三消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第三消息验证码进行完整性保护，所述第三消息验证码的输入参数包括所述 y 个比特位。

60、如权利要求 59 所述的方法，其特征在于，所述方法还包括：
所述第二终端设备通过所述目标密钥对所述第三消息进行解密；
在所述第三消息中携带的信息未遭受篡改的情况下，且所述第三消息验证码有效的情况下，所述第二终端设备将所述 x 个比特位与所述 y 个比特位合并得到所述第二密钥的标识。

61、如权利要求 52 或 53 所述的方法，其特征在于，所述方法还包括：
所述第二终端设备通过所述中继设备向所述第一终端设备发送错误消息；其中，所述错误消息包括以下至少之一：原因信息，第四消息验证码；其中，所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全策略冲突，或者，所述原因信息用于指示所述第一消息验证码验证失败，或者，所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全算法协商失败，所述第四消息验证码的输入参数包括以下至少之一：所述原因信息。

62、如权利要求 52 至 61 中任一项所述的方法，其特征在于，
所述完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥；和/或，
所述机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

63、如权利要求 52 至 62 中任一项所述的方法，其特征在于，所述方法还包括：
所述第二终端设备通过所述中继设备向所述第一终端设备发送认证请求消息；
其中，所述认证请求消息包括以下至少之一：所述第二终端设备所属用户的信息，所述第二终端设备生成的第一临时公钥，所述第二终端设备的签名，所述中继设备的相关信息；

其中，所述第二终端设备所属用户的信息包括所述第二终端设备的标识和所述第二终端设备的 PVT 和 KPAK；所述第二终端设备的签名的输入参数包括以下至少之一：所述第二终端设备所属用户的信息和所述第一临时公钥；所述第一临时公钥和所述中继设备的相关信息用于所述第一终端设备派生第一密钥。

64、如权利要求 63 所述的方法，其特征在于，
所述第二终端设备的签名由所述第二终端设备的秘密签名密钥生成。

65、一种中继通信的方法，其特征在于，包括：
中继设备接收第一终端设备发送的第一消息；其中，所述第一消息包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安全策略信息，所述第一终端设备所属用户的信息，所述第一终端设备生成的第一随机数，所述第一终端设备生成的第二临时公钥，所述第一终端设备生成的第一密钥的标识的 M 个比特位，所述第一终端设备的签名，第一消息验证码；其中，所述第一终端设备所属用户的信息包括所述第一终端设备的标识和所述第一终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK；所述第一终端设备的签名的输入参数包括以下至少之一：所述第一终端设备所属用户的信息，所述第二临时公钥，所述 M 个比特位，第二终端设备的签名；其中，所述第一消息通过基于所述第一密钥生成的所述第一消息验证码进行完整性保护，且所述第一消息验证码的输入参数包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安

全策略信息, 所述第一终端设备所属用户的信息, 所述第一随机数, 所述第二临时公钥, 所述 M 个比特位, 所述第一终端设备的签名;

5 在所述第一终端设备的 KPAK 有效, 且基于所述第一终端设备的标识和所述第一终端设备的 PVT 对所述第一终端设备的签名验证成功的情况下, 所述中继设备向所述第二终端设备发送验证之后的第一消息; 其中, 所述验证之后的第一消息包括以下至少之一: 所述第一终端设备的安全能力信息, 所述
10 所述第一终端设备的安全策略信息, 所述第一终端设备所属用户的信息, 所述中继设备所属用户的信息, 所述第一终端设备生成的第一随机数, 所述第一终端设备生成的与所述第二临时私钥配对的第二临时公钥, 所述第一终端设备生成的所述第一密钥的标识的 M 个比特位, 所述第一终端设备的签名, 所述
15 所述中继设备的签名, 所述中继设备的相关信息, 所述第一消息验证码; 其中, 所述中继设备所属用户的信息包括所述中继设备的标识和所述中继设备的 PVT 和 KPAK; 所述中继设备的签名的输入参数包括以下至少之一: 所述中继设备所属用户的信息, 所述第一终端设备的签名, 所述第二终端设备的
20 签名, 所述验证之后的第一消息;

其中, 所述第二临时公钥和所述中继设备的相关信息用于所述第二终端设备派生所述第一密钥, 所述
25 所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥, 所述第二
30 密钥用于派生完整性保护密钥和/或机密性保护密钥, 所述第一密钥的标识由所述 M 个比特位与所述
35 第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数; 其中, 所述中继设备的相关信息
40 包括以下之一: 所述中继设备的身份信息, 所述中继设备生成的随机数, 所述中继设备生成的计数器。

66、如权利要求 65 所述的方法, 其特征在于, 所述方法还包括:

所述中继设备将所述第二终端设备发送的第二消息转发至所述第一终端设备;

20 其中, 所述第二消息包括以下至少之一: 所述第二终端设备生成的所述第二随机数, 所述第二终
25 端设备生成的所述第一密钥的标识的 N 个比特位, 所述第二终端设备生成的所述第二密钥的标识的 x
30 个比特位, 所述第二终端设备选取的安全算法, 所述第二终端设备选取的安全策略, 第二消息验证码;

其中, 所述第二消息通过基于所述第二密钥生成的所述第二消息验证码进行完整性保护, 或者,
35 所述第二消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第二消息验证码进行完整性
40 保护, 且所述第二消息验证码的输入参数包括以下至少之一: 所述第二随机数, 所述 N 个比特位, 所
45 述 x 个比特位, 所述第二终端设备选取的安全算法, 所述第二终端设备选取的安全策略; 其中, 所述
50 第二密钥的标识由所述 x 个比特位与所述第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正
55 整数。

67、如权利要求 66 所述的方法, 其特征在于,

30 所述第二消息通过所述第一密钥进行加密, 或者, 所述第二消息不用于所述第一密钥进行加密。

68、如权利要求 66 所述的方法, 其特征在于,

所述第一消息为认证响应消息, 所述第二消息为安全模式命令消息。

69、如权利要求 67 所述的方法, 其特征在于,

所述第一消息为安全模式命令消息, 所述第二消息为安全模式响应消息。

70、如权利要求 55 至 69 中任一项所述的方法, 其特征在于, 所述方法还包括:

35 所述中继设备将所述第一终端设备发送的第三消息转发至所述第二终端设备;

其中, 所述第三消息用于指示安全模式建立完成, 所述第三消息通过目标密钥进行加密, 且所述
40 第三消息包括以下至少之一: 所述第一终端设备生成的所述第二密钥的标识的 y 个比特位, 第三消息
45 验证码;

40 其中, 所述目标密钥包括以下之一: 所述第一密钥, 所述第二密钥, 所述第二密钥派生的机密性
45 保护密钥;

其中, 所述第三消息通过基于所述第二密钥生成的所述第三消息验证码进行完整性保护, 或者,
50 所述第三消息通过基于所述第二密钥派生的完整性保护密钥生成的所述第三消息验证码进行完整性
55 保护, 所述第三消息验证码的输入参数包括所述 y 个比特位。

71、如权利要求 65 所述的方法, 其特征在于, 所述方法还包括:

所述中继设备将所述第二终端设备发送的错误消息转发至所述第一终端设备; 其中, 所述错误消
50 息包括以下至少之一: 原因信息, 第四消息验证码; 其中, 所述原因信息用于指示所述第二终端设备
55 与所述第一终端设备的安全策略冲突, 或者, 所述原因信息用于指示所述第一消息验证码验证失败,
或者, 所述原因信息用于指示所述第二终端设备与所述第一终端设备的安全算法协商失败, 所述第四
60 消息验证码的输入参数包括以下至少之一: 所述原因信息。

72、如权利要求 65 至 71 中任一项所述的方法, 其特征在于,

所述完整性保护密钥包括控制面的完整性保护密钥和用户面的完整性保护密钥; 和/或,

所述机密性保护密钥包括控制面的机密性保护密钥和用户面的机密性保护密钥。

73、如权利要求 65 至 72 中任一项所述的方法，其特征在于，所述方法还包括：

所述中继设备接收所述第二终端设备发送的认证请求消息；其中，所述认证请求消息包括以下至少之一：所述第二终端设备所属用户的信息，所述第二终端设备生成的第一临时公钥，所述第二终端设备的签名；其中，所述第二终端设备所属用户的信息包括所述第二终端设备的标识和所述第二终端设备的 PVT 和 KPAK；所述第二终端设备的签名的输入参数包括以下至少之一：所述第二终端设备所属用户的信息和所述第一临时公钥；所述第一临时公钥和所述中继设备的相关信息用于所述第一终端设备派生所述第一密钥；

在所述第二终端设备的 KPAK 有效，且基于所述第二终端设备的标识和所述第二终端设备的 PVT 对所述第二终端设备的签名验证成功的情况下，所述中继设备向所述第一终端设备发送验证之后的认证请求消息；其中，所述验证之后的认证请求消息包括以下至少之一：所述第二终端设备所属用户的信息，所述中继设备所属用户的信息，所述第一临时公钥，所述第二终端设备的签名，所述中继设备的签名，所述中继设备的相关信息；其中，所述中继设备所属用户的信息包括所述中继设备的标识和所述中继设备的 PVT 和 KPAK；所述中继设备的签名的输入参数包括以下至少之一：所述第二终端设备的签名和所述中继设备所属用户的信息。

74、如权利要求 73 所述的方法，其特征在于，

所述第二终端设备的签名由所述第二终端设备的秘密签名密钥生成，和/或，所述中继设备的签名由所述中继设备的秘密签名密钥生成。

75、一种中继通信的方法，其特征在于，包括：

第一终端设备通过中继设备向第二终端设备发送直接通信请求；

其中，所述直接通信请求包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安全策略信息，所述第一终端设备生成的第一临时公钥，所述第一终端设备生成的第一随机数；

其中，所述直接通信请求通过第一加密密钥进行加密，以及所述直接通信请求通过第一完整性保护密钥进行完整性保护，所述第一加密密钥为基于已注册并被授权使用终端至终端中继 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥，所述第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥；

其中，所述第一临时公钥和所述中继设备的相关信息用于所述第二终端设备派生第一密钥；所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥，且所述第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥；

其中，所述中继设备的相关信息包括以下之一：所述中继设备的身份信息，所述中继设备生成的随机数，所述中继设备生成的计数器。

76、如权利要求 75 所述的方法，其特征在于，所述方法还包括：

所述第一终端设备接收所述第二终端设备通过所述中继设备发送的安全模式命令；

其中，所述安全模式命令包括以下至少之一：所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略，所述第二终端设备生成的第二临时公钥，所述第二终端设备生成的所述第二随机数，所述第二终端设备生成的所述第一密钥的标识的 M 个比特位，所述中继设备的相关信息，第一消息验证码；

其中，所述安全模式命令通过所述第一加密密钥进行加密，所述安全模式命令通过所述第一完整性保护密钥进行完整性保护，所述第一消息验证码基于所述第二完整性保护密钥生成，且所述第一消息验证码的输入参数包括以下至少之一：所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略，所述第二临时公钥，所述第二随机数，所述 M 个比特位，所述中继设备的相关信息；

其中，所述第二临时公钥和所述中继设备的相关信息用于所述第一终端设备派生所述第一密钥，所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数。

77、如权利要求 76 所述的方法，其特征在于，

在所述第一随机数、所述第一密钥和所述第二随机数用于派生所述第二密钥的情况下，所述安全模式命令还包括所述第二终端设备生成的所述第二密钥的标识的 x 个比特位，以及所述第一消息验证码的输入参数包括所述 x 个比特位；

其中，所述第二密钥的标识由所述 x 个比特位与所述第二密钥的标识的另外 y 个比特位合并得到，x 和 y 均为正整数。

78、如权利要求 77 所述的方法，其特征在于，所述方法还包括：

所述第一终端设备使用所述第一加密密钥解密所述安全模式命令,以及使用所述第一完整性保护密钥判断所述安全模式命令的完整性;

在所述安全模式命令中携带的信息未遭受篡改的情况下,所述第一终端设备根据与所述第一临时公钥配对的第一临时私钥、所述第二临时公钥、所述中继设备的相关信息派生所述第一密钥,且所述第一终端设备生成所述第一密钥的标识的所述 N 个比特位,以及将所述 M 个比特位和所述 N 个比特位合并得到所述第一密钥的标识;

所述第一终端设备至少根据所述第一随机数、所述第一密钥和所述第二随机数生成所述第二密钥,所述第一终端设备根据所述第二密钥生成所述第二完整性保护密钥和/或所述第二加密密钥,以及所述第一终端设备生成所述第二密钥的标识的所述 y 个比特位,并将所述 x 个比特位和所述 y 个比特位合并得到所述第二密钥的标识;

在所述第一消息验证码有效的情况下,所述第一终端设备根据所述第二终端设备选取的安全算法、所述第二完整性保护密钥和/或所述第二加密密钥、所述第二终端设备选取的安全策略,与所述第二终端设备进行通信。

79、如权利要求 78 所述的方法,其特征在于,所述方法还包括:

所述第一终端设备通过所述中继设备向所述第二终端设备发送安全模式建立完成消息;

其中,所述安全模式建立完成消息通过所述第二密钥或所述第二加密密钥进行加密,所述安全模式建立完成消息通过所述第二密钥或所述第二完整性保护密钥进行完整性保护;

其中,所述安全模式建立完成消息至少包括所述第二密钥的标识的所述 y 个比特位。

80、如权利要求 78 或 79 所述的方法,其特征在于,

所述第二完整性保护密钥的输入参数包括以下至少之一:所述第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,

所述第二加密密钥的输入参数包括以下至少之一:所述第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

81、如权利要求 76 所述的方法,其特征在于,在所述第一随机数、所述第一密钥和所述第二随机数用于派生所述第二加密密钥和/或所述第二完整性保护密钥的情况下,所述方法还包括:

所述第一终端设备使用所述第一加密密钥解密所述安全模式命令,以及使用所述第一完整性保护密钥判断所述安全模式命令的完整性;

在所述安全模式命令中携带的信息未遭受篡改的情况下,所述第一终端设备根据与所述第一临时公钥配对的第一临时私钥、所述第二临时公钥、所述中继设备的相关信息派生所述第一密钥,且所述第一终端设备生成所述第一密钥的所述 N 个比特位,以及将所述 M 个比特位和所述 N 个比特位合并得到所述第一密钥的标识;

所述第一终端设备至少根据所述第一随机数、所述第一密钥和所述第二随机数生成所述第二完整性保护密钥和/或所述第二加密密钥;

在所述第一消息验证码有效的情况下,所述第一终端设备根据所述第二终端设备选取的安全算法、所述第二完整性保护密钥和/或所述第二加密密钥、所述第二终端设备选取的安全策略,与所述第二终端设备进行通信。

82、如权利要求 81 所述的方法,其特征在于,所述方法还包括:

所述第一终端设备通过所述中继设备向所述第二终端设备发送安全模式建立完成消息;

其中,所述安全模式建立完成消息通过所述第二加密密钥进行加密,所述安全模式建立完成消息通过所述第二完整性保护密钥进行完整性保护。

83、如权利要求 81 或 82 所述的方法,其特征在于,

所述第二完整性保护密钥的输入参数包括以下至少之一:所述第一随机数,所述第一密钥,所述第二随机数,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,

所述第二加密密钥的输入参数包括以下至少之一:所述第一随机数,所述第一密钥,所述第二随机数,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

84、如权利要求 75 至 83 中任一项所述的方法,其特征在于,所述第一加密密钥为邻近业务加密密钥 PEK,所述第一完整性保护密钥为邻近业务完整性保护密钥 PIK。

85、一种中继通信的方法,其特征在于,包括:

第二终端设备接收第一终端设备通过中继设备发送的直接通信请求;

其中,所述直接通信请求包括以下至少之一:所述第一终端设备的安全能力信息,所述第一终端

设备的安全策略信息,所述第一终端设备生成的第一临时公钥,所述第一终端设备生成的第一随机数,所述中继设备的标识,所述中继设备的相关信息;

其中,所述直接通信请求通过第一加密密钥进行加密,以及所述直接通信请求通过第一完整性保护密钥进行完整性保护,所述第一加密密钥为基于已注册并被授权使用终端至终端中继 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥,所述第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥;

其中,所述中继设备的相关信息包括以下之一:所述中继设备的身份信息,所述中继设备生成的随机数,所述中继设备生成的计数器;所述第一临时公钥和所述中继设备的相关信息用于所述第二终端设备派生第一密钥;所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥,且所述第二密钥用于派生第二加密密钥和/或第二完整性保护密钥,或者,所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

86、如权利要求 85 所述的方法,其特征在于,在所述第一随机数、所述第一密钥和所述第二随机数用于派生所述第二密钥的情况下,所述方法还包括:

所述第二终端设备使用所述第一加密密钥解密所述直接通信请求,以及使用所述第一完整性保护密钥判断所述直接通信请求的完整性;

在所述直接通信请求中携带的信息未遭受篡改的情况下,所述第二终端设备生成第二临时私钥,以及所述第二终端设备根据所述第一临时公钥、所述第二临时私钥和所述中继设备的相关信息派生所述第一密钥,且所述第二终端设备生成所述第一密钥的标识的 M 个比特位;

所述第二终端设备生成所述第二随机数,以及所述第二终端设备至少根据所述第一随机数、所述第一密钥和所述第二随机数生成所述第二密钥,所述第二终端设备根据所述第二密钥生成所述第二完整性保护密钥和/或所述第二加密密钥,且所述第二终端设备生成所述第二密钥的标识的 x 个比特位;

其中,所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数,所述第二密钥的标识由所述 x 个比特位与所述第二密钥的标识的另外 y 个比特位合并得到, x 和 y 均为正整数。

87、如权利要求 86 所述的方法,其特征在于,所述方法还包括:

所述第二终端设备通过所述中继设备向所述第一终端设备发送安全模式命令;

其中,所述安全模式命令包括以下至少之一:所述第二终端设备选取的安全算法,所述第二终端设备选取的安全策略,所述第二终端设备生成的与所述第二临时私钥配对的所述第二临时公钥,所述第二随机数,所述第一密钥的标识的所述 M 个比特位,所述第二密钥的标识的所述 x 个比特位,第一消息验证码;

其中,所述安全模式命令通过所述第一加密密钥进行加密,所述安全模式命令通过所述第一完整性保护密钥进行完整性保护,所述第一消息验证码基于所述第二完整性保护密钥生成,且所述第一消息验证码的输入参数包括以下至少之一:所述第二终端设备选取的安全算法,所述第二终端设备选取的安全策略,所述第二临时公钥,所述第二随机数,所述 M 个比特位,所述 x 个比特位,所述中继设备的相关信息;所述第二临时公钥和所述中继设备的相关信息用于所述第一终端设备派生所述第一密钥。

88、如权利要求 87 所述的方法,其特征在于,所述方法还包括:

所述第二终端设备接收所述第一终端设备通过所述中继设备发送的安全模式建立完成消息;

其中,所述安全模式建立完成消息通过所述第二密钥或所述第二加密密钥进行加密,所述安全模式建立完成消息通过所述第二密钥或所述第二完整性保护密钥进行完整性保护;

其中,所述安全模式建立完成消息至少包括所述第二密钥的标识的所述 y 个比特位。

89、如权利要求 86 至 88 中任一项所述的方法,其特征在于,

所述第二完整性保护密钥的输入参数包括以下至少之一:所述第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,完整性保护算法标识,完整性保护算法标识的长度;和/或,

所述第二加密密钥的输入参数包括以下至少之一:所述第二密钥,选定的算法类型标识符,选定的算法类型标识符的长度,机密性保护算法标识,机密性保护算法标识的长度。

90、如权利要求 85 所述的方法,其特征在于,在所述第一随机数、所述第一密钥和所述第二随机数用于派生所述第二加密密钥和/或所述第二完整性保护密钥的情况下,所述方法还包括:

所述第二终端设备使用所述第一加密密钥解密所述直接通信请求,以及使用所述第一完整性保护密钥判断所述直接通信请求的完整性;

在所述直接通信请求中携带的信息未遭受篡改的情况下,所述第二终端设备生成第二临时私钥,

以及所述第二终端设备根据所述第一临时公钥、所述第二临时私钥和所述中继设备的相关信息派生所述第一密钥，且所述第二终端设备生成所述第一密钥的标识的 M 个比特位；

所述第二终端设备生成所述第二随机数，以及所述第二终端设备至少根据所述第一随机数、所述第一密钥和所述第二随机数生成所述第二完整性保护密钥和/或所述第二加密密钥；

其中，所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数。

91、如权利要求 90 所述的方法，其特征在于，所述方法还包括：

所述第二终端设备通过所述中继设备向所述第一终端设备发送安全模式命令；

其中，所述安全模式命令包括以下至少之一：所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略，所述第二终端设备生成的与所述第二临时私钥配对的所述第二临时公钥，所述第二随机数，所述第一密钥的标识的所述 M 个比特位，第一消息验证码；

其中，所述安全模式命令通过所述第一加密密钥进行加密，所述安全模式命令通过所述第一完整性保护密钥进行完整性保护，所述第一消息验证码基于所述第二完整性保护密钥生成，且所述第一消息验证码的输入参数包括以下至少之一：所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略，所述第二临时公钥，所述第二随机数，所述 M 个比特位；所述第二临时公钥和所述中继设备的相关信息用于所述第一终端设备派生所述第一密钥。

92、如权利要求 91 所述的方法，其特征在于，所述方法还包括：

所述第二终端设备接收所述第一终端设备通过所述中继设备发送的安全模式建立完成消息；

其中，所述安全模式建立完成消息通过所述第二加密密钥进行加密，所述安全模式建立完成消息通过所述第二完整性保护密钥进行完整性保护。

93、如权利要求 90 至 92 中任一项所述的方法，其特征在于，

所述第二完整性保护密钥的输入参数包括以下至少之一：所述第一随机数，所述第一密钥，所述第二随机数，选定的算法类型标识符，选定的算法类型标识符的长度，完整性保护算法标识，完整性保护算法标识的长度；和/或，

所述第二加密密钥的输入参数包括以下至少之一：所述第一随机数，所述第一密钥，所述第二随机数，选定的算法类型标识符，选定的算法类型标识符的长度，机密性保护算法标识，机密性保护算法标识的长度。

94、如权利要求 87 或 91 所述的方法，其特征在于，所述安全模式命令还包括所述中继设备的相关信息，以及所述第一消息验证码的输入参数还包括所述中继设备的相关信息。

95、如权利要求 88 或 92 所述的方法，其特征在于，所述方法还包括：

所述第二终端设备根据所述第二终端设备选取的安全算法、所述第二完整性保护密钥和/或所述第二加密密钥、所述第二终端设备选取的安全策略，与所述第一终端设备进行通信。

96、如权利要求 85 至 95 中任一项所述的方法，其特征在于，所述第一加密密钥为邻近业务加密密钥 PEK，所述第一完整性保护密钥为邻近业务完整性保护密钥 PIK。

97、一种中继通信的方法，其特征在于，包括：

中继设备接收第一终端设备发送的直接通信请求；其中，所述直接通信请求包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安全策略信息，所述第一终端设备生成的所述第一临时公钥，所述第一终端设备生成的所述第一随机数；其中，所述直接通信请求通过所述第一加密密钥进行加密，以及所述直接通信请求通过所述第一完整性保护密钥进行完整性保护，所述第一加密密钥为基于已注册并被授权使用终端至终端中继 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥，所述第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥；

所述中继设备验证是否被配置为转发直接通信请求，在验证通过之后所述中继设备使用所述第一加密密钥解密所述直接通信请求以获取服务质量 QoS 和计费信息，以及所述中继设备使用所述第一完整性保护密钥验证所述直接通信请求的完整性，在验证通过之后所述中继设备在所述直接通信请求中添加所述中继设备的相关信息和所述中继设备的标识，并且所述中继设备使用所述第一加密密钥加密所述直接通信请求，使用所述第一完整性保护密钥保护所述直接通信请求的完整性，并将所述直接通信请求转发至第二终端设备；

其中，所述中继设备的相关信息包括以下之一：所述中继设备的身份信息，所述中继设备生成的随机数，所述中继设备生成的计数器；所述第一临时公钥和所述中继设备的相关信息用于第二终端设备派生第一密钥；所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥，且所述第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，所述第一随机数、

所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

98、如权利要求 97 所述的方法，其特征在于，在所述第一随机数、所述第一密钥和所述第二随机数用于派生所述第二密钥的情况下，所述方法还包括：

所述中继设备接收所述第二终端设备发送的安全模式命令；其中，所述安全模式命令包括以下至少之一：所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略，所述第二终端设备生成的第二临时公钥，所述第二终端设备生成的所述第二随机数，所述第二终端设备生成的所述第一密钥的标识的 M 个比特位，所述第二终端设备生成的所述第二密钥的标识的 x 个比特位，第一消息验证码；其中，所述安全模式命令通过所述第一加密密钥进行加密，所述安全模式命令通过所述第一完整性保护密钥进行完整性保护，所述第一消息验证码基于所述第二完整性保护密钥生成，且所述第一消息验证码的输入参数包括以下至少之一：所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略，所述第二临时公钥，所述第二随机数，所述 M 个比特位，所述 x 个比特位，所述中继设备的相关信息；所述第二临时公钥和所述中继设备的相关信息用于所述第一终端设备派生所述第一密钥；

所述中继设备使用所述第一加密密钥解密所述安全模式命令，以获取 QoS 和计费信息，并在向所述第一终端设备转发所述安全模式命令；

其中，所述第二临时公钥和所述中继设备的相关信息用于所述第一终端设备派生所述第一密钥，所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数，所述第二密钥的标识由所述 x 个比特位与所述第二密钥的标识的另外 y 个比特位合并得到，x 和 y 均为正整数。

99、如权利要求 98 所述的方法，其特征在于，所述方法还包括：

所述中继设备向所述第二终端设备转发所述第一终端设备发送的安全模式建立完成消息；

其中，所述安全模式建立完成消息通过所述第二密钥或所述第二加密密钥进行加密，所述安全模式建立完成消息通过所述第二密钥或所述第二完整性保护密钥进行完整性保护；

其中，所述安全模式建立完成消息至少包括所述第二密钥的标识的所述 y 个比特位。

100、如权利要求 97 所述的方法，其特征在于，在所述第一随机数、所述第一密钥和所述第二随机数用于派生所述第二加密密钥和/或所述第二完整性保护密钥的情况下，所述方法还包括：

所述中继设备接收所述第二终端设备发送的安全模式命令；其中，所述安全模式命令包括以下至少之一：所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略，所述第二终端设备生成的第二临时公钥，所述第二终端设备生成的所述第二随机数，所述第二终端设备生成的所述第一密钥的标识的 M 个比特位，第一消息验证码；其中，所述安全模式命令通过所述第一加密密钥进行加密，所述安全模式命令通过所述第一完整性保护密钥进行完整性保护，所述第一消息验证码基于所述第二完整性保护密钥生成，且所述第一消息验证码的输入参数包括以下至少之一：所述第二终端设备选取的安全算法，所述第二终端设备选取的安全策略，所述第二临时公钥，所述第二随机数，所述 M 个比特位，所述中继设备的相关信息；所述第二临时公钥和所述中继设备的相关信息用于所述第一终端设备派生所述第一密钥；

所述中继设备使用所述第一加密密钥解密所述安全模式命令，以获取 QoS 和计费信息，并在向所述第一终端设备转发所述安全模式命令；

其中，所述第二临时公钥和所述中继设备的相关信息用于所述第一终端设备派生所述第一密钥，所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到，M 和 N 均为正整数。

101、如权利要求 100 所述的方法，其特征在于，所述方法还包括：

所述中继设备向所述第二终端设备转发所述第一终端设备发送的安全模式建立完成消息；

其中，所述安全模式建立完成消息通过所述第二加密密钥进行加密，所述安全模式建立完成消息通过所述第二完整性保护密钥进行完整性保护。

102、如权利要求 98 至 101 中任一项所述的方法，其特征在于，

所述安全模式命令包括所述中继设备的相关信息，以及所述第一消息验证码的输入参数还包括所述中继设备的相关信息；或者，所述中继设备在向所述第一终端设备转发的所述安全模式命令中添加了所述中继设备的相关信息。

103、如权利要求 97 至 102 中任一项所述的方法，其特征在于，所述第一加密密钥为邻近业务加密密钥 PEK，所述第一完整性保护密钥为邻近业务完整性保护密钥 PIK。

104、一种终端设备，其特征在于，所述终端设备为第一终端设备，所述终端设备包括：

通信单元, 用于接收第二终端设备通过中继设备发送的认证请求消息;

其中, 所述认证请求消息包括以下至少之一: 所述第二终端设备所属用户的信息, 所述中继设备所属用户的信息, 所述第二终端设备生成的第一临时公钥, 所述第二终端设备的签名, 所述中继设备的签名, 所述中继设备的相关信息;

5 其中, 所述第二终端设备所属用户的信息包括所述第二终端设备的标识和所述第二终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK; 所述中继设备所属用户的信息包括所述中继设备的标识和所述中继设备的 PVT 和 KPAK; 所述第二终端设备的签名的输入参数包括以下至少之一: 所述第二终端设备所属用户的信息和所述第一临时公钥; 所述中继设备的签名的输入参数包
10 括以下至少之一: 所述第二终端设备的签名和所述中继设备所属用户的信息; 所述第一临时公钥和所述中继设备的相关信息用于所述第一终端设备派生第一密钥; 所述中继设备的相关信息包括以下之一: 所述中继设备的身份信息, 所述中继设备生成的随机数, 所述中继设备生成的计数器。

105、一种终端设备, 其特征在于, 所述终端设备为第二终端设备, 所述终端设备包括:

通信单元, 用于通过中继设备向第一终端设备发送认证请求消息;

15 其中, 所述认证请求消息包括以下至少之一: 所述第二终端设备所属用户的信息, 所述第二终端设备生成的第一临时公钥, 所述第二终端设备的签名, 所述中继设备的相关信息;

其中, 所述第二终端设备所属用户的信息包括所述第二终端设备的标识和所述第二终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK; 所述第二终端设备的签名的输入参数包
20 括以下至少之一: 所述第二终端设备所属用户的信息和所述第一临时公钥; 所述第一临时公钥和所述中继设备的相关信息用于所述第一终端设备派生第一密钥; 所述中继设备的相关信息包括以下之一: 所述中继设备的身份信息, 所述中继设备生成的随机数, 所述中继设备生成的计数器。

106、一种终端设备, 其特征在于, 所述终端设备为中继设备, 所述终端设备包括:

通信单元, 用于接收第二终端设备发送的认证请求消息; 其中, 所述认证请求消息包括以下至少
25 之一: 所述第二终端设备所属用户的信息, 所述第二终端设备生成的第一临时公钥, 所述第二终端设备的签名; 其中, 所述第二终端设备所属用户的信息包括所述第二终端设备的标识和所述第二终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK; 所述第二终端设备的签名的输入
参数包括以下至少之一: 所述第二终端设备所属用户的信息和所述第一临时公钥;

在所述第二终端设备的 KPAK 有效, 且基于所述第二终端设备的标识和所述第二终端设备的 PVT
30 对所述第二终端设备的签名验证成功的情况下, 所述通信单元还用于向第一终端设备发送验证之后的认证请求消息; 其中, 所述验证之后的认证请求消息包括以下至少之一: 所述第二终端设备所属用户的信息, 所述中继设备所属用户的信息, 所述第一临时公钥, 所述第二终端设备的签名, 所述中继设备的签名, 所述中继设备的相关信息; 其中, 所述中继设备所属用户的信息包括所述中继设备的标识
和所述中继设备的 PVT 和 KPAK; 所述中继设备的签名的输入参数包括以下至少之一: 所述第二终端设备的签名和所述中继设备所属用户的信息; 其中, 所述第一临时公钥和所述中继设备的相关信息
35 用于所述第一终端设备派生第一密钥; 所述中继设备的相关信息包括以下之一: 所述中继设备的身份信息, 所述中继设备生成的随机数, 所述中继设备生成的计数器。

107、一种终端设备, 其特征在于, 所述终端设备为第一终端设备, 所述终端设备包括:

通信单元, 用于通过中继设备向第二终端设备发送第一消息;

40 其中, 所述第一消息包括以下至少之一: 所述第一终端设备的安全能力信息, 所述第一终端设备的安全策略信息, 所述第一终端设备所属用户的信息, 所述第一终端设备生成的第一随机数, 所述第一终端设备生成的第二临时公钥, 所述第一终端设备生成的第一密钥的标识的 M 个比特位, 所述第一终端设备的签名, 第一消息验证码;

45 其中, 所述第一终端设备所属用户的信息包括所述第一终端设备的标识和所述第一终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK; 所述第一终端设备的签名的输入参数包括以下至少之一: 所述第一终端设备所属用户的信息, 所述第二临时公钥, 所述 M 个比特位, 所述第二终端设备的签名;

其中, 所述第一消息通过基于所述第一密钥生成的所述第一消息验证码进行完整性保护, 且所述
50 第一消息验证码的输入参数包括以下至少之一: 所述第一终端设备的安全能力信息, 所述第一终端设备的安全策略信息, 所述第一终端设备所属用户的信息, 所述第一随机数, 所述第二临时公钥, 所述 M 个比特位, 所述第一终端设备的签名;

其中, 所述第二临时公钥和所述中继设备的相关信息用于所述第二终端设备派生所述第一密钥,
所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥, 所述第二
密钥用于派生完整性保护密钥和/或机密性保护密钥, 所述第一密钥的标识由所述 M 个比特位与所述

第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数;

其中, 所述中继设备的相关信息包括以下之一: 所述中继设备的身份信息, 所述中继设备生成的随机数, 所述中继设备生成的计数器。

108、一种终端设备, 其特征在于, 所述终端设备为第二终端设备, 所述终端设备包括:

5 通信单元, 用于接收第一终端设备通过中继设备发送的第一消息;

其中, 所述第一消息包括以下至少之一: 所述第一终端设备的安全能力信息, 所述第一终端设备的安全策略信息, 所述第一终端设备所属用户的信息, 所述中继设备所属用户的信息, 所述第一终端设备生成的第一随机数, 所述第一终端设备生成的第二临时公钥, 所述第一终端设备生成的第一密钥的标识的 M 个比特位, 所述第一终端设备的签名, 所述中继设备的签名, 第一消息验证码;

10 其中, 所述第一终端设备所属用户的信息包括所述第一终端设备的标识和所述第一终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK; 所述中继设备所属用户的信息包括所述中继设备的标识和所述中继设备的 PVT 和 KPAK; 所述第一终端设备的签名的输入参数包括以下至少之一: 所述第一终端设备所属用户的信息, 所述第二临时公钥, 所述 M 个比特位, 所述第二终端设备的签名; 所述中继设备的签名的输入参数包括以下至少之一: 所述中继设备所属用户的信息, 所述
15 所述第一终端设备的签名, 所述第二终端设备的签名, 所述第一消息;

其中, 所述第一消息通过基于所述第一密钥生成的所述第一消息验证码进行完整性保护, 且所述第一消息验证码的输入参数包括以下至少之一: 所述第一终端设备的安全能力信息, 所述第一终端设备的安全策略信息, 所述第一终端设备所属用户的信息, 所述第一随机数, 所述第二临时公钥, 所述
20 M 个比特位, 所述第一终端设备的签名;

其中, 所述第二临时公钥和所述中继设备的相关信息用于所述第二终端设备派生所述第一密钥, 所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥, 所述第二
25 密钥用于派生完整性保护密钥和/或机密性保护密钥, 所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数;

其中, 所述中继设备的相关信息包括以下之一: 所述中继设备的身份信息, 所述中继设备生成的
30 随机数, 所述中继设备生成的计数器。

109、一种终端设备, 其特征在于, 所述终端设备为中继设备, 所述终端设备包括:

通信单元, 用于接收第一终端设备发送的第一消息; 其中, 所述第一消息包括以下至少之一: 所述
35 第一终端设备的安全能力信息, 所述第一终端设备的安全策略信息, 所述第一终端设备所属用户的信息, 所述第一终端设备生成的第一随机数, 所述第一终端设备生成的第二临时公钥, 所述第一终端设备生成的第一密钥的标识的 M 个比特位, 所述第一终端设备的签名, 第一消息验证码; 其中, 所述
40 所述第一终端设备所属用户的信息包括所述第一终端设备的标识和所述第一终端设备的公共验证令牌 PVT 和密钥管理服务器的公共认证密钥 KPAK; 所述第一终端设备的签名的输入参数包括以下至少之一: 所述第一终端设备所属用户的信息, 所述第二临时公钥, 所述 M 个比特位, 所述第二终端设备的
45 签名; 其中, 所述第一消息通过基于所述第一密钥生成的所述第一消息验证码进行完整性保护, 且
50 所述第一消息验证码的输入参数包括以下至少之一: 所述第一终端设备的安全能力信息, 所述第一终端设备的安全策略信息, 所述第一终端设备所属用户的信息, 所述第一随机数, 所述第二临时公钥, 所述 M 个比特位, 所述第一终端设备的签名;

在所述第一终端设备的 KPAK 有效, 且基于所述第一终端设备的标识和所述第一终端设备的 PVT
40 对所述第一终端设备的签名验证成功的情况下, 所述通信单元还用于向所述第二终端设备发送验证之
后的第一消息; 其中, 所述验证之后的第一消息包括以下至少之一: 所述第一终端设备的安全能力信息, 所述第一终端设备的安全策略信息, 所述第一终端设备所属用户的信息, 所述中继设备所属用户
5 的信息, 所述第一终端设备生成的第一随机数, 所述第一终端设备生成的与所述第二临时私钥配对的
第二临时公钥, 所述第一终端设备生成的所述第一密钥的标识的 M 个比特位, 所述第一终端设备的
45 签名, 所述中继设备的签名, 所述中继设备的相关信息, 所述第一消息验证码; 其中, 所述中继设备
所属用户的信息包括所述中继设备的标识和所述中继设备的 PVT 和 KPAK; 所述中继设备的签名的
输入参数包括以下至少之一: 所述中继设备所属用户的信息, 所述第一终端设备的签名, 所述第二终
50 端设备的签名, 所述验证之后的第一消息;

其中, 所述第二临时公钥和所述中继设备的相关信息用于所述第二终端设备派生所述第一密钥, 所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥, 所述第二
55 密钥用于派生完整性保护密钥和/或机密性保护密钥, 所述第一密钥的标识由所述 M 个比特位与所述第一密钥的标识的另外 N 个比特位合并得到, M 和 N 均为正整数; 其中, 所述中继设备的相关信息
包括以下之一: 所述中继设备的身份信息, 所述中继设备生成的随机数, 所述中继设备生成的计数器。

110、一种终端设备，其特征在于，所述终端设备为第一终端设备，所述终端设备包括：

通信单元，用于通过中继设备向第二终端设备发送直接通信请求；

其中，所述直接通信请求包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安全策略信息，所述第一终端设备生成的第一临时公钥，所述第一终端设备生成的第一随机数；

其中，所述直接通信请求通过第一加密密钥进行加密，以及所述直接通信请求通过第一完整性保护密钥进行完整性保护，所述第一加密密钥为基于已注册并被授权使用终端至终端中继 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥，所述第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥；

其中，所述第一临时公钥和所述中继设备的相关信息用于所述第二终端设备派生第一密钥；所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥，且所述第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥；

其中，所述中继设备的相关信息包括以下之一：所述中继设备的身份信息，所述中继设备生成的随机数，所述中继设备生成的计数器。

111、一种终端设备，其特征在于，所述终端设备为第二终端设备，所述终端设备包括：

通信单元，用于接收第一终端设备通过中继设备发送的直接通信请求；

其中，所述直接通信请求包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安全策略信息，所述第一终端设备生成的第一临时公钥，所述第一终端设备生成的第一随机数，所述中继设备的标识，所述中继设备的相关信息；

其中，所述直接通信请求通过第一加密密钥进行加密，以及所述直接通信请求通过第一完整性保护密钥进行完整性保护，所述第一加密密钥为基于已注册并被授权使用终端至终端中继 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥，所述第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥；

其中，所述中继设备的相关信息包括以下之一：所述中继设备的身份信息，所述中继设备生成的随机数，所述中继设备生成的计数器；所述第一临时公钥和所述中继设备的相关信息用于所述第二终端设备派生第一密钥；所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥，且所述第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

112、一种终端设备，其特征在于，所述终端设备为中继设备，所述终端设备包括：

通信单元，用于接收第一终端设备发送的直接通信请求；其中，所述直接通信请求包括以下至少之一：所述第一终端设备的安全能力信息，所述第一终端设备的安全策略信息，所述第一终端设备生成的第一临时公钥，所述第一终端设备生成的第一随机数；其中，所述直接通信请求通过第一加密密钥进行加密，以及所述直接通信请求通过第一完整性保护密钥进行完整性保护，所述第一加密密钥为基于已注册并被授权使用终端至终端中继 UE-to-UE relay 通信的终端的对称密钥衍生的加密密钥，所述第一完整性保护密钥为基于已注册并被授权使用 UE-to-UE relay 通信的终端的对称密钥衍生的完整性保护密钥；

处理单元，用于验证是否被配置为转发直接通信请求，在验证通过之后所述处理单元还用于使用所述第一加密密钥解密所述直接通信请求以获取服务质量 QoS 和计费信息，以及所述处理单元还用于使用所述第一完整性保护密钥验证所述直接通信请求的完整性，在验证通过之后所述处理单元还用于在所述直接通信请求中添加所述中继设备的相关信息和所述中继设备的标识，并且所述处理单元还用于使用所述第一加密密钥加密所述直接通信请求，使用所述第一完整性保护密钥保护所述直接通信请求的完整性，所述通信单元还用于并将所述直接通信请求转发至第二终端设备；

其中，所述中继设备的相关信息包括以下之一：所述中继设备的身份信息，所述中继设备生成的随机数，所述中继设备生成的计数器；所述第一临时公钥和所述中继设备的相关信息用于第二终端设备派生第一密钥；所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二密钥，且所述第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，所述第一随机数、所述第一密钥和所述第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

113、一种终端设备，其特征在于，包括：处理器和存储器，所述存储器用于存储计算机程序，所述处理器用于调用并运行所述存储器中存储的计算机程序，使得所述终端设备执行如权利要求 1 至 14 中任一项所述的方法，或者，使得所述终端设备执行如权利要求 15 至 27 中任一项所述的方法，

或者，使得所述终端设备执行如权利要求 28 至 37 中任一项所述的方法，或者，使得所述终端设备执行如权利要求 38 至 51 中任一项所述的方法，或者，使得所述终端设备执行如权利要求 52 至 64 中任一项所述的方法，或者，使得所述终端设备执行如权利要求 65 至 74 中任一项所述的方法，或者，使得所述终端设备执行如权利要求 75 至 84 中任一项所述的方法，或者，使得所述终端设备执行如权利要求 85 至 96 中任一项所述的方法，或者，使得所述终端设备执行如权利要求 97 至 103 中任一项所述的方法。

114、一种芯片，其特征在于，包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有该芯片的设备执行如权利要求 1 至 14 中任一项所述的方法，或者，执行如权利要求 15 至 27 中任一项所述的方法，或者，执行如权利要求 28 至 37 中任一项所述的方法，或者，执行如权利要求 38 至 51 中任一项所述的方法，或者，执行如权利要求 52 至 64 中任一项所述的方法，或者，执行如权利要求 65 至 74 中任一项所述的方法，或者，执行如权利要求 75 至 84 中任一项所述的方法，或者，执行如权利要求 85 至 96 中任一项所述的方法，或者，执行如权利要求 97 至 103 中任一项所述的方法。

115、一种计算机可读存储介质，其特征在于，用于存储计算机程序，所述计算机程序使得计算机执行如权利要求 1 至 14 中任一项所述的方法，或者，执行如权利要求 15 至 27 中任一项所述的方法，或者，执行如权利要求 28 至 37 中任一项所述的方法，或者，执行如权利要求 38 至 51 中任一项所述的方法，或者，执行如权利要求 52 至 64 中任一项所述的方法，或者，执行如权利要求 65 至 74 中任一项所述的方法，或者，执行如权利要求 75 至 84 中任一项所述的方法，或者，执行如权利要求 85 至 96 中任一项所述的方法，或者，执行如权利要求 97 至 103 中任一项所述的方法。

116、一种计算机程序产品，其特征在于，包括计算机程序指令，该计算机程序指令使得计算机执行如权利要求 1 至 14 中任一项所述的方法，或者，执行如权利要求 15 至 27 中任一项所述的方法，或者，执行如权利要求 28 至 37 中任一项所述的方法，或者，执行如权利要求 38 至 51 中任一项所述的方法，或者，执行如权利要求 52 至 64 中任一项所述的方法，或者，执行如权利要求 65 至 74 中任一项所述的方法，或者，执行如权利要求 75 至 84 中任一项所述的方法，或者，执行如权利要求 85 至 96 中任一项所述的方法，或者，执行如权利要求 97 至 103 中任一项所述的方法。

117、一种计算机程序，其特征在于，所述计算机程序使得计算机执行如权利要求 1 至 14 中任一项所述的方法，或者，执行如权利要求 15 至 27 中任一项所述的方法，或者，执行如权利要求 28 至 37 中任一项所述的方法，或者，执行如权利要求 38 至 51 中任一项所述的方法，或者，执行如权利要求 52 至 64 中任一项所述的方法，或者，执行如权利要求 65 至 74 中任一项所述的方法，或者，执行如权利要求 75 至 84 中任一项所述的方法，或者，执行如权利要求 85 至 96 中任一项所述的方法，或者，执行如权利要求 97 至 103 中任一项所述的方法。

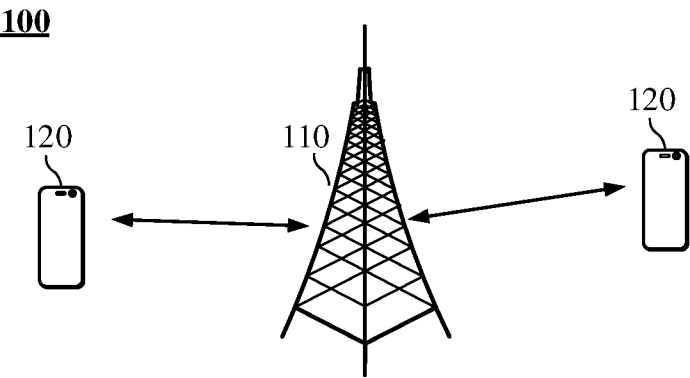


图 1

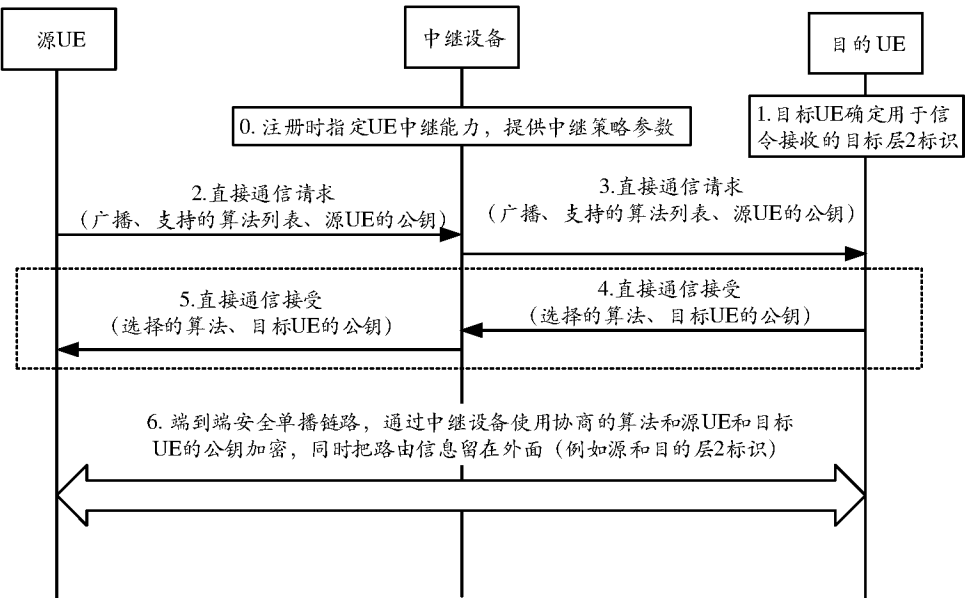


图 2

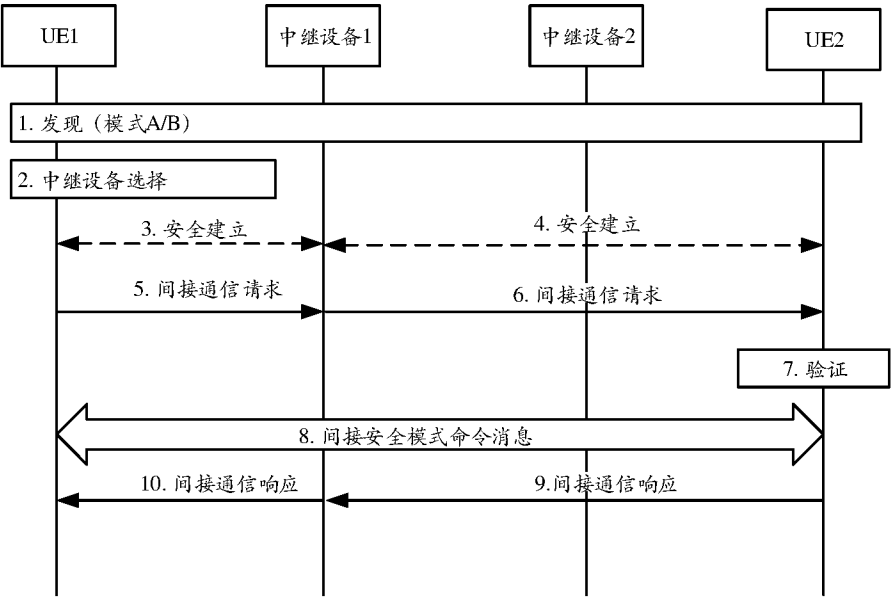


图 3

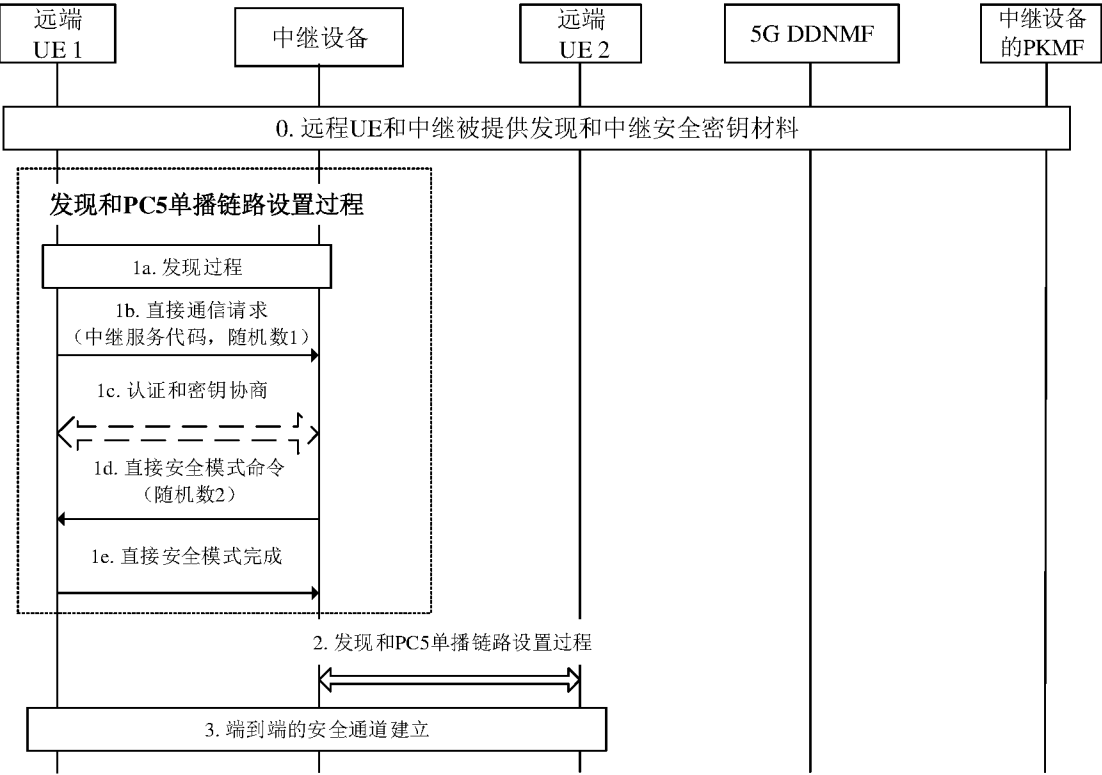


图 4

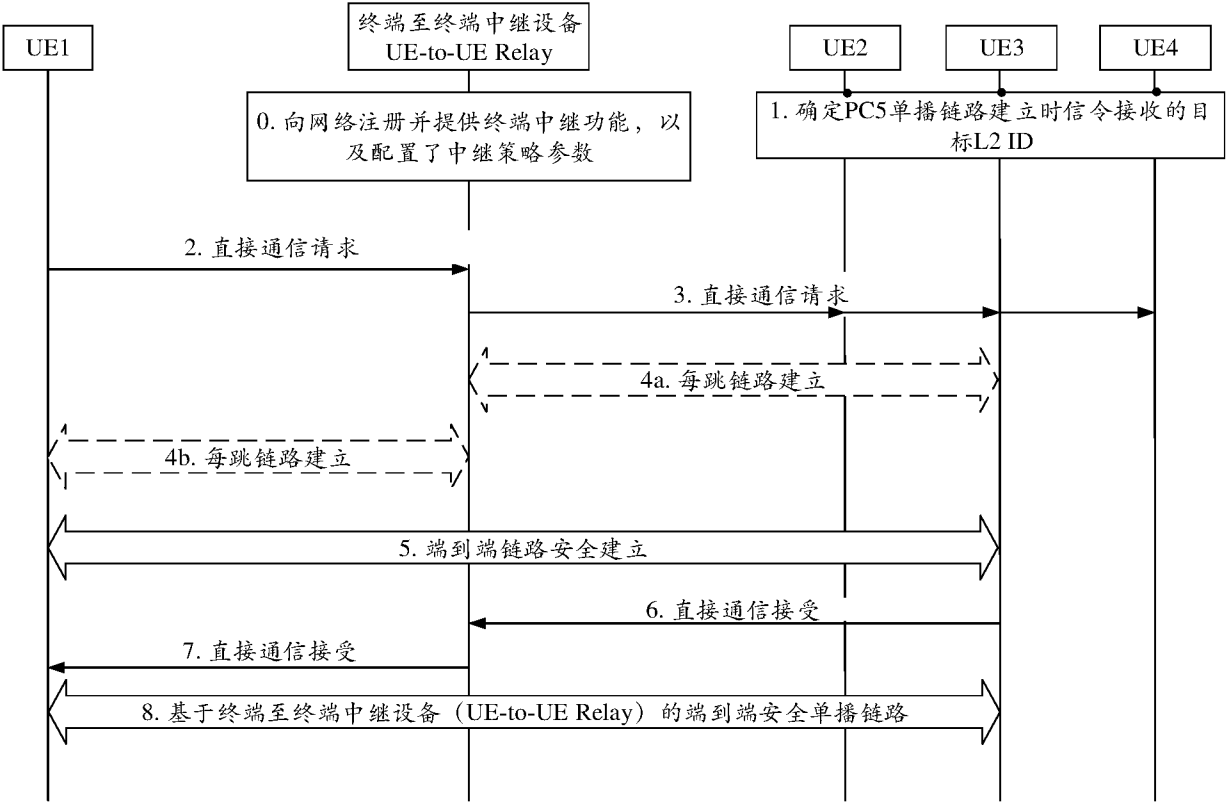


图 5

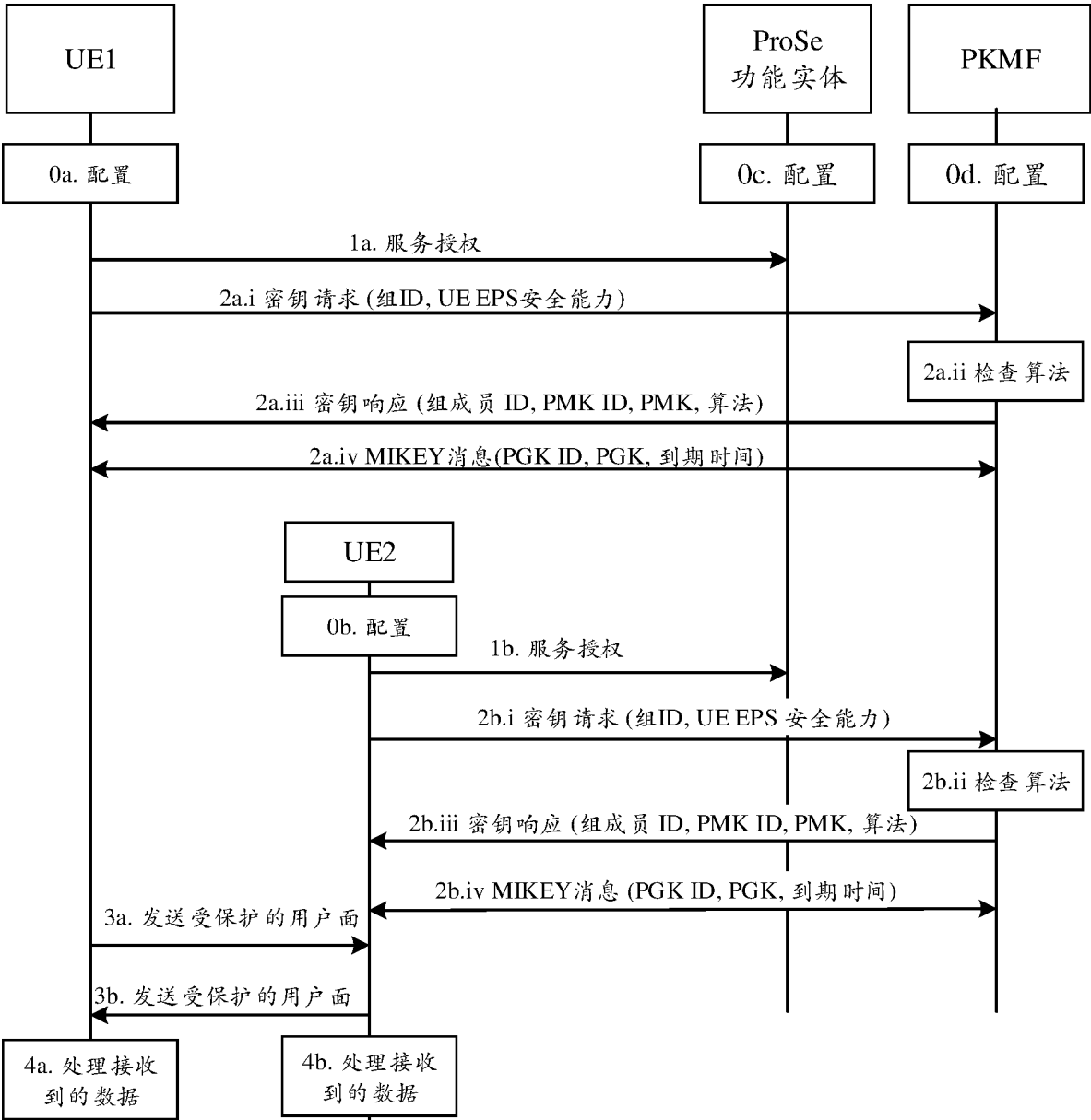


图 6

200

第一终端设备接收第二终端设备通过中继设备发送的认证请求消息；其中，该认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该中继设备所属用户的信息，该第二终端设备生成的第一临时公钥，该第二终端设备的签名，该中继设备的签名，该中继设备的相关信息；其中，该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的PVT和KPAK；该中继设备所属用户的信息包括该中继设备的标识和该中继设备的PVT和KPAK；该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥；该中继设备的签名的输入参数包括以下至少之一：该第二终端设备的签名和该中继设备所属用户的信息；该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥；该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

S210

图 7

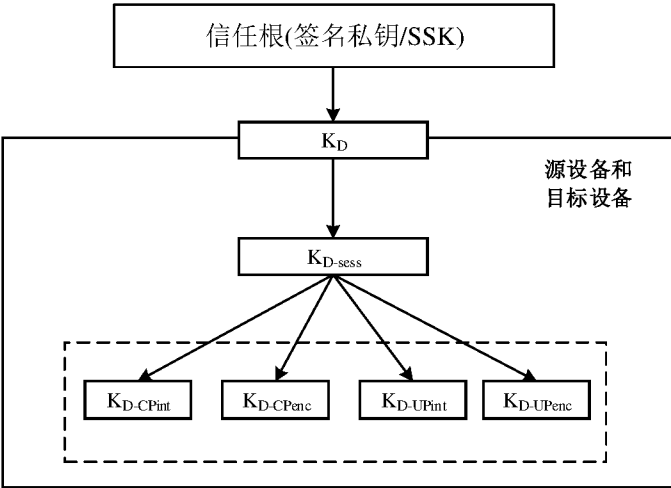


图 8

300

第二终端设备通过中继设备向第一终端设备发送认证请求消息；其中，该认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该第二终端设备生成的第一临时公钥，该第二终端设备的签名，该中继设备的相关信息；其中，该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的PVT和KPAK；该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥；该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥；该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

S310

图 9

400

中继设备接收第二终端设备发送的认证请求消息；其中，该认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该第二终端设备生成的第一临时公钥，该第二终端设备的签名；其中，该第二终端设备所属用户的信息包括该第二终端设备的标识和该第二终端设备的PVT和KPAK；该第二终端设备的签名的输入参数包括以下至少之一：该第二终端设备所属用户的信息和该第一临时公钥；

S410

在该第二终端设备的KPAK有效，且基于该第二终端设备的标识和该第二终端设备的PVT对该第二终端设备的签名验证成功的情况下，该中继设备向第一终端设备发送验证之后的认证请求消息；其中，该验证之后的认证请求消息包括以下至少之一：该第二终端设备所属用户的信息，该中继设备所属用户的信息，该第一临时公钥，该第二终端设备的签名，该中继设备的签名，该中继设备的相关信息；其中，该中继设备所属用户的信息包括该中继设备的标识和该中继设备的PVT和KPAK；该中继设备的签名的输入参数包括以下至少之一：该第二终端设备的签名和该中继设备所属用户的信息；其中，该第一临时公钥和该中继设备的相关信息用于该第一终端设备派生第一密钥；该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

S420

图 10

500

第一终端设备通过中继设备向第二终端设备发送第一消息；其中，该第一消息包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的第二临时公钥，该第一终端设备生成的第一密钥的标识的M个比特位，该第一终端设备的签名，第一消息验证码；其中，该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的PVT和KPAK；该第一终端设备的签名的输入参数包括以下至少之一：该第一终端设备所属用户的信息，该第二临时公钥，该第一密钥的标识的M个比特位，该第二终端设备的签名；其中，该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护，且该第一消息验证码的输入参数包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一随机数，该第二临时公钥，该M个比特位，该第一终端设备的签名；其中，该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，该第二密钥用于派生完整性保护密钥和/或机密性保护密钥，该第一密钥的标识由该M个比特位与该第一密钥的标识的另外N个比特位合并得到，M和N均为正整数；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

S510

图 11

600

第二终端设备接收第一终端设备通过中继设备发送的第一消息；其中，该第一消息包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该中继设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的第二临时公钥，该第一终端设备生成的第一密钥的标识的M个比特位，该第一终端设备的签名，该中继设备的签名，第一消息验证码；其中，该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的PVT和KPAK；该中继设备所属用户的信息包括该中继设备的标识和该中继设备的PVT和KPAK；该第一终端设备的签名的输入参数包括以下至少之一：该第一终端设备所属用户的信息，该第二临时公钥，该第一密钥的标识的M个比特位，该第二终端设备的签名；该中继设备的签名的输入参数包括以下至少之一：该中继设备所属用户的信息，该第一终端设备的签名，该第二终端设备的签名；其中，该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护，且该第一消息验证码的输入参数包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一随机数，该第二临时公钥，该M个比特位，该第一终端设备的签名；其中，该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，该第二密钥用于派生完整性保护密钥和/或机密性保护密钥，该第一密钥的标识由该M个比特位与该第一密钥的标识的另外N个比特位合并得到，M和N均为正整数；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

S610

图 12

700

中继设备接收第一终端设备发送的第一消息；其中，该第一消息包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的第二临时公钥，该第一终端设备生成的第一密钥的标识的M个比特位，该第一终端设备的签名，第一消息验证码；其中，该第一终端设备所属用户的信息包括该第一终端设备的标识和该第一终端设备的PVT和KPAK；该第一终端设备的签名的输入参数包括以下至少之一：该第一终端设备所属用户的信息，该第二临时公钥，该第一密钥的标识的M个比特位，该第二终端设备的签名；其中，该第一消息通过基于该第一密钥生成的该第一消息验证码进行完整性保护，且该第一消息验证码的输入参数包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该第一随机数，该第二临时公钥，该M个比特位，该第一终端设备的签名；

S710

在该第一终端设备的KPAK有效，且基于该第一终端设备的标识和该第一终端设备的PVT对该第一终端设备的签名验证成功的情况下，该中继设备向该第二终端设备发送验证之后的第一消息；其中，该验证之后的第一消息包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备所属用户的信息，该中继设备所属用户的信息，该第一终端设备生成的第一随机数，该第一终端设备生成的与该第二临时私钥配对的第二临时公钥，该第一终端设备生成的该第一密钥的标识的M个比特位，该第一终端设备的签名，该中继设备的签名，该中继设备的相关信息，该第一消息验证码；其中，该中继设备所属用户的信息包括该中继设备的标识和该中继设备的PVT和KPAK；该中继设备的签名的输入参数包括以下至少之一：该中继设备所属用户的信息，该第一终端设备的签名，该第二终端设备的签名，该验证之后的第一消息；其中，该第二临时公钥和该中继设备的相关信息用于该第二终端设备派生该第一密钥，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，该第二密钥用于派生完整性保护密钥和/或机密性保护密钥，该第一密钥的标识由该M个比特位与该第一密钥的标识的另外N个比特位合并得到，M和N均为正整数；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

S720

图 13

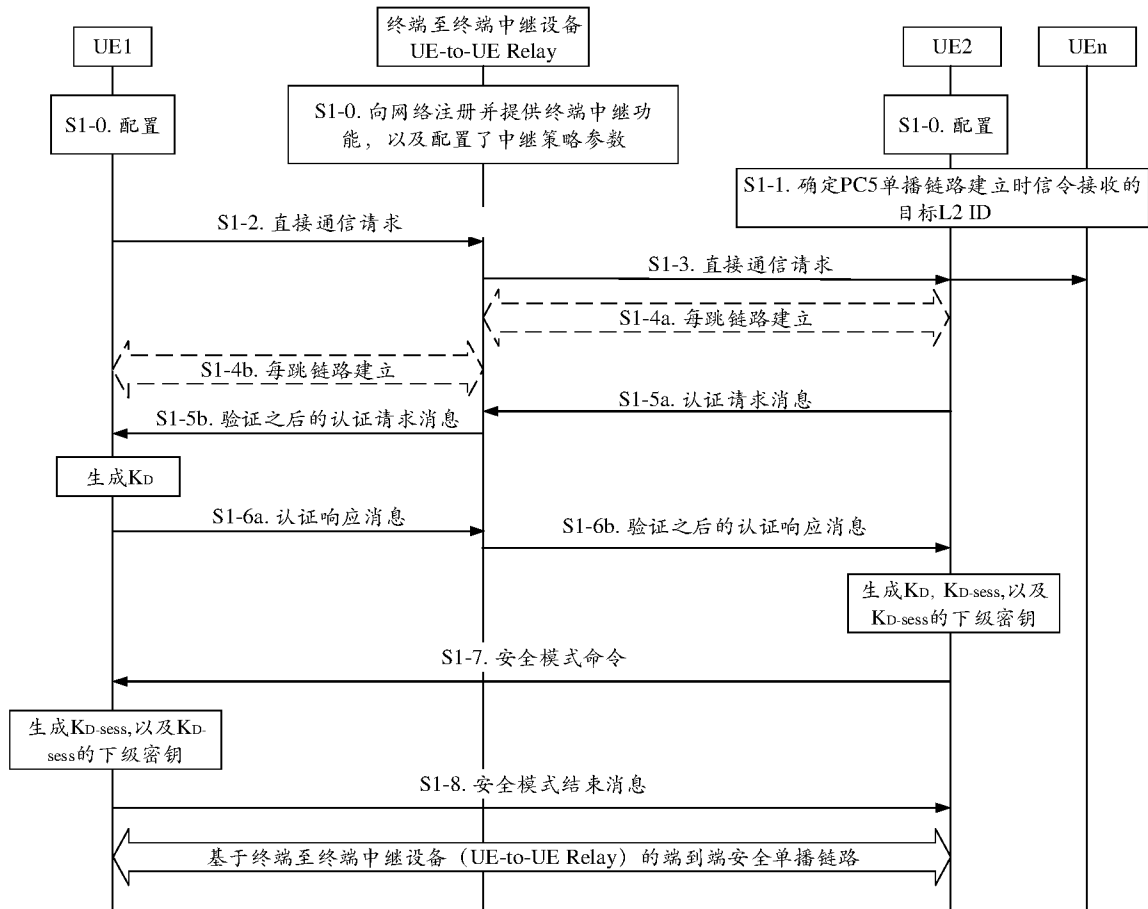


图 14

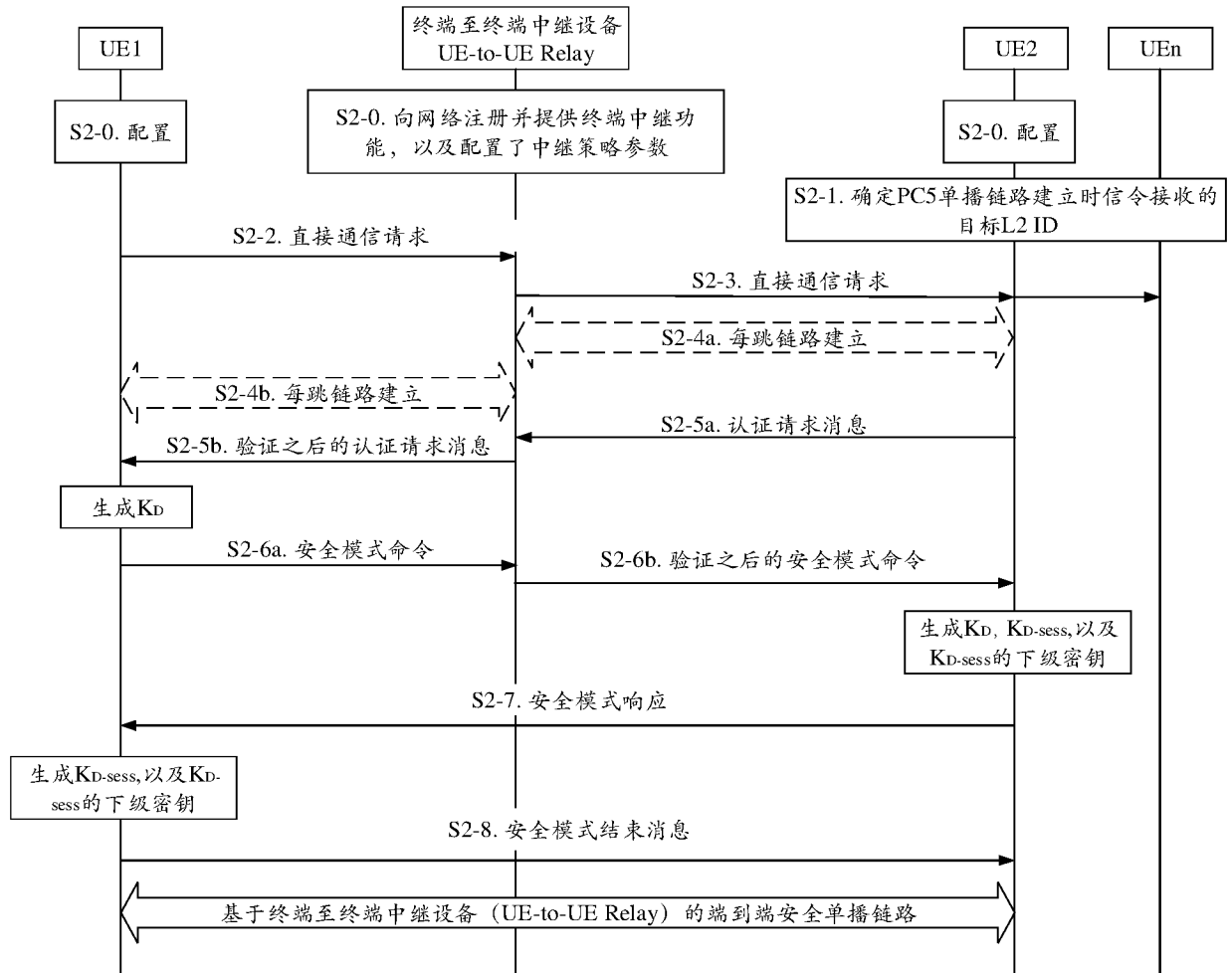


图 15

800

第一终端设备通过中继设备向第二终端设备发送直接通信请求；其中，该直接通信请求包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备生成的第一临时公钥，该第一终端设备生成的第一随机数；其中，该直接通信请求通过第一加密密钥进行加密，以及该直接通信请求通过第一完整性保护密钥进行完整性保护，该第一加密密钥为基于已注册并被授权使用终端至终端中继（UE-to-UE relay）通信的终端的对称密钥衍生的加密密钥，该第一完整性保护密钥为基于已注册并被授权使用UE-to-UE relay通信的终端的对称密钥衍生的完整性保护密钥；其中，该第一临时公钥和该中继设备的相关信息用于该第二终端设备派生第一密钥；该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器。

S810

图 16

900

第二终端设备接收第一终端设备通过中继设备发送的直接通信请求；其中，该直接通信请求包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备生成的第一临时公钥，该第一终端设备生成的第一随机数，该中继设备的标识，该中继设备的相关信息；其中，该直接通信请求通过第一加密密钥进行加密，以及该直接通信请求通过第一完整性保护密钥进行完整性保护，该第一加密密钥为基于已注册并被授权使用终端至终端中继（UE-to-UE relay）通信的终端的对称密钥衍生的加密密钥，该第一完整性保护密钥为基于已注册并被授权使用UE-to-UE relay通信的终端的对称密钥衍生的完整性保护密钥；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器；该第一临时公钥和该中继设备的相关信息用于该第二终端设备派生第一密钥；该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

S910

图 17

1000

中继设备接收第一终端设备发送的直接通信请求；其中，该直接通信请求包括以下至少之一：该第一终端设备的安全能力信息，该第一终端设备的安全策略信息，该第一终端设备生成的第一临时公钥，该第一终端设备生成的第一随机数；其中，该直接通信请求通过第一加密密钥进行加密，以及该直接通信请求通过第一完整性保护密钥进行完整性保护，该第一加密密钥为基于已注册并被授权使用终端至终端中继（UE-to-UE relay）通信的终端的对称密钥衍生的加密密钥，该第一完整性保护密钥为基于已注册并被授权使用UE-to-UE relay通信的终端的对称密钥衍生的完整性保护密钥；

S1010

该中继设备验证是否被配置为转发直接通信请求，在验证通过之后该中继设备使用该第一加密密钥解密该直接通信请求以获取QoS和计费信息，以及该中继设备使用该第一完整性保护密钥验证该直接通信请求的完整性，在验证通过之后该中继设备在该直接通信请求中添加该中继设备的相关信息和该中继设备的标识，并且该中继设备使用该第一加密密钥加密该直接通信请求，使用该第一完整性保护密钥保护该直接通信请求的完整性，并将所述直接通信请求转发至第二终端设备；其中，该中继设备的相关信息包括以下之一：该中继设备的身份信息，该中继设备生成的随机数，该中继设备生成的计数器；该第一临时公钥和该中继设备的相关信息用于该第二终端设备派生第一密钥；该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二密钥，且该第二密钥用于派生第二加密密钥和/或第二完整性保护密钥，或者，该第一随机数、该第一密钥和该第二终端设备生成的第二随机数用于派生第二加密密钥和/或第二完整性保护密钥。

S1020

图 18

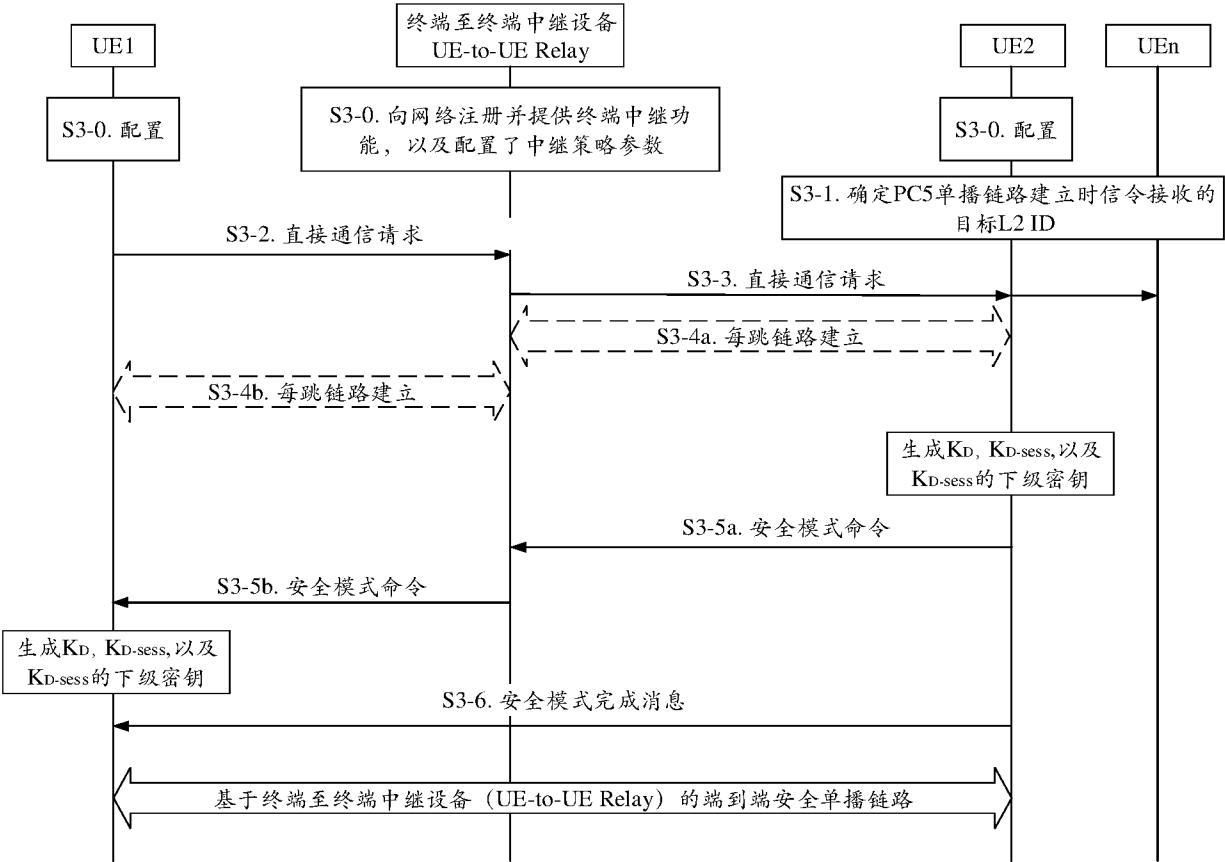


图 19

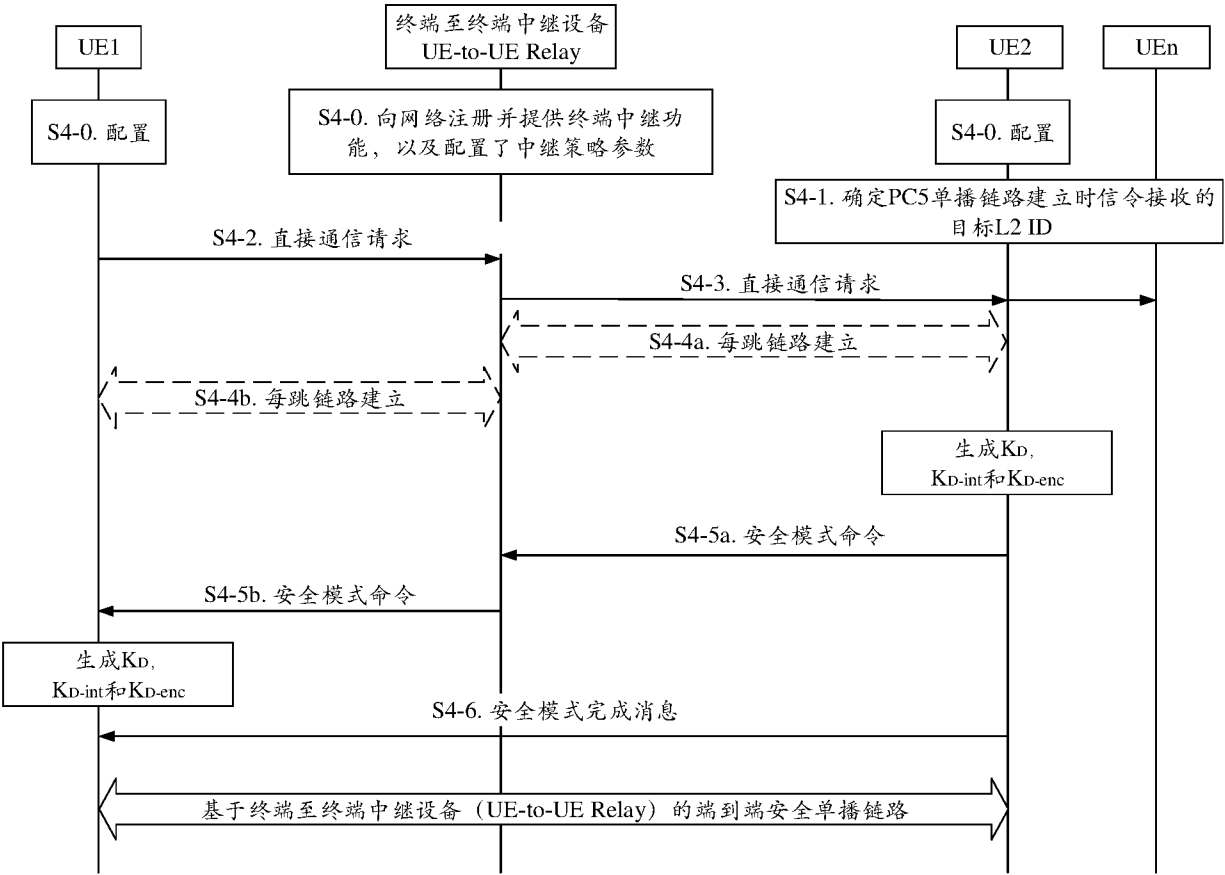


图 20

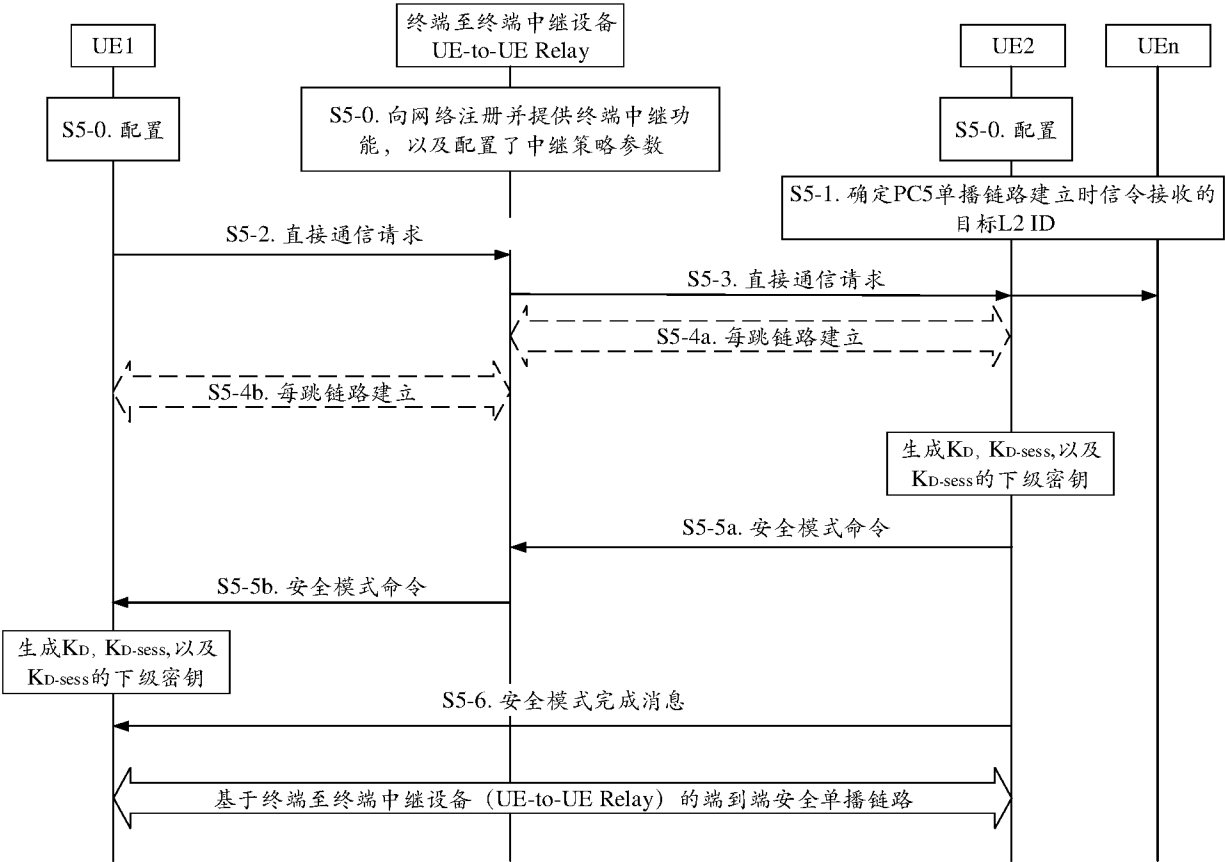


图 21

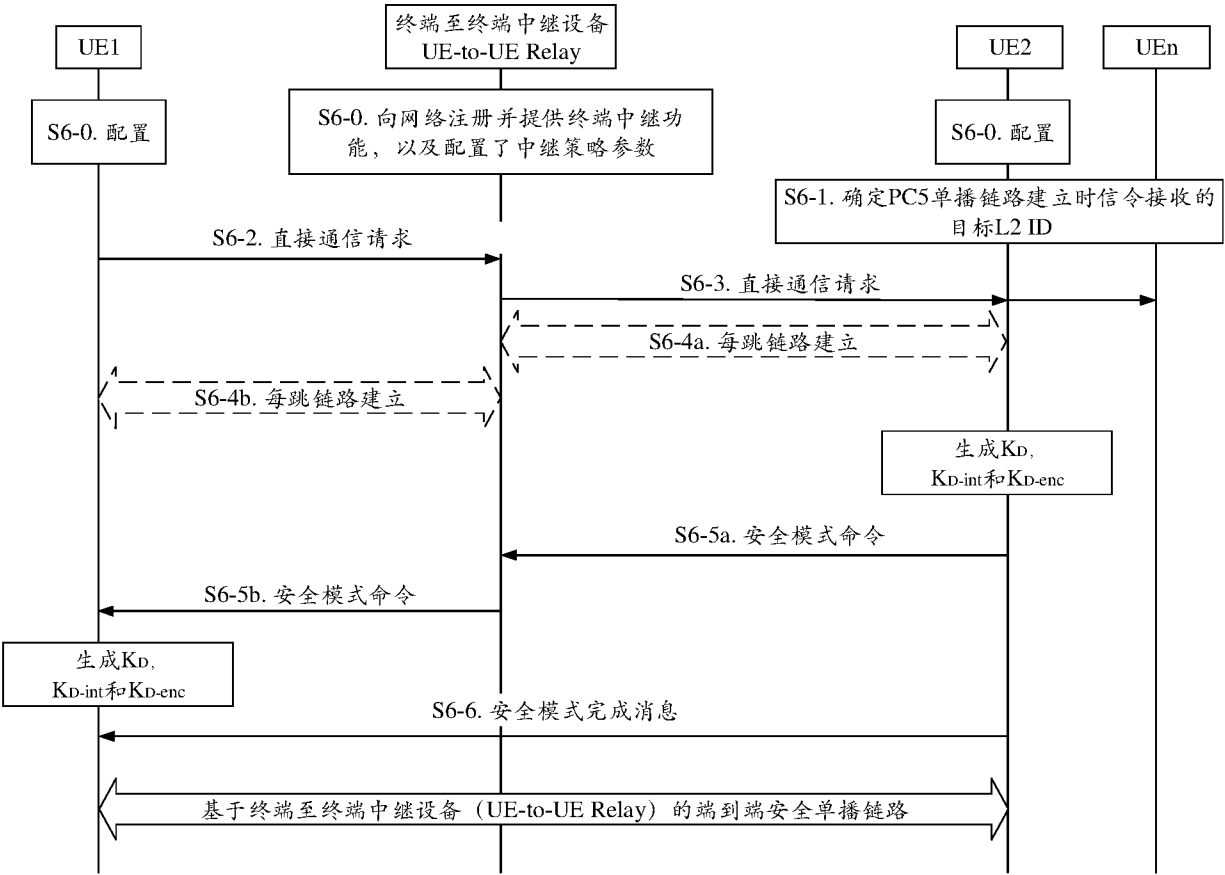


图 22

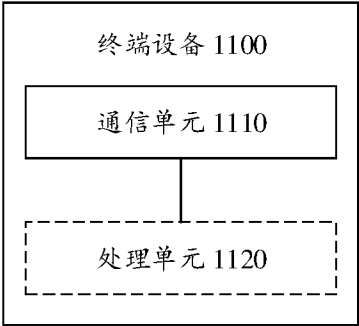


图 23

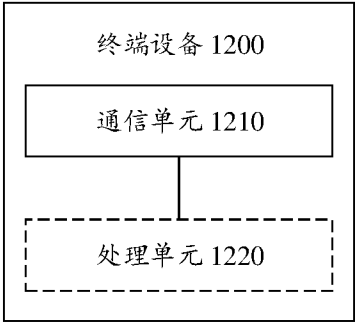


图 24



图 25

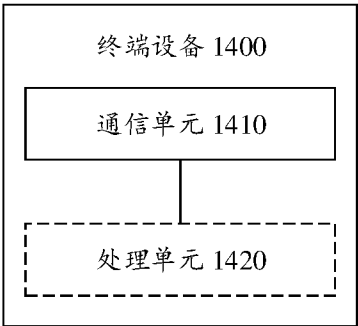


图 26

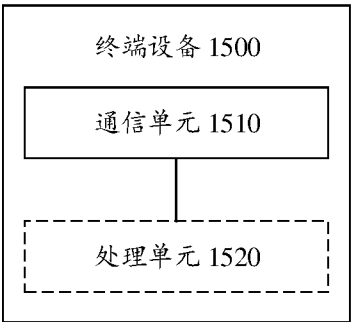


图 27



图 28

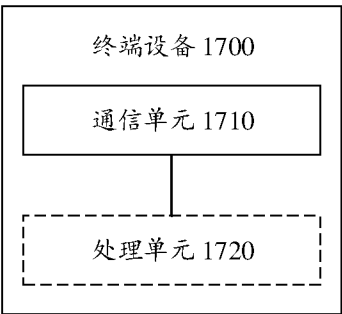


图 29

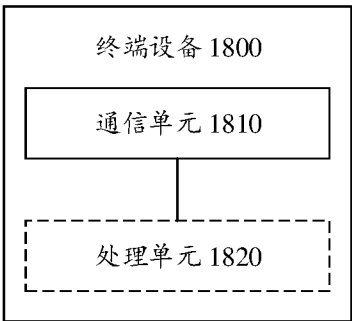


图 30

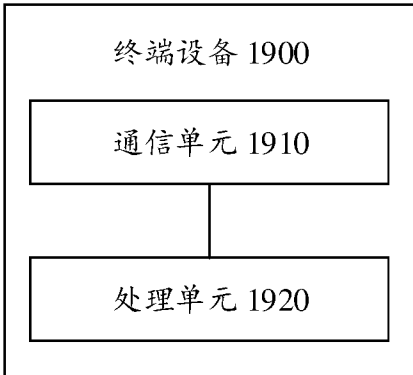


图 31

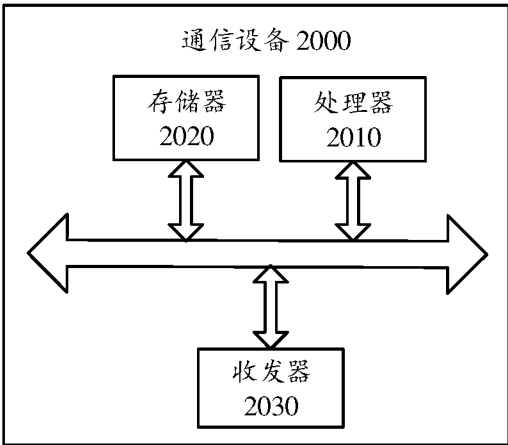


图 32

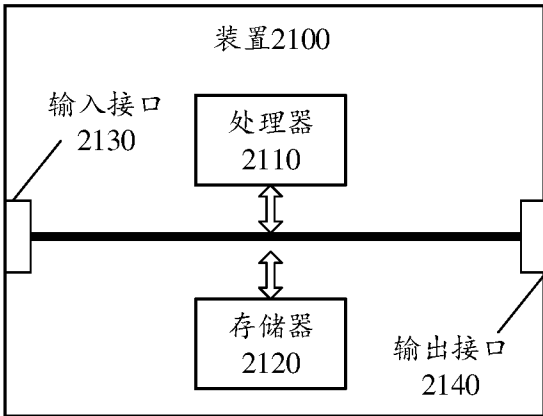


图 33

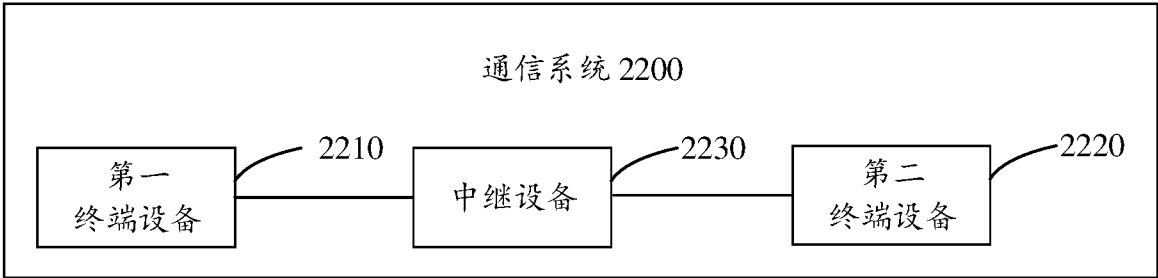


图 34

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/091125

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(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)

H04L9/-, H04W12/-

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)

CNTXT; WPABSC; CNABS; CNKI: 认证, 命令, 消息, 中继, 终端, 钥 EPTXT; USTXT; WOTXT; 3GPP; VEN; DWPI; IETF: symmetric key, public key, confidentiality, sign, KPAK, PVT, ECCSI, security, integrity protection, relay, ue to ue

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016269185 A1 (INTEL IP CORP.) 15 September 2016 (2016-09-15) description, paragraphs [0028]-[0057], and figure 13	1-117
X	US 2022109996 A1 (QUALCOMM INC.) 07 April 2022 (2022-04-07) description, paragraphs [0079]-[0091]	1-117
A	CN 110192381 A (HUAWEI TECHNOLOGIES CO., LTD.) 30 August 2019 (2019-08-30) entire document	1-117
A	WO 2022079572 A1 (TELEFONAKIEBOLAGET LM ERICSSONPUBL) 21 April 2022 (2022-04-21) entire document	1-117
A	3GPP ORGANIZATIONAL PARTNER. "S3-152079_TR33.833v1_5_0_rm" 3GPP tsq_sa\WG3_Security, 28 August 2015 (2015-08-28), entire document	1-117



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

16 January 2023

Date of mailing of the international search report

28 January 2023

Name and mailing address of the ISA/CN

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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/091125

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2016269185	A1	15 September 2016	EP	3269166	A1	17 January 2018
				CN	107251591	A	13 October 2017
				KR	20170128230	A	22 November 2017
				HK	1246556	A1	07 September 2018
				WO	2016148819	A1	22 September 2016
				CN	107251591		13 October 2017
				US	9893894	B2	13 February 2018
				JP	2018514092	W	31 May 2018
				JP	6732763	B2	29 July 2020
				CN	107251591	B	10 December 2021
				KR	102352724	B1	18 January 2022
US	2022109996	A1	07 April 2022	WO	2022072891	A1	07 April 2022
CN	110192381	A	30 August 2019	WO	2019051776	A1	21 March 2019
				CN	110192381	B	09 February 2021
WO	2022079572	A1	21 April 2022	None			

国际检索报告

国际申请号

PCT/CN2022/091125

A. 主题的分类

H04L 9/32 (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)

H04L9/-, H04W12/-

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))

CNTXT;WPABSC;CNABS;CNKI:认证, 命令, 消息, 中继, 终端, 钥 EPTXT;USTXT;WOTXT;3GPP;VEN;DWPI;IETF:symmetric key, public key, confidentiality, sign, KPAK, PVT, ECCSI, security, integrity protection, relay, ue to ue

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	US 2016269185 A1 (INTEL IP CORPORATION) 2016年9月15日 (2016 - 09 - 15) 说明书[0028]-[0057]段, 附图13	1-117
X	US 2022109996 A1 (QUALCOMM INCORPORATED) 2022年4月7日 (2022 - 04 - 07) 说明书[0079]-[00910]段	1-117
A	CN 110192381 A (华为技术有限公司) 2019年8月30日 (2019 - 08 - 30) 全文	1-117
A	WO 2022079572 A1 (TELEFONAKIEBOLAGET LM ERICSSONPUBL) 2022年4月21日 (2022 - 04 - 21) 全文	1-117
A	3GPP ORGANIZATIONAL PARTNER. "S3-152079_TR33.833v1_5_0_rm" 3GPP tsg_sa\WG3_Security, 2015年8月28日 (2015 - 08 - 28), 全文	1-117

☐ 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

2023年1月16日

国际检索报告邮寄日期

2023年1月28日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (ISA/CN)

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

李晓琳

电话号码 (86-28) 62969274

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/091125

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)
US	2016269185	A1	2016年9月15日	EP	3269166	A1	2018年1月17日
				CN	107251591	A	2017年10月13日
				KR	20170128230	A	2017年11月22日
				HK	1246556	A1	2018年9月7日
				WO	2016148819	A1	2016年9月22日
				CN	107251591		2017年10月13日
				US	9893894	B2	2018年2月13日
				JP	2018514092	W	2018年5月31日
				JP	6732763	B2	2020年7月29日
				CN	107251591	B	2021年12月10日
				KR	102352724	B1	2022年1月18日
US	2022109996	A1	2022年4月7日	WO	2022072891	A1	2022年4月7日
CN	110192381	A	2019年8月30日	WO	2019051776	A1	2019年3月21日
				CN	110192381	B	2021年2月9日
WO	2022079572	A1	2022年4月21日	无			