

说明书

安全通信方法和装置

5 本申请要求在 2023 年 05 月 15 日提交中国国家知识产权局、申请号为 202310544449.3、发明名称为“安全通信方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

10 本申请涉及无线通信领域，并且更具体地，涉及安全通信方法和装置。

背景技术

15 移动通信的安全问题正越来越多地受到关注。在互联网协议（internet protocol, IP）多媒体子系统（IP multimedia subsystem, IMS）中安全是基于一个长期的安全密钥。终端设备和网络设备完成认证之后，终端设备与第一个交互点（例如代理呼叫会话控制功能（proxy call session control function, P-CSCF））会获得共享密钥。进一步地，终端设备与 P-CSCF 之间可以根据共享密钥建立互联网安全协议(internet protocol security, IPSEC)通道，该 IPSEC 通道用于终端设备与 P-CSCF 之间进行上行/下行通信，其中终端设备与 P-CSCF 之间的上行/下行通信使用的密钥、盐值和初始化向量(initialization vector, IV)可能相同。

20 对于终端设备与 P-CSCF 之间的上下行通信，如何保证上下行通信的安全，是当前需要解决的问题。

发明内容

25 本申请提供一种安全通信方法和装置，能够保证终端设备和 P-CSCF 之间的上行、下行的通信安全。

30 第一方面，提供了一种安全通信方法。该方法可以由终端设备执行，或者，也可以由配置于终端设备中的芯片或电路执行；或者，该方法可以由网络设备执行，也可以由配置于网络设备中的芯片或电路执行，本申请对此不作限定。

 该方法可以包括：

35 第一设备通过第一消息向第二设备发送第一设备的第一信息，第一消息包括第一端口号、第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的一项或多项；第一设备接收来自第二设备的包括第二信息的第二消息，第二消息包括第二端口号、第二安全参数索引 SPI、第二互联网协议 IP 地址、第二安全算法列表、第二随机数中的一项或多项；第一设备根据第一信息和/或第二信息，使用第一计算方式确定用于第一设备与第二设备之间的上行传输的第一盐值，和/或使用第二计算方式确定用于第一设备与第二设备之间的下行传输的第二盐值。

40 根据本申请提供的方法，对于第一设备与第二设备之间的上行传输，第一设备可以根据第一设备的第一信息和来自第二设备的第二信息，使用第一计算方式确定第一盐值；相应地，第二设备根据第二设备的第二信息和来自第一设备的第一信息，使用第一计算方式确定第一盐值。可以看出，在第一设备和第二设备之间的上行传输中，第一设备和第二设备能够通过同一种计算方式，确定相同的盐值，即能够保证第一设备和第二设备之间的上行通信安全。对于第一设备与第二设备之间的下行传输，第一设备可以根据第一设备的第一信息和来自第二设备的第二信息，使用第二计算方式确定第二盐值；相应地，第二设备根据第二设备的第二信息和来自第一设备的第一信息，使用第二计算方式确定第二盐值。可以看出，在第一设备和第二设备之间的下行传输中，第一设备和第二设备能够通过同一种计算方式，确定相同的盐值，即能够保证第一设备和第二设备之间的下行通信安全。

45 结合第一方面，在一些可能实现的方式中，第一信息包括在第一消息的第一端口号、第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的一项中；和/或，第二信息包括在第二消息的第二端口号、第二安全参数索引 SPI、第二互联网协议 IP 地址、第二安全算法列表、

第二随机数中的一项中。

基于上述技术方案，第一设备向第二设备发送第一消息，该第一消息包括第一端口号、第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的一项或者多项，该第一消息中包括的第一信息可以携带在该第一消息中的第一端口号、第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的任意一项。第一设备接收来自第二设备发送的第二消息，该第二消息包括第二端口号、第二安全参数索引 SPI、第二互联网协议 IP 地址、第二安全算法列表、第二随机数中的一项或者多项，且该第二消息中包括的第二信息可以携带在该第二消息中的第二端口号、第二安全参数索引 SPI、第二互联网协议 IP 地址、第二安全算法列表、第二随机数中的任意一项。

10 在一种可能实现的方式中，该第一信息携带在第一端口号、第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的任意一项中时，该第一信息可以通过比特的形式进行表示。

在另一种可能实现的方式中，该第一信息携带在第一安全算法列表，第一端口号中的任意一项时，该第一信息还可以通过列表中的一个条目进行表示，如新增一个算法标识进行表示。

15 结合第一方面，在一些可能实现的方式中，使用第一计算方式确定第一盐值包括：

使用第一安全参数计算第一盐值，

其中，第一安全参数包括以下一项或者多项：上行传输的方向标识、上行传输的方向标识符、第一设备和/或第二设备的上行端口号、第一设备和/或第二设备的上行 IP 地址、第一设备和/或第二设备的上行 SPI、第一设备和/或第二设备的上行计数器、第一设备和/或第二设备的随机数；

20 使用第二计算方式确定第二盐值包括：使用第二安全参数计算第二盐值，

其中，第二安全参数包括以下一项或者多项：下行传输的方向标识、下行传输的方向标识符、第一设备和/或第二设备的下行端口号、第一设备和/或第二设备的下行 IP 地址、第一设备和/或第二设备的下行 SPI、第一设备和/或第二设备的下行计数器、第一设备和/或第二设备的随机数。

25 应理解，第一设备的上行 SPI 和端口号，第一设备的下行 SPI 和端口号均可以是第一设备本地生成的，第二设备的上行 SPI 和端口号，第二设备的下行 SPI 和端口号均可以是第二设备本地生成的。

在一种可能实现的方式中，第一设备的上行端口号、第一设备的上行 IP 地址、第一设备的上行 SPI、第一设备的上行计数器、第一设备的随机数可以通过第一消息发送给第二设备，用于第二设备使用第一安全参数计算第一盐值；第二设备的上行端口号、第二设备的上行 IP 地址、第二设备的上行 SPI、第二设备的上行计数器、第二设备的随机数可以通过第二消息发送给第一设备，用于第一设备使用第一安全参数计算第一盐值。

30 在另一中实现的方式中，第一设备的上行端口号、第一设备的下行 IP 地址、第一设备的下行 SPI、第一设备的下行计数器、第一设备的随机数可以通过第一消息发送给第二设备，用于第二设备使用第二安全参数计算第二盐值；第二设备的下行端口号、第二设备的下行 IP 地址、第二设备的下行 SPI、第二设备的下行计数器、第二设备的随机数可以通过第二消息发送给第一设备，用于第一设备使用第二安全参数计算第二盐值。

结合第一方面，在一些可能实现的方式中，第一设备使用第一安全参数确定用于上行传输的第一向量，和/或，使用第二安全参数确定用于下行传输的第二向量；

第一设备向第二设备发送第一向量和/或第二向量。

40 基于上述技术方案，第一设备使用区别上下行传输的相关参数（例如，端口号、方向标识、方向标识符、IP 地址、SPI、计数器、随机数），确定第一向量和/或第二向量，并将第一向量和/或第二向量发送给第二设备。该第一向量与第二向量不同，能够进一步地保证第一设备和第二设备之间上下行使用的第一向量和第二向量不同，从而保证第一设备和第二设备之间上行、下行的通信安全。

第二方面，提供了一种安全通信方法。该方法可以由终端设备执行，或者，也可以由配置于终端设备中的芯片或电路执行；或者，该方法可以由网络设备执行，或者，也可以由配置于网络设备中的芯片或电路执行，本申请对此不作限定。

该方法包括：

第一设备使用第一安全参数确定用于第一设备与第二设备之间的上行传输的第一向量，和/或使用第二安全参数确定用于第一设备与第二设备之间的下行传输的第二向量；

其中，第一安全参数包括以下一项或者多项：上行传输的方向标识、上行传输的方向标识符、第一设备和/或第二设备的上行端口号、第一设备和/或第二设备的上行 IP 地址、第一设备和/或第二设备的上行 SPI、第一设备和/或第二设备的上行计数器、第一设备和/或第二设备的随机数；第二安全参数包括以下一项或者多项：下行传输的方向标识、下行传输的方向标识符、第一设备和/或第二设备的下行端口号、第一设备和/或第二设备的下行 IP 地址、第一设备和/或第二设备的下行 SPI、第一设备和/或第二设备的下行计数器、第一设备和/或第二设备的随机数；

第一设备向第二设备发送第一向量和/或第二向量。

基于上述技术方案，第一设备使用区别上行、下行传输的相关参数（例如，端口号、方向标识、方向标识符、IP 地址、SPI、计数器、随机数），确定第一向量和/或第二向量，并将第一向量和/或第二向量发送给第二设备。其中，该第一向量是根据上行传输相关的第一安全参数确定的，第二向量是根据下行传输相关的第二安全参数确定的，即第一设备和第二设备之间上行、下行使用的第一向量和第二向量不同，从而保证第一设备和第二设备之间上行、下行的通信安全。

第三方面，提供一种安全通信装置，该装置用于执行上述第一方面和/或第二方面提供的方法。具体地，该装置可以包括用于执行第一方面、第二方面任意一种实现方式提供的方法的单元和/或模块，如处理单元和/或收发单元（或者称为通信单元）。

在一种实现方式中，该装置为通信设备（如终端设备，又如网络设备）。当该装置为通信设备时，通信单元可以是收发器或者收发单元，或，输入/输出接口；处理单元可以是至少一个处理器。可选地，收发器可以为收发电路。可选地，输入/输出接口可以为输入/输出电路。

在另一种实现方式中，该装置为用于通信设备（如终端设备，又如网络设备）中的芯片、芯片系统或电路。当该装置为用于通信设备中的芯片、芯片系统或电路时，通信单元可以是该芯片、芯片系统或电路上的输入/输出接口、接口电路、输出电路、输入电路、管脚或相关电路等；处理单元可以是至少一个处理器、处理电路或逻辑电路等。

第四方面，提供一种通信装置，该装置包括：存储器，用于存储计算机程序或指令；至少一个处理器，用于执行存储器存储的计算机程序或指令，以执行上述第一方面、第二方面中任意一种实现方式提供的方法。

在一种实现方式中，该装置为通信设备（如终端设备，又如网络设备）。

在另一种实现方式中，该装置为用于通信设备（如终端设备，又如网络设备）中的芯片、芯片系统或电路。

第五方面，本申请提供一种处理器，用于执行上述各方面提供的方法。

对于处理器所涉及的发送和获取/接收等操作，如果没有特殊说明，或者，如果未与其在相关描述中的实际作用或者内在逻辑相抵触，则可以理解为处理器输出和输入等操作，也可以理解为由射频电路和天线所进行的发送和接收操作，本申请对此不做限定。

第六方面，提供一种计算机可读存储介质，该计算机可读介质存储用于设备执行的程序代码，该程序代码包括用于执行上述第一方面、第二方面中上述任意一种实现方式提供的方法。

第七方面，提供一种包含指令的计算机程序产品，当该计算机程序产品在计算机上运行时，使得计算机执行上述第一方面、第二方面中任意一种实现方式提供的方法。

第八方面，提供一种芯片，芯片包括处理器与通信接口，处理器通过通信接口读取存储器上存储的指令，执行上述第一方面、第二方面中任意一种实现方式提供的方法。

可选地，作为一种实现方式，芯片还包括存储器，存储器中存储有计算机程序或指令，处理器用于执行存储器上存储的计算机程序或指令，当计算机程序或指令被执行时，处理器用于执行上述第一方面、第二方面中任意一种实现方式提供的方法。

附图说明

图 1 是适用于本申请实施例提供的方法的网络架构的示意图。

图 2 是根据本申请实施例提供的安全通信方法的示意性流程图。

图 3 是本申请另一实施例提供的安全通信方法的示意性流程图。

图 4 是本申请实施例提供的安全通信装置 400 的示意图。

图 5 是本申请另一实施例提供种安全通信装置 500 的示意图。

图 6 是本申请实施例提供一种芯片系统 600 的示意图。

具体实施方式

5 下面将结合附图，对本申请中的技术方案进行描述。

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、LTE 频分双工（Frequency Division Duplex, FDD）系统、LTE 时分双工（Time Division Duplex, TDD）、通用移动通信系统（Universal Mobile Telecommunication System, UMTS）、全球互联微波接入（Worldwide Interoperability for Microwave Access, WiMAX）通信系统、第五代（5th Generation, 5G）系统、新无线（New Radio, NR）、第六代（6th Generation, 6G）系统或未来的通信系统等。

应理解，本申请实施例并未对本申请实施例提供的方法的执行主体的具体结构特别限定，只要能
15 够通过运行记录有本申请实施例的提供的方法的代码的程序，以根据本申请实施例提供的方法进行通信即可，例如，本申请实施例提供的方法的执行主体可以是终端侧或网络侧设备，或者，是终端侧或网络侧设备中能够调用程序并执行程序的功能模块。

为便于理解本申请实施例，首先结合图 1 详细说明本申请实施例的一个应用场景。

图 1 是适用于本申请实施例提供的方法的网络架构的示意图。如图 1 所示，该网络架构具体可以
20 包括下列网元：

1、终端设备（user equipment, UE）：可以称用户设备、终端、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、无线通信设备、用户代理或用户装置。终端设备还可以是蜂窝电话、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、个人数字处理（Personal Digital Assistant, PDA）、具有
25 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，未来 5G 网络中的终端设备或者未来演进的公用陆地移动通信网络（Public Land Mobile Network, PLMN）中的终端设备等，本申请实施例对此并不限定。

2、代理呼叫会话控制功能（proxy call session control function, P-CSCF）：IMS 域拜访域控制平面统一的初步入口点，主要将来自拜访地接入网络的会话发起协议（session initiation protocol, SIP）消息代理转接到其归属地的服务呼叫会话控制功能（serving call session control function, S-CSCF）或者查询
30 呼叫会话控制功能（interrogating call session control function, I-CSCF）。

该 P-CSCF 还用于提供 IMS 与终端设备之间的 SIP 信息的完整与安全。

3、查询呼叫会话控制功能（I-CSCF）：当用户漫游时，I-CSCF 主要作为终端设备接入归属网络的接入点。

35 I-CSCF 与归属用户服务器（home subscriber server, HSS）交互可以获取该用户归属的 S-CSCF 地址。I-CSCF 可以向 S-CSCF 转发 SIP 的请求与相应。

4、服务呼叫会话控制功能（S-CSCF）：S-CSCF 在整个 IMS 核心网的会话控制中处于核心的控制位置。S-CSCF 接收来自拜访地网络 IMS 用户经过 P-CSCF 转发的注册请求，与 HSS 配合对 IMS 的终端设备进行鉴权，从 HSS 中下载 IMS 的基本签约数据，执行针对主叫端及被叫端 IMS 终端的基本会话
40 话路由功能。

5、归属用户服务器（HSS）：HSS 主要用于归属网络中保存 IMS 用户的签约信息的集中综合数据库。其中 IMS 用户的签约信息包括标识信息、路由信息以及业务签约信息等。HSS 位于 IMS 核心网架构中的最顶层。

HSS 中保存的主要信息包括：IMS 用户标识（包括公共以及私有标识）、号码和地址信息；IMS
45 用户安全上下文：用户网络接入认证的密钥信息；IMS 用户的路由信息；HSS 支持用户的注册，并且存储用户的位置信息；IMS 用户的业务签约信息：包括其他应用服务器（application server, AS）的增值业务数据。

6、应用服务器（AS）：提供 IMS 的业务，例如：短信、彩铃、彩印等等。AS 接收与处理来自 IMS 的 SIP 请求。

应理解，IMS 建立在一个归属地网络和一个访问地网络的概念上，一般地，根据 IMS 用户是否漫游存在两个情景。一种情景：终端设备接入 IMS 的第一个交互点（例如 P-CSCF）位于归属地网络中：

5 另一种情景：P-CSCF 位于访问地网络中，意味着终端设备是以接入 IMS 的第一个交互点不在归属地网络的方式进行漫游。本申请提供的方式可以使用与上述两种任意一种场景，对此本申请不做具体限定。

还应理解，终端设备与网络设备进行认证的详细过程可以参见现有技术，此处不再赘述。在终端设备与网络设备完成认证之后，终端设备和 P-CSCF 会获得共享密钥，其中共享密钥包括完整性密钥（integrity key, IK）和机密性密钥（confidentiality key, CK），终端设备和 P-CSCF 根据 IK 和 CK 建立 IP 安全（IP Security, IPSEC）通道。

其中，IPSEC 通道可以包括终端设备与 P-CSCF 之间的上行传输，终端设备与 P-CSCF 之间的下行传输，即该 IPSEC 通道的方向是双向的，包括上行和下行两个方向。终端设备与 P-CSCF 之间进行上行传输和/或下行传输时，终端设备和 P-CSCF 各自需要确定针对上行传输和/或下行传输的盐值，该盐值用于加密或者解密上行传输和/或下行传输的信息。如何保证在终端设备和 P-CSCF 之间的上行传输中，终端设备和 P-CSCF 分别确定的盐值相同，在终端设备和 P-CSCF 之间的下行传输中，终端设备和 P-CSCF 分别确定的盐值相同，是本领域目前研究的热点问题。

为了便于理解本申请实施例中提供的技术方案，下面对本申请中涉及到的专业术语进行简单介绍：

1. 盐值（salt 值）可以是一个随机的字段，也可以是通过某种算法生成的数值。盐值主要用于对传输信息的密码保护，通过对密码进行加盐（混入随机字符拼接在密码明文），可以增加系统的复杂度，得到更强更安全的密文摘要值。

2. 初始化向量（initialization vector, IV）可以成为初始变量、或者初始向量，是一个固定长度的输入值。每次加密都需要随机生成一个不同比特序列作为 IV，一般不采用静态的 IV。IV 的取值根据不同的密码算法确定的，但其基本要求“唯一性”，即同一个密钥不重复使用同一初始化向量 IV。IPSEC 通道中的两个方向使用相同的初始化向量 IV，可能由于 IPSEC 未提供 IV 的协调机制，导致终端设备和 P-CSCF 生成的 IV 也完全一样。

目前，IPSEC 通道的上行传输和下行通信会使用相同的密钥（即 IK 和 CK）、相同的盐值和相同的 IV。假设，同一文本分别从 IPSEC 通道中的上行和下行方向进行传输时，该文本会经过相同的密钥、盐值和初始化向量 IV，即上行和下行传输会获得相同的加密文本，导致通信安全性能较低。

其中，由于终端设备和 P-CSCF 生成盐值的参数是完全一样的，则 IPSEC 通道中的上行传输和下行传输的盐值完全一样，即终端设备和 P-CSCF 分别针对上行传输和下行传输，确定的盐值完全一样。例如，针对终端设备和 P-CSCF 之间的上行传输，终端设备确定用于上行传输的盐值为盐值#1，P-CSCF 确定用于上行传输的盐值为盐值#1'；针对终端设备和 P-CSCF 之间的下行传输，终端设备确定用于下行传输的盐值为盐值#2，P-CSCF 确定用于下行传输的盐值为盐值#2'；其中，盐值#1，盐值#1'，盐值#2 和盐值#2'完全相同。

考虑 IPSEC 通道传输的通信安全，在 IPSEC 通道中上行传输和下行传输在使用相同的密钥（IK 和 CK）的情况下，需要保证终端设备和 P-CSCF 上行传输的盐值与终端设备和 P-CSCF 下行传输的盐值不同。为了保证终端设备和 P-CSCF 上行传输的盐值与终端设备和 P-CSCF 下行传输的盐值不同，可以终端设备和 P-CSCF 的盐值推导参数中添加安全关联（security association, SA）中的安全参数索引（security parameter index, SPI）。其中 SA 是单向且唯一的，该 SPI 是 SA 的唯一标识 ID，即上行传输和下行传输对应的 SPI 不同，从而保证上行传输和下行传输使用的盐值不同。

其中，限定了上行传输和下行传输对应的盐值不同，例如，针对终端设备和 P-CSCF 之间的上行传输，终端设备确定用于上行传输的盐值为盐值#1，P-CSCF 确定用于上行传输的盐值为盐值#1'；针对终端设备和 P-CSCF 之间的下行传输，终端设备确定用于下行传输的盐值为盐值#2，P-CSCF 确定用于下行传输的盐值为盐值#2'。用于上行传输的盐值（盐值#1 和盐值#1'），与用于下行传输的盐值（盐值#2 和盐值#2'）不同，并未考虑用于上行传输的盐值#1 和盐值#1'是否相同，用于下行传输的盐值#2 和盐值#2'是否相同。

终端设备和 P-CSCF 无法保证在上行传输中终端设备和 P-CSCF 确定的盐值是否相同，或者在下行

传输中终端设备和 P-CSCF 确定的盐值是否相同。当在上行传输或者下行传输中，终端设备和 P-CSCF 确定的用于传输的上行/下行的盐值不同，则会导致终端设备和 P-CSCF 对传输信息的加密解密失败，从而影响通信性能。

针对上述存在的技术问题，终端设备与 P-CSCF 之间的上下行传输，如何保证终端设备与 P-CSCF 在上行传输中确定同样的盐值，以及终端设备与 P-CSCF 在下行传输中确定同样的盐值是本申请解决的技术问题。

本申请提供一种安全通信方法，能够保证通信设备之间的上行、下行的通信安全。例如第一设备与第二设备之间进行上行传输，即第一设备的上行传输确定的盐值和第二设备的上行传输确定的盐值相同，从而能够提高第一设备与第二设备之间的通信安全。

图 2 是本申请实施例提供的一种安全通信方法的流程性示意图。

210，第一设备通过第一消息向第二设备发送第一设备的第一信息。

相应地，第二设备接收来自第一设备通过第一消息发送的第一设备的第一信息。

其中，第一信息包括第一设备支持的盐值计算方式。该第一设备支持的盐值计算方式可以理解为第一设备支持的盐值计算能力，或者可以理解为第一设备支持的算法，第一设备支持的盐值计算方式和第一设备支持的盐值计算能力均可以用于确定第一设备计算盐值的方式。本申请实施例中主要以第一设备支持的盐值计算方式进行描述，还可以替换为其他描述，对此本申请不做具体限定。

应理解，该第一消息包括第一端口号、第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的一项或多项。

在一种可能实现的方式中，该第一设备通过第一消息向第二设备发送第一信息，可以是第一设备通过单独的指示发送给第二设备，该第一信息无需承载在任何其他信令或者算法列表中。

在另一种可能实现的方式中，该第一信息携带在第一消息包括的第一端口号、第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的任一项中，通过第一消息发送给第二设备。例如，第一消息包括第一端口号、第一互联网协议 IP 地址。该第一端口号可以携带该第一信息，或者该第一 IP 地址可以携带第一信息。

其中，该第一信息可以通过比特的形式进行表示。

作为一种示例，当第一信息携带在第一消息中的第一端口号、第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的任意一项中时，假设该第一信息包括第一比特，该第一比特包含在第一端口号中，该第一比特用于指示第一设备支持的盐值计算方式。

例如，假设第一比特的长度为 1bit，第一比特取 0 时，表示第一设备支持的盐值计算方式为方式 #1，第一比特取 1 时，表示第一设备支持的盐值计算方式为方式 #2。

应理解，未来第一设备可能支持的盐值计算方式可以有 2 种或者 2 种以上，第一信息均可以通过比特的形式表示第一设备支持的盐值计算方式。

其中，该第一信息可以通过信息元素（information element，IE）的形式进行表示。

作为一种示例，当第一信息携带在第一消息中的第一安全算法列表中时，该第一信息可以通过信息元素的方式进行表示第一设备支持的盐值计算方式。

例如，该第一信息为算法中的一个算法标识或指示，和/或，该第一信息为加密算法的一个算法标识或指示。

220，第一设备接收来自第二设备的包含第二信息的第二消息。

相应地，第二设备向第一设备发送包括第二信息的第二消息。

其中，第二信息包括第二设备支持的盐值计算方式。该第二设备支持的盐值计算方式可以理解为第二设备支持的盐值计算能力，或者可以理解为第二设备支持的算法，第二设备支持的盐值计算方式和第二设备支持的盐值计算能力均可以用于确定第二设备计算盐值的方式。本申请实施例中主要以第二设备支持的盐值计算方式进行描述，还可以替换为其他描述，对此本申请不做具体限定。

应理解，该第二消息包括第二端口号、第二安全参数索引 SPI、第二互联网协议 IP 地址、第二安全算法列表中、第二随机数中的一项或多项。

在一种可能实现的方式中，该第二设备通过第二消息向第一设备发送第二信息，该第二信息可以是第二设备通过单独的指示发送给第一设备，该第二信息无需承载在任何其他信令或者算法列表中。

在另一种可能实现的方式中，该第二信息携带在第二消息包括的第二端口号、第二安全参数索引

SPI、第二互联网协议 IP 地址、第二安全算法列表、第二随机数中的任一项中，并通过第二消息发送给第一设备。例如，第二消息包括第二端口号、第二互联网协议 IP 地址。该第二端口号可以携带该第二信息，或者该第二 IP 地址可以携带第二信息。

5 应理解，该第二信息可以表示第二设备支持的盐值计算方式，具体地，该第二信息可以通过比特的形式进行表示，或者通过信元的形式进行表示，对此本申请不做具体限定。

还应理解，步骤 220 中的第二信息的传输方式以及第二信息的具体表现形式，与步骤 210 中的第一信息的传输方式以及第一信息的具体表现形式类似，具体可以参见步骤 210 中的详细举例，此处不再赘述。

需要说明的是，本申请不限定步骤 210 与步骤 220 之间步骤的先后顺序，步骤 210 可以在步骤 220 之前发生，步骤 220 可以发生在步骤 210 之前，或者步骤 210 和步骤 220 同时发生，本申请不做具体限定。

还需要说明的是，步骤 210 和步骤 220 之间，具有明显的先后逻辑关系时，该步骤 210 可以在步骤 220 之前。如下所述：

15 作为一种可能实现的方式，当第二设备接收到来自第一设备发送的包括第一信息的第一消息之后，第二设备确定第二设备支持第一设备的计算盐值的计算方式，该第二设备才会执行步骤 220，即第二设备向第一设备发送包括第二信息的第二消息。

其中，当第二设备确定第二设备支持第一设备的计算盐值的计算方式时，该第二设备根据自身支持的第一设备的计算盐值的计算方式，计算第一盐值。

20 步骤 230，根据第一信息和/或第二信息，使用第一计算方式确定第一盐值，和/或使用第二计算方式确定第二盐值。

其中，第一设备和第二设备可以通过第一信息和第二信息，能够使用第一计算方式确定用于第一设备与第二设备之间的上行传输的第一盐值，和/或，使用第二计算方式确定用于第一设备与第二设备之间的下行传输的第二盐值。

25 在一种可能实现的方式中，第一设备接收到第二信息之后，第一设备根据第二信息中包括的第二设备支持的盐值计算方式和第一设备自身支持的盐值计算方式，确定第一计算方式。第一设备通过该第一计算方式，确定第一设备和第二设备之间上行传输的第一盐值。

类似地，第二设备接收到第一信息之后，第二设备根据第一信息中包括的第一设备支持的盐值计算方式和第二设备自身支持的盐值计算方式，确定第一计算方式。第二设备通过第一计算方式，确定第一设备和第二设备之间上行传输的第一盐值。

30 在另一种可能实现的方式中，第一设备接收到第二信息之后，第一设备根据第二信息中包括的第二设备支持的盐值计算方式和第一设备自身支持的盐值计算方式，确定第二计算方式。第一设备通过该第二计算方式，确定第一设备和第二设备之间下行传输的第二盐值。

35 类似地，第二设备接收到第一信息之后，第二设备根据第一信息中包括的第一设备支持的盐值计算方式和第二设备自身支持的盐值计算方式，确定第二计算方式。第二设备通过第二计算方式，确定第一设备和第二设备之间下行传输的第二盐值。

其中，第一设备可以根据第二信息，使用第一计算方式确定第一盐值，和/或，使用第二计算方式确定第二盐值。

40 在一种可能实现的方式中，第一设备接收到第二信息之后，第一设备可以确定第二设备支持第一设备支持的盐值计算方式，第一设备可以根据第二信息，确定第一计算方式和/或第二计算方式。第一设备通过第一计算方式，确定第一设备和第二设备之间上行传输的第一盐值；和/或，第一设备通过第二计算方式，确定第一设备和第二设备之间下行传输的第二盐值。

45 作为一种示例，假设第一设备为终端设备，第二设备为 P-CSCF。终端设备接收到来自 P-CSCF 的第二信息之后，终端设备确定 P-CSCF 已经接收到终端设备的第一信息，并且 P-CSCF 支持该第一信息中终端设备支持的盐值计算方式。终端设备可以根据 P-CSCF 的第二信息，确定第一计算方式和/或第二计算方式，并通过第一计算方式确定第一盐值和/或通过第二计算方式确定第二盐值。

其中，第一设备可以根据第一信息，使用第一计算方式确定第一盐值，和/或，使用第二计算方式确定第二盐值。

在一种可能实现的方式中，第一设备接收到第二设备的第二信息之后，第一设备根据第二信息确

定自身支持第二设备支持的盐值计算方式，第一设备可以根据第一信息确定第一计算方式和/或第二计算方式。第一设备通过第一计算方式，确定第一设备和第二设备之间上行传输的第一盐值；和/或，第一设备通过第二计算方式，确定第一设备和第二设备之间下行传输的第二盐值。

5 作为一种示例，假设第一设备为 P-CSCF，第二设备为终端设备。P-CSCF 接收到来自终端设备的第二信息之后，P-CSCF 根据第二信息中终端设备支持的盐值计算方式和该第一信息中 P-CSCF 支持的盐值计算方式，确定 P-CSCF 支持终端设备支持的盐值计算方式。P-CSCF 可以根据第一信息，确定第一计算方式和/或第二计算方式，并通过第一计算方式确定第一盐值和/或通过第二计算方式确定第二盐值。

10 应理解，第一设备和第二设备使用第一计算方式和/或第二计算方式，确定第一盐值和/或第二盐值时，使用的参数不同（例如，上行端口号和下行端口号不同），第一计算方式和第二计算方式的内部算法可能相同。即第一设备和第二设备确定的第一盐值和第二盐值不同。在保证第一设备和第二设备之间上行传输和下行传输使用的盐值不同的情况下，第一设备和第二设备上行传输时，第一设备确定的盐值和第二设备确定的盐值相同；第一设备和第二设备下行传输时，第一设备确定的盐值和第二设备确定的盐值相同。即保证了第一设备和第二设备之间的上行、下行的通信安全，还避免了第一设备和第二设备使用不同的密钥，产生加密解密失败的问题。

20 在一种可能实现的方式中，第一设备和第二设备使用第一计算方式确定第一盐值，可以包括第一设备和第二设备使用第一安全参数确定第一盐值。其中，该第一安全参数包括以下一项或者多项：上行传输的方向标识、上行传输的方向标识符、第一设备和/或第二设备的上行端口号、第一设备和/或第二设备的上行 IP 地址、第一设备和/或第二设备的上行 SPI、第一设备和/或第二设备的上行计数器、第一设备和/或第二设备的随机数。

其中，第一设备和第二设备自身能够确定上行传输的方向标识、上行传输的方向标识符、随机数。其中上行传输的方向标识和上行传输的方向标识符还可以是约定的，对此本申请不做具体限定。

25 其中，第一设备的上行端口号、第一设备的上行 IP 地址、第一设备的上行 SPI、第一设备的上行计数器、第一设备的随机数中的一项或者多项可以是第一设备通过第一消息发送给第二设备；第二设备的上行端口号、第二设备的上行 IP 地址、第二设备的上行 SPI、第二设备的上行计数器、第二设备的随机数中的一项或者多项可以是第二设备通过第二消息发送给第一设备。

30 在一种可能实现的方式中，第一设备和第二设备使用第二计算方式确定第二盐值，可以包括第一设备和第二设备使用第二安全参数确定第二盐值。其中，该第二安全参数包括以下一项或者多项：下行传输的方向标识、下行传输的方向标识符、第一设备和/或第二设备的下行端口号、第一设备和/或第二设备的下行 IP 地址、第一设备和/或第二设备的下行 SPI、第一设备和/或第二设备的下行计数器、第一设备和/或第二设备的随机数。

其中，第一设备和第二设备自身能够确定下行传输的方向标识、下行传输的方向标识符、随机数。其中，下行传输的方向标识和下行传输的方向标识符还可以是约定的，对此本申请不做具体限定。

35 其中，第一设备的下行端口号、第一设备的下行 IP 地址、第一设备的下行 SPI、第一设备的下行计数器、第一设备的随机数中的一项或者多项可以是第一设备通过第一消息发送给第二设备；第二设备的下行端口号、第二设备的下行 IP 地址、第二设备的下行 SPI、第二设备的上行计数器、第二设备的随机数中的一项或者多项可以是第二设备通过第二消息发送给第一设备。

40 作为一种示例，假设第一设备支持的盐值计算方式包括方式#1 和方式#2，第二设备支持的盐值计算方式包括方式#2，则第一设备和第二设备根据第一设备支持的盐值计算方式和第二设备支持的盐值计算方式确定第一计算方式为方式#2，第一设备和第二设备使用方式#2，确定第一设备和第二设备之间上行传输的第一盐值。其中，第一设备和第二设备可以分别使用上行传输的方向标识、上行传输的方向标识符、第一设备的上行端口号和第二设备的上行端口通过方式#2，计算第一盐值。

45 作为另一种示例，假设第一设备支持的盐值计算方式包括方式#1，第二设备支持的盐值计算方式包括方式#1，则第一设备和第二设备根据第一设备支持的盐值计算方式和第二设备支持的盐值计算方式确定第二计算方式为方式#1，第一设备和第二设备使用方式#1，确定第一设备和第二设备之间下行传输的第二盐值。其中，第一设备和第二设备可以分别使用下行传输的方向标识符、第一设备的下行 SPI 和第二设备的下行 SPI、第一设备的下行计数器和第二设备的下行计数器通过方式#1，计算第二盐值。

应理解, 使用第一安全参数和第二安全参数确定第一盐值和第二盐值, 能够区分第一设备和第二设备之间的上行传输和下行传输。本领域技术人员还可以通过其他能够区分第一设备和第二设备之间的上行传输和下行传输的参数, 用于确定该第一盐值和第二盐值。

还应理解, 本申请中的第一设备可以是终端设备, 第二设备可以是 P-CSCF; 或者, 第一设备为 P-CSCF, 第二设备为终端设备。

作为一种示例, 当第一设备为终端设备, 第二设备为 P-CSCF 时, 在第一设备和第二设备之间的上行传输中, 终端设备可以作为客户端 (client), P-CSCF 可以作为服务端 (server); 在第一设备和第二设备之间的下行传输中, 终端设备可以作为服务端 (server), P-CSCF 可以作为客户端 (client)。例如, 在第一设备和第二设备之间的上行传输中, 终端设备的上行 SPI 的取值可以表示为 SPI_{uc}, SPI_{uc} 用于表示终端设备作为 client 时的 SPI 值; P-CSCF 的上行 SPI 的取值可以表示为 SPI_{ps}, SPI_{ps} 用于表示 P-CSCF 作为 server 时的 SPI 值。

根据上述图 2 所示的方法, 第一设备与第二设备之间通过交互彼此能够支持的盐值计算方式, 可以使用第一计算方式确定第一设备和第二设备之间的上行传输的第一盐值, 和/或, 可以使用第二计算方式确定第一设备和第二设备之间的下行传输的第一盐值。在第一设备和第二设备之间的下行或者上行传输中, 第一设备和第二设备可以得到相同的盐值, 即能够保证即使第一设备和第二设备中任意一个设备升级或者其他配置发生变化时, 第一设备和第二设备仍然能够根据双方支持的盐值计算方式确定一个计算方式, 第一设备和第二设备通过该计算方式得到的盐值相同, 避免在第一设备和第二设备之间的上行传输或者下行传输中, 第一设备和第二设备确定的盐值不同, 而导致信息加密解密失败的问题。

同时, 本申请实施例中的方法得到的, 用于第一设备与第二设备之间的上行传输的第一盐值, 和用于第一设备与第二设备之间的下行传输的第二盐值不同, 提高了上行、下行的安全性能。

如图 2 所示的方法, 该方法还包括如下步骤:

240, 第一设备使用第一安全参数确定用于上行传输的第一向量, 和/或使用第二安全参数确定用于下行传输的第二向量。

250, 第一设备向第二设备发送第一向量和/或第二向量。

应理解, 第一向量和第二向量不同。

其中, 第一设备通过第一安全参数确定用于上行传输的第一向量, 其中, 第一安全参数为上行传输相关的参数。第一设备通过第二安全参数确定用于下行传输的第二向量, 其中, 第二安全参数为下行传输相关的参数。其中第一安全参数与第二安全参数不同, 则第一向量和第二向量不同。

还应理解, 上述步骤 240 和步骤 250 与图 3 中的步骤 310 至 330 类似, 具体请参看图 3 中的详细介绍, 为了避免冗余此处不再赘述。

图 3 是本申请实施例提供的另一种安全通信方法的流程性示意图。

310, 第一设备使用第一安全参数确定第一向量, 和/或, 第一设备使用第二安全参数确定第二向量。

其中, 第一向量是用于第一设备与第二设备之间的上行传输的; 第二向量是用于第一设备与第二设备之间的下行传输的。

其中, 第一安全参数包括以下一项或者多项: 上行传输的方向标识、上行传输的方向标识符、第一设备和/或第二设备的上行端口号、第一设备和/或第二设备的上行 IP 地址、第一设备和/或第二设备的上行 SPI、第一设备和/或第二设备的上行计数器、第一设备和/或第二设备的随机数; 第二安全参数包括以下一项或者多项: 下行传输的方向标识、下行传输的方向标识符、第一设备和/或第二设备的下行端口号、第一设备和/或第二设备的下行 IP 地址、第一设备和/或第二设备的下行 SPI、第一设备和/或第二设备的下行计数器、第一设备和/或第二设备的随机数。

应理解, 第一安全参数和第二安全参数是用于区分第一设备和第二设备之间上行和下行传输的参数。即第一安全参数与第二安全参数不同。例如, 第一安全参数中包括的第一设备的上行端口号与第二安全参数中包括的第一设备的上行端口号不相同; 第一安全参数中包括的第一设备的上行计数器与第二安全参数中包括的第一设备的上行计数器不相同。

还应理解, 用于确定第一向量的第一安全参数和用于确定第二向量的第二安全参数不同, 则第一向量和第二向量不同。

可选地, 第一向量是第一设备确定的用于上行传输的初始化向量 IV, 第一向量是第一设备确定的

用于下行传输的初始化向量 IV。

320, 第一设备向第二设备发送第一向量和/或第二向量。

具体地, 第一设备确定第一向量和/或第二向量之后, 第一设备将该第一向量和/或第二向量发送给第二设备。

5 可选地, 该第一向量用于第二设备对接收到来自第一设备通过上行通信链路发送的加密消息进行解密处理。该第二向量用于第二设备在下行通信链路上准备为第一设备发送的消息进行加密处理。

应理解, 该第一向量可以与第一设备向第二设备发送的加密消息在同一条消息中传输给第二设备, 或者, 该第一向量也可以承载在其他信令或者算法列表中发送给第二设备, 或者, 该第一向量还可以通过单独的指示信息发送给第二设备, 本申请对此不做具体限定。

10 根据图 3 所示的方法, 第一设备使用区别上行、下行传输的相关参数 (例如, 端口号、方向标识、方向标识符、IP 地址、SPI、计数器、随机数), 确定第一向量和/或第二向量, 并将第一向量和/或第二向量发送给第二设备。其中, 该第一向量是根据上行传输相关的第一安全参数确定的, 第二向量是根据下行传输相关的第二安全参数确定的, 即第一设备和第二设备之间的上行传输和下行传输对应的第一向量和第二向量不同, 从而保证了第一设备和第二设备之间上行、下行的通信安全。

15 应理解, 在本文描述的各个实施例中, 各过程的序号的大小并不意味着执行顺序的先后, 各过程的执行顺序应以其功能和内在逻辑确定, 而不应对本申请实施例的实施过程构成任何限定。

本文中描述的各个实施例可以为独立的方案, 也可以根据内在逻辑进行组合, 这些方案都落入本申请的保护范围内。

20 可以理解的是, 上述各个方法实施例中, 由终端侧实现的方法和操作, 也可以由可用于终端侧设备的部件 (例如芯片或者电路) 实现, 由网络侧实现的方法和操作, 也可以由可用于网络侧设备的部件 (例如芯片或者电路) 实现。

以上, 结合图 2 和图 3 详细说明了本申请实施例提供的方法。以下, 结合图 4 至图 6 详细说明本申请实施例提供的安全通信装置。应理解, 装置实施例的描述与方法实施例的描述相互对应, 因此, 未详细描述的内容可以参见上文方法实施例, 为了简洁, 这里不再赘述。

25 上述主要从各个设备之间交互的角度对本申请实施例提供的方案进行了介绍。可以理解的是, 各个设备, 例如发射端设备或者接收端设备, 为了实现上述功能, 其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该可以意识到, 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, 本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行, 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。

30 本申请实施例可以根据上述方法示例对第一设备或者第二设备进行功能模块的划分, 例如, 可以对应各个功能划分各个功能模块, 也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现, 也可以采用软件功能模块的形式实现。需要说明的是, 本申请实施例中对模块的划分是示意性的, 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。下面以采用对应各个功能划分各个功能模块为例进行说明

35 图 4 是本申请实施例提供的一种安全通信装置的示意性框图。该装置 400 包括收发单元 410, 收发单元 410 可以用于实现相应的通信功能。收发单元 410 还可以称为通信接口或通信单元。

可选地, 该装置 400 还可以包括处理单元 420, 处理单元 420 可以用于进行数据处理。

40 可选地, 该装置 400 还包括存储单元, 该存储单元可以用于存储指令和/或数据, 处理单元 420 可以读取存储单元中的指令和/或数据, 以使得装置实现前述各个方法实施例中不同的终端设备的动作, 例如, 第一设备的动作/第二设备的动作。

45 该装置 400 可以用于执行上文各个方法实施例中第一设备或者第二设备所执行的动作, 这时, 该装置 400 可以为第一设备, 或者第一设备的组成部件, 或者第二设备, 或者第二设备的组成部件, 收发单元 410 用于执行上文方法实施例中第一设备或者第二设备的收发相关的操作, 处理单元 420 用于执行上文方法实施例中第一设备或者第二设备的处理相关的操作。

还应理解, 这里的装置 400 以功能单元的形式体现。这里的术语“单元”可以指应用特有集成电路 (application specific integrated circuit, ASIC)、电子电路、用于执行一个或多个软件或固件程序的处理

理器 (例如共享处理器、专有处理器或组处理器等) 和存储器、合并逻辑电路和/或其它支持所描述的

功能的合适组件。在一个可选例子中，本领域技术人员可以理解，装置 400 可以具体为上述实施例中的第一设备，可以用于执行上述各方法实施例中与第一设备应的各个流程和/或步骤，或者，装置 400 可以具体为上述实施例中的第二设备，可以用于执行上述各方法实施例中与第二设备对应的各个流程和/或步骤，为避免重复，在此不再赘述。

5 上述各个方案的装置 400 具有实现上述方法中第一设备所执行的相应步骤的功能，或者，上述各个方案的装置 400 具有实现上述方法中第二设备所执行的相应步骤的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块；例如收发单元可以由收发机替代（例如，收发单元中的发送单元可以由发送机替代，收发单元中的接收单元可以由接收机替代），其它单元，如处理单元等可以由处理器替代，分别执行各个方法实施例中的收发操作以及相关的处理操作。

10 此外，上述收发单元 410 还可以是收发电路（例如可以包括接收电路和发送电路），处理单元可以是处理电路。

需要指出的是，图 4 中的装置可以是前述实施例中的网元或设备，也可以是芯片或者芯片系统，例如：片上系统（system on chip, SoC）。其中，收发单元可以是输入输出电路、通信接口；处理单元为 15 为该芯片上集成的处理器或者微处理器或者集成电路。在此不做限定。

如图 5 所示，本申请实施例提供另一种通信装置 500。该装置 500 包括处理器 510，处理器 510 与存储器 520 耦合，存储器 520 用于存储计算机程序或指令和/或数据，处理器 510 用于执行存储器 520 存储的计算机程序或指令，或读取存储器 520 存储的数据，以执行上文各方法实施例中的方法。

20 可选地，处理器 510 为一个或多个。

可选地，存储器 520 为一个或多个。

可选地，该存储器 520 与该处理器 510 集成在一起，或者分离设置。

可选地，如图 5 所示，该装置 500 还包括收发器 530，收发器 1130 用于信号的接收和/或发送。例如，处理器 510 用于控制收发器 530 进行信号的接收和/或发送。

作为一种方案，该装置 500 用于实现上文各个方法实施例中由第一设备执行的操作。

25 例如，处理器 510 用于执行存储器 520 存储的计算机程序或指令，以实现上文各个方法实施例中的第一控制面设备的相关操作。例如，图 2 或图 3 中任意一个所示实施例中的第一设备，或者第二设备。

应理解，本申请实施例中提及的处理器可以是中央处理单元（central processing unit, CPU），还可以是其他通用处理器、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 30 其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。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。

还应理解，本申请实施例中提及的存储器可以是易失性存储器和/或非易失性存储器。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）。 35 例如，RAM 可以用作外部高速缓存。作为示例而非限定，RAM 包括如下多种形式：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）。 40

需要说明的是，当处理器为通用处理器、DSP、ASIC、FPGA 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件时，存储器（存储模块）可以集成在处理器中。

还需要说明的是，本文描述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。

45 如图 6，本申请实施例提供一种芯片系统 600。该芯片系统 600（或者也可以称为处理系统）包括逻辑电路 610 以及输入/输出接口（input/output interface）620。

其中，逻辑电路 610 可以为芯片系统 600 中的处理电路。逻辑电路 610 可以耦合连接存储单元，调用存储单元中的指令，使得芯片系统 600 可以实现本申请各实施例的方法和功能。输入/输出接口 620，

可以为芯片系统 600 中的输入输出电路, 将芯片系统 600 处理好的信息输出, 或将待处理的数据或指令信息输入芯片系统 600 进行处理。

作为一种方案, 该芯片系统 600 用于实现上文各个方法实施例中由第一设备或者第二设备执行的操作。

- 5 例如, 逻辑电路 610 用于实现上文方法实施例中由第一设备的处理相关的操作, 或者由第二设备的处理相关的操作, 如图 2 或图 3 中任意一个所示实施例中的第一设备或者第二设备的处理相关的操作; 输入/输出接口 620 用于实现上文方法实施例中由第一设备的发送和/或接收相关的操作, 或者由第二设备的发送和/或接收相关的操作。

- 10 本申请实施例还提供一种计算机可读存储介质, 其上存储有用于实现上述各方法实施例中由第一设备、第二设备执行的方法的计算机指令。

例如, 该计算机程序被计算机执行时, 使得该计算机可以实现上述方法各实施例中由第一设备、第二设备执行的方法。

本申请实施例还提供一种计算机程序产品, 包含指令, 该指令被计算机执行时以实现上述各方法实施例中由第一设备、第二设备执行的方法。

- 15 上述提供的任一种装置中相关内容的解释及有益效果均可参考上文提供的对应的方法实施例, 此处不再赘述。

- 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。此外, 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。

- 20 在上述实施例中, 可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时, 可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时, 全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。例如, 所述计算机可以是个人计算机, 服务器, 或者网络设备等。所述计算机指令可以存储在计算机可读存储介质中, 或者从一个计算机可读存储介质向另一个计算机可读存储介质传输, 例如, 所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。
- 25 所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质(例如, 软盘、硬盘、磁带)、光介质(例如, DVD)、或者半导体介质(例如固态硬盘(solid state disk, SSD)等。例如, 前述的可用介质包括但不限于: 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。

- 30 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以所述权利要求的保护范围为准。

权 利 要 求 书

1. 一种安全通信方法，其特征在于，包括：
第一设备通过第一消息向第二设备发送所述第一设备的第一信息，所述第一消息包括第一端口号、
5 第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的一项或多项；
所述第一设备接收来自所述第二设备的包括第二信息的第二消息，所述第二消息包括第二端口号、
第二安全参数索引 SPI、第二互联网协议 IP 地址、第二安全算法列表、第二随机数中的一项或多项；
所述第一设备根据所述第一信息和/或所述第二信息，使用第一计算方式确定用于所述第一设备与
10 所述第二设备之间的上行传输的第一盐值，和/或，使用第二计算方式确定用于所述第一设备与所述第
二设备之间的下行传输的第二盐值。
2. 根据权利要求 1 所述的方法，其特征在于，所述第一信息包括在所述第一消息的第一端口号、
第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的一项；和/或
所述第二信息包括在所述第二消息的第二端口号、第二安全参数索引 SPI、第二互联网协议 IP 地
址、第二安全算法列表、第二随机数中的一项中。
- 15 3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述使用所述第一计算方式确定所述第一盐值
包括：
使用第一安全参数计算所述第一盐值，
其中，所述第一安全参数包括以下一项或者多项：所述上行传输的方向标识、所述上行传输的方
向标识符、所述第一设备和/或所述第二设备的上行端口号、所述第一设备和/或所述第二设备的上行 IP
20 地址、所述第一设备和/或所述第二设备的上行 SPI、所述第一设备和/或所述第二设备的上行计数器、
所述第一设备和/或所述第二设备的随机数；
所述使用所述第二计算方式确定所述第二盐值包括：
使用第二安全参数计算所述第二盐值，
其中，所述第二安全参数包括以下一项或者多项：所述下行传输的方向标识、所述下行传输的方
25 向标识符、所述第一设备和/或所述第二设备的下行端口号、所述第一设备和/或所述第二设备的下行 IP
地址、所述第一设备和/或所述第二设备的下行 SPI、所述第一设备和/或所述第二设备的下行计数器、
所述第一设备和/或所述第二设备的随机数。
4. 根据权利要求 3 所述的方法，其特征在于，所述方法还包括：
所述第一设备使用所述第一安全参数确定用于所述上行传输的第一向量，和/或使用所述第二安全
30 参数确定用于所述下行传输的第二向量；
所述第一设备向所述第二设备发送所述第一向量和/或所述第二向量。
5. 一种安全通信方法，其特征在于，包括：
第一设备通过第一消息向第二设备发送所述第一设备的第一信息，所述第一消息包括第一端口号、
35 第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的一项或多项；
所述第二设备接收来自所述第一设备通过第一消息发送的所述第一设备的第一信息；
所述第一设备接收来自所述第二设备的包括第二信息的第二消息，所述第二消息包括第二端口号、
第二安全参数索引 SPI、第二互联网协议 IP 地址、第二安全算法列表、第二随机数中的一项或多项；
所述第一设备根据所述第一信息和/或所述第二信息，使用第一计算方式确定用于所述第一设备与
40 所述第二设备之间的上行传输的第一盐值，和/或，使用第二计算方式确定用于所述第一设备与所述第
二设备之间的下行传输的第二盐值。
6. 一种安全通信方法，其特征在于，包括：
第一设备使用第一安全参数确定用于所述第一设备与第二设备之间的上行传输的第一向量，
所述第一设备向所述第二设备发送所述第一向量；
和/或，
45 所述第一设备使用第二安全参数确定用于所述第一设备与所述第二设备之间的下行传输的第二向
量；
所述第一设备向所述第二设备发送所述第二向量，

- 其中,所述第一安全参数包括以下一项或者多项:上行传输的方向标识、上行传输的方向标识符、第一设备和/或第二设备的上行端口号、第一设备和/或第二设备的上行 IP 地址、第一设备和/或第二设备的上行 SPI、第一设备和/或第二设备的上行计数器、第一设备和/或第二设备的随机数;第二安全参数包括以下一项或者多项:下行传输的方向标识、下行传输的方向标识符、第一设备和/或第二设备的下行端口号、第一设备和/或第二设备的下行 IP 地址、第一设备和/或第二设备的下行 SPI、第一设备和/或第二设备的下行计数器、第一设备和/或第二设备的随机数。
- 5 7. 一种安全通信方法,其特征在于,包括:
第一设备使用第一安全参数确定用于所述第一设备与第二设备之间的上行传输的第一向量,
所述第一设备向所述第二设备发送所述第一向量;
10 所述第二设备接收来自所述第一设备的所述第一向量;
和/或,
所述第一设备使用第二安全参数确定用于所述第一设备与所述第二设备之间的下行传输的第二向量;
所述第一设备向所述第二设备发送所述第二向量;
15 所述第二设备接收来自所述第一设备的所述第二向量,
其中,第一安全参数包括以下一项或者多项:上行传输的方向标识、上行传输的方向标识符、第一设备和/或第二设备的上行端口号、第一设备和/或第二设备的上行 IP 地址、第一设备和/或第二设备的上行 SPI、第一设备和/或第二设备的上行计数器、第一设备和/或第二设备的随机数;第二安全参数包括以下一项或者多项:下行传输的方向标识、下行传输的方向标识符、第一设备和/或第二设备的下行端口号、第一设备和/或第二设备的下行 IP 地址、第一设备和/或第二设备的下行 SPI、第一设备和/或第二设备的下行计数器、第一设备和/或第二设备的随机数。
- 20 8. 根据权利要求 1 至 7 中任一项所述的方法,其特征在于,所述第一设备为终端设备或者所述第一设备配置于所述终端设备中的芯片或者电路,所述第二设备为网络设备或者所述第二设备配置于所述网络设备中的芯片或者电路;
25 或者,
所述第一设备为所述网络设备或者所述第一设备配置于所述网络设备中的芯片或者电路,所述第二设备为所述终端设备或者所述第二设备配置于所述终端设备中的芯片或者电路。
9. 一种安全通信装置,其特征在于,所述安全通信装置包括用于执行如权利要求 1 至 8 中任一项所述方法的单元和模块。
- 30 10. 一种安全通信装置,包括处理器,所述处理器和存储器耦合,所述存储器用于存储指令,所述处理器用于读取所述存储器中存储的指令,使得所述安全通信装置实现上述权利要求 1 至 8 中任一项所述的方法。
11. 一种计算机可读存储介质,其特征在于,所述计算机可读存储介质上存储有指令,当所述指令在计算机上运行时,使得所述计算机执行如权利要求 1 至 8 中任一项所述的方法。
- 35 12. 一种计算机程序产品,其特征在于,所述计算机程序产品中包括用于执行上述权利要求 1 至 8 中任一项所述的方法的指令。
13. 一种芯片,其特征在于,所述芯片包括处理器与通信接口,所述处理器通过所述通信接口读取计算机程序或指令并运行时,使得所述通信装置执行如权利要求 1 至 8 中任一项所述的方法。
14. 一种通信系统,其特征在于,包括第一设备和第二设备,所述第一设备用于执行如权利要求 1 至 4 中任一项所述的方法;所述第二设备用于:
40 通过第一消息接收所述第一设备的第一信息,所述第一消息包括第一端口号、第一安全参数索引 SPI、第一互联网协议 IP 地址、第一安全算法列表、第一随机数中的一项或多项;
向所述第一设备发送包括第二信息的第二消息,所述第二消息包括第二端口号、第二安全参数索引 SPI、第二互联网协议 IP 地址、第二安全算法列表、第二随机数中的一项或多项。
- 45 15. 一种通信系统,其特征在于,包括第一设备和第二设备,所述第一设备用于执行如权利要求 6 所述的方法;所述第二设备用于:接收第一向量和/或第二向量。