(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 7 月 2 日 (02.07.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/134413 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/112548

(22) 国际申请日: 2019 年 10 月 22 日 (22.10.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811628535.8 2018年12月28日 (28.12.2018) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 毛玉欣 (MAO, Yuxin); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 闫新成 (YAN, Xincheng); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 吴华强 (WU, Huaqiang); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。 刘艳昌 (LIU, Yanchang); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京康信知识产权代理有限责任公司 (KANGXIN PARTNERS, P.C.); 中国北京市海淀区知春路甲48号盈都大厦A座16层, Beijing 100098 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) **Title:** DATA TRANSMISSION METHOD AND APPARATUS, RELATED DEVICE, AND STORAGE MEDIUM

(54) **发明名称:** 一种数据传输方法、装置、相关设备及存储介质

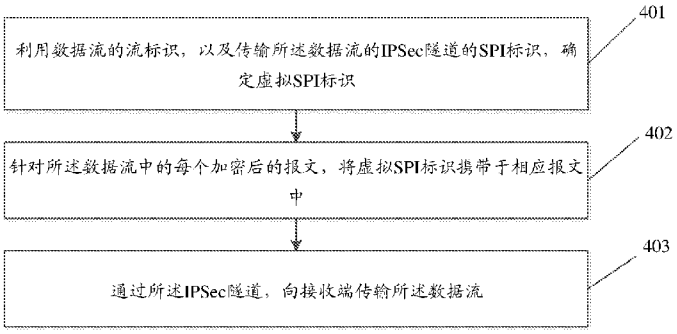

图 4

401 Determine a virtual SPI identifier by using a stream identifier of a data stream, and an SPI identifier of an IPSec tunnel for transmitting the data stream
402 Carry the virtual SPI identifier in a corresponding packet for each encrypted packet in the data stream
403 Transmit the data stream to a receiving end by means of the IPSec tunnel

(57) **Abstract:** Disclosed are a data transmission method and apparatus, a related device, and a storage medium. The method comprises: determining a virtual security parameter index (SPI) identifier by using a stream identifier of a data stream, and an SPI identifier of an Internet protocol security (IPSec) tunnel for transmitting the data stream; carrying the virtual SPI identifier in a corresponding packet for each encrypted packet in the data stream; and transmitting the data stream to a receiving end by means of the IPSec tunnel, the virtual SPI identifier being used by the receiving end to deliver packets of the data stream into the same decryption unit for decrypting.

WO 2020/134413 A1

[见续页]

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

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

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本申请公开了一种数据传输方法，装置、相关设备及存储介质。其中，该方法包括：利用数据流的流标识，以及传输所述数据流的网络协议安全(IPSec，Internet Protocol Security)隧道的安全参数索引(SPI，Security Parameter Index)标识，确定虚拟SPI标识；针对所述数据流中的每个加密后的报文，将虚拟SPI标识携带于相应报文中；通过所述IPSec隧道，向接收端传输所述数据流；所述虚拟SPI标识用于供所述接收端将所述数据流的各报文送入同一个解密单元进行解密处理。

一种数据传输方法、装置、相关设备及存储介质

技术领域

本申请涉及网络通信安全技术领域，尤其涉及一种数据传输方法、装置、相关设备及存储介质。

背景技术

目前，在第五代移动通信（5G，the 5th Generation mobile communication technology）网络中，为保证数据传输的安全性，通常会使用 IPSec 隧道对数据进行完整性保护。目前，为了提高 IPSec 隧道的处理性能，加密端将数据流通过 IPSec 隧道传输至解密端后，解密端会按照预设算法将数据流的各报文传输至多个解密单元进行解密处理。

上述方式解密端通过多个解密单元对数据流的各报文进行分别处理，很可能会加剧报文乱序。

发明内容

为解决存在的相关技术问题，在本申请实施例中提供了一种数据传输方法、装置、相关设备及存储介质。

本申请实施例的技术方案是这样实现的：

本申请实施例提供了一种数据传输方法，应用于发送端，所述方法包括：利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识；针对所述数据流中的每个加密后的报文，将虚拟 SPI 标识携带于相应报文中；通过所述 IPSec 隧道，向接收端传输所述数据流；所述虚拟 SPI 标识用于供所述接收端将所述数据流的各报文送入同一个解密单元进行解密处理。

本申请实施例提供了一种数据传输方法，应用于接收端，所述方法包括：接收发送端通过 IPSec 隧道发送的数据流；所述数据流的各报文中携带有虚拟 SPI 标识；所述虚拟 SPI 标识是所述发送端基于所述数据流的流标识以及传输

所述数据流的 IPSec 隧道的 SPI 标识确定的；利用虚拟 SPI 标识，将所述数据流的各报文送入同一个解密单元进行解密处理。

本申请实施例提供了一种数据传输装置，应用于发送端，所述装置包括：第一确定单元，设置为利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识；加密单元，设置为针对所述数据流中的每个加密后的报文，将虚拟 SPI 标识携带于相应报文中；第一传输单元，设置为通过所述 IPSec 隧道，向接收端传输所述数据流；所述虚拟 SPI 标识用于供所述接收端将所述数据流的各报文送入同一个解密单元进行解密处理。

本申请实施例提供了一种数据传输装置，应用于接收端，所述装置包括：第一接收单元，设置为接收发送端通过 IPSec 隧道发送的数据流；所述数据流的各报文中携带有虚拟 SPI 标识；所述虚拟 SPI 标识是所述发送端基于所述数据流的流标识以及传输所述数据流的 IPSec 隧道的 SPI 标识确定的；第一解密单元，设置为利用虚拟 SPI 标识，将所述数据流的各报文送入同一个解密单元进行解密处理。

本申请实施例提供了一种数据传输装置，应用于发送端，所述装置包括：第一确定单元，设置为确定数据流的区分标识；还设置为利用数据流的区分标识与子 IPSec 隧道的 SPI 标识的映射关系，确定所述数据流传输所使用的子 IPSec 隧道；第二传输单元，设置为利用确定的子 IPSec 隧道，向接收端传输所述数据流；通过所述确定的子 IPSec 隧道将所述数据流传输至所述接收端的与所述子 IPSec 隧道对应的解密单元进行解密处理。

本申请实施例提供了一种数据传输装置，应用于接收端，所述装置包括：第二接收单元，设置为接收发送端通过子 IPSec 隧道发送的数据流；第二解密单元，设置为将通过子 IPSec 隧道传输的所述数据流发送至与所述子 IPSec 隧道对应的解密单元进行解密处理。

本申请实施例提供了一种发送设备，包括：第一处理器和设置为存储能够在处理器上运行的计算机程序的第一存储器，其中，所述第一处理器设置为运行所述计算机程序时，执行上面所述任一项发送端数据传输方法的步骤。

本申请实施例提供了一种接收设备，包括：第二处理器和设置为存储能够在处理器上运行的计算机程序的第二存储器，其中，所述第一处理器设置为运行所述计算机程序时，执行上面所述任一项接收端数据传输方法的步骤。

本申请实施例提供了一种存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现上面所述任一项数据传输方法的步骤。

本申请实施例提供的数据传输方法、装置、相关设备及存储介质，利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识；针对所述数据流中的每个加密后的报文，将虚拟 SPI 标识携带于相应报文中；通过所述 IPSec 隧道，向接收端传输所述数据流；所述虚拟 SPI 标识用于供所述接收端将所述数据流的各报文送入同一个解密单元进行解密处理。采用本申请实施例的方案，所述发送端将携带有虚拟 SPI 标识的各报文发送给接收端，这样，所述接收端可以将具有相同虚拟 SPI 标识的报文送入同一个解密单元进行解密处理。如此，可避免报文乱序问题的发生，同时还能提高 IPSec 隧道的处理性能。

附图说明

图 1 为相关技术中 IPSec 隧道的示意图；

图 2 为相关技术中通过 IPSec 隧道进行数据传输的示意图；

图 3 为相关技术中报文乱序的示意图；

图 4 为本申请实施例数据传输方法的实现流程示意图一；

图 5 为本申请实施例数据传输方法的实现流程示意图二；

图 6 为本申请实施例数据传输方法的实现流程示意图三；

图 7 为本申请实施例数据传输方法的实现流程示意图四；

图 8 为本申请实施例确定虚拟 SPI 标识的示意图；

图 9 为本申请实施例对报文进行解密的示意图；

图 10 为本申请实施例通过子 IPSec 隧道传输数据流的示意图；

图 11 为本申请实施例数据传输装置的组成结构示意图一；

图 12 为本申请实施例数据传输装置的组成结构示意图二；

图 13 为本申请实施例数据传输装置的组成结构示意图三；

图 14 为本申请实施例数据传输装置的组成结构示意图四；

图 15 为本申请实施例数据传输装置的组成结构示意图五；

图 16 为本申请实施例数据传输装置的组成结构示意图六。

具体实施方式

下面结合附图及实施例对本申请再作进一步详细的描述。

目前，为了保证数据传输的安全性以及对数据的完整性进行保护，需要在所述发送端与所述接收端之间建立 IPSec 隧道。IPSec 隧道可以用安全联盟（SA，Security Association）表示。在正式建立 IPSec 隧道之前，发送端和接收端需要进行协商，以建立 SA。由于 IPSec 隧道是单向的，因此，一个 IPSec 隧道包括两个 SA，每个 SA 可以使用 SPI 进行唯一标识。SA 约定了隧道两端使用相同的封装模式、加密算法、加密密钥、验证算法、验证密钥。其中，封装模式可以包括封装安全载荷(ESP，Encapsulating Security Payload)、验证头（AH，Authentication Header)；加密算法可以包括数据加密标准(DES，Data Encryption Standard)、数字加密标准 3(3DES，Triple DES)、高级加密标准(AES，Advanced Encryption Standard)；验证算法可以包括消息摘要 5(MD5，Message Digest 5)、安全哈希算法 1(SHA1，Secure Hash Algorithm1)、安全哈希算法 2（SHA，Secure Hash Algorithm12）。

这里，IPSec 隧道的建立方式可以包括手动建立方式和因特网密钥交换协议(IKE，Internet Key Exchange)动态协商建立方式。

手动建立方式可以包括以下步骤：

步骤 1，配置 ACL，通过访问控制列表（ACL，Access Control List）定义需要保护的数据流，即 ACL 包含需要保护的数据流的标识，通常为五元组。

这里，只有 ACL 定义的数据流才被 IPSec 隧道保护，其他数据流不受保护。

步骤 2，建立 IPSec SA。

可选地，配置 IPSec 安全提议：隧道两端在各自的安全提议中配置相同的封装模式、加密算法、验证算法。配置 IPSec 安全策略：定义隧道两端使用的地址、SA 标识符 SPI、加密密钥、验证密钥等等。配置应用 IPSec 安全策略，建立 IPSec 隧道，按照 ACL 策略并通过建立的 IPSec 隧道对报文传输。

IKE 动态协商方式可以包括以下步骤：

步骤 1，配置 ACL，通过 ACL 定义被保护的数据流，即 ACL 包含需要保

护的数据流的标识。

这里，如果使用 IKEv1，则不协商 ACL 规则，隧道两端设备配置的 ACL 规则互为镜像，避免 IPSec SA 协商失败。如果使用 IKEv2，则通过传输选择器(TS，Traffic Selector)载荷实现两端设备的 ACL 规则协商，最终结果取双方 ACL 规则的交集。

步骤 2，建立 IKE SA。

可选地，协商 IKE 安全提议：配置建立 IKE SA 时的加密和验证算法，协商消息接收方在自己配置的 IKE 安全提议中寻找与发送方相匹配的 IKE 安全提议，如果没有匹配的安全提议则协商失败.配置 IKE 对等体：配置 IKE 版本、身份认证和交换模式。建立 IPSec SA：可选地，配置 IPSec 安全提议：隧道两端在各自的安全提议中配置相同的封装模式、加密算法、验证算法。配置 IPSec 安全策略：定义隧道两端使用的地址、SA 标识符 SPI、加密密钥、验证密钥等等。配置应用 IPSec 安全策略，建立 IPSec 隧道，按照 ACL 策略并通过建立的 IPSec 隧道对报文传输。

这里，IKE 动态协商建立方式中，增加了 IKE SA 建立的过程。

需要说明的是，手动建立方式和 IKE 方式协商方式都必须要求隧道两端所使用的 IP 地址固定。建立 IPSec 隧道后，发送端在接收一个数据流后，首先根据 ACL 判断所述数据流的各报文是否使用 IPSec 加密，如果需要，则查找对应的 SA，利用所述 SA 将加密后的各报文发送给接收端。接收端对所述数据流的加密后的各报文进行解密，并向报文目的地转发解密后的各报文。

图 1 是 IPSec 隧道的示意图，如图 1 所示，在网关 A 和网关 B 之间建立 IPSec 隧道 1（用 SA1 表示），用于供网关 A 发送数据、网关 B 接收数据；并建立 IPSec 隧道 2（用 SA2 表示），用于供网关 B 发送数据、网关 A 接收数据。

图 2 是通过 IPSec 隧道进行数据传输的示意图，如图 2 所示，5G 网络中的集中单元(CU，Central Unit)所在的数据中心和分布式单元（DU，Distributed Unit）所在的数据中心在非信任网络中进行数据传输时，需要在两个数据中心之间建立 IPSec 隧道，以对数据进行完整性保护，防止数据被窃取或篡改。此外，无线接入和核心网之间的回传网、业务网络网元和管理域网元之间的管理编排网络也存在数据安全传输的需求。5G 网络中，对数据传输的速率存在极高的需求，比如，国际电信联盟（ITU，International Telecommunication Union）定义了单

用户峰值速率需达到 10-20Gbps，对回传网的数据速率要求更高。如果数据传输路径上需要使用 IPSec 隧道，则要求 IPSec 隧道的处理性能也应达到相应要求。

目前，IPSec 隧道的处理性能受限于硬件处理性能的局限，如果加密端或解密端分别使用单一处理单元对报文进行加密或解密，IPSec 隧道仅能达到数百 Mbps 的处理性能。如果加密端或解密端分别使用多处理单元或分布式处理单元，加密端将数据流通过 IPSec 隧道传输至解密端后，解密端会按照预设算法将数据流的各报文传输至多个解密单元进行解密处理。这样，虽然可提升 IPSec 隧道的处理性能，但分流处理会加剧报文乱序，影响到业务体验。

图 3 是相关技术中报文乱序的示意图，如图 3 所示，数据流由报文 A、报文 B、报文 C、报文 D 组成。网关 A 接收到数据流后，网关 A 按照预设算法，将报文 A 分配给处理单元 1 进行加密处理，将报文 B 分配给处理单元 2 进行加密处理，将报文 C 分配给处理单元 3 进行加密处理，将报文 D 分配给处理单元 4 进行加密处理，并通过 IPSec 隧道将加密后的各报文发送给网关 B。网关 B 接收到数据流的各加密报文后，按照预设算法，将加密后的报文 A 分配给处理单元 1 进行解密处理，将加密后的报文 B 分配给处理单元 2 进行解密处理，将加密后的报文 C 分配给处理单元 3 进行解密处理，将加密后的报文 D 分配给处理单元 4 进行解密处理。由于每个处理单元接收报文的时序可能不同，每个处理单元对报文的处理方式可能不同，因此，可能会导致报文乱序问题的发生。

基于此，在本申请的各种实施例中，利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识；针对所述数据流中的每个加密后的报文，将虚拟 SPI 标识携带于相应报文中；通过所述 IPSec 隧道，向接收端传输所述数据流；所述虚拟 SPI 标识用于供所述接收端将所述数据流的各报文送入同一个解密单元进行解密处理。

本申请实施例提供一种数据传输方法，应用于发送端，如图 4 所示，该方法包括：

步骤 401：利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识。

其中，IPSec，即 IP Security，它是 IETF 制定的三层隧道加密协议，可以是基于端对端的安全模式，在源 IP 地址和目的 IP 地址之间建立信任和安全性。

这里，为了保证数据传输的安全性，可以在所述发送端和接收端之间建立多条 IPSec 隧道，并用 SPI 标识进行唯一标识。其中，所述接收端为每条 IPSec 隧道分配多个解密单元。

实际应用时，为了使所述接收端在对所述数据流的各报文进行解密前，就能够将同一个数据流的各报文送入多个解密单元中的同一个解密单元进行解密处理，可以利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识；所述虚拟 SPI 标识用于供所述接收端将具有相同虚拟 SPI 标识的报文送入同一个解密单元进行处理。

这里，在确定虚拟 SPI 标识之前，所述发送端还需要针对虚拟 SPI 支持能力与所述接收端进行协商，以确定所述接收端是否具有支持虚拟 SPI 的能力。

基于此，在一个可选的实施例中，所述利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识之前，所述方法还包括：判断所述接收端是否具有支持虚拟 SPI 的能力；当确定所述接收端具有支持虚拟 SPI 的能力时，利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识。

这里，所述发送端与所述接收端关于是否支持虚拟 SPI 的能力进行协商，协商的过程可以为：所述发送端对所述数据流的 IPSec 隧道的 SPI 标识进行设置，比如将 SPI 标识的最高比特位设置为 1，以表征所述发送端具有支持虚拟 SPI 的能力；所述发送端将设置的 SPI 标识发送至所述接收端；所述接收端读取所述发送端支持虚拟 SPI 能力；所述接收端也进行 SPI 最高位设置，并将设置的 SPI 标识发送至所述发送端；所述发送端根据所述接收端发送的 SPI 标识，确定所述接收端是否具有支持虚拟 SPI 的能力，可选地，如果所述接收端将最高位的取值设置为 1，则表示所述接收端具有支持虚拟 SPI 的能力，如表 1 所示；如果所述接收端将最高位的取值设置为 0，则表示所述接收端不具有支持虚拟 SPI 的能力，如表 2 所示。

1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	**0**	**0**	**0**	**0**

表 1

0	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

表 2

这里，在对所述接收端是否具有支持虚拟 SPI 的能力进行确认之前，所述

发送端与所述接收端还需要进行 IKE SA、IPSec SA 的协商，以确定数据流传输所使用的 IPSec 隧道，即建立 IPSec 安全策略，IPSec 安全策略包含所述数据流的流标识与 IPSec 隧道的 SPI 标识的映射关系。

基于此，在一实施例中，所述利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识之前，所述方法还包括：与所述接收端进行 IPSec SA 协商；建立 IPSec 隧道；其中，在建立 IPSec 隧道的过程中，建立 IPSec 安全策略，在所述 IPSec 安全策略中包含所述数据流的流标识和所述 IPSec 隧道的 SPI 标识的映射关系。

可选地，为所述数据流建立 ACL，ACL 中包含所述数据流的流标识，并建立所述数据流的流标识和 IPSec 隧道的 SPI 标识的映射关系。

这里，所述发送端与所述接收端进行 IPSec SA 协商的内容可以包括隧道两端使用的封装模式、加密算法、加密密钥、验证算法、验证密钥等等。

实际应用时，如果所述发送端确定所述接收端具备支持虚拟 SPI 的能力，则所述发送端向所述接收端传输所述数据流之前，可以将所述数据流的流标识经过哈希得到的哈希值填入 SPI 标识的字段中，得到虚拟 SPI 标识。

基于此，在一个可选的实施例中，所述利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识，包括：对所述数据流的流标识进行哈希运算处理，得到哈希值；利用得到的哈希值设置所述 SPI 标识的字段，得到虚拟 SPI 标识。

这里，可以利用得到的哈希值，设置所述 SPI 标识中特定位置的字段。比如，假设所述 SPI 标识可以用 26 比特表示，则所述特定位置可以是指 26 比特中的末四位比特等等。

这里，对所述数据流的流标识进行哈希运算处理，可以得到预设长度的哈希值。流标识不同的数据流，得到的哈希值也不同，对应的虚拟 SPI 标识也就不同。

实际应用时，所述发送端将所述数据流发送至所述接收端之前，还需要对所述数据流的各报文进行加密。

基于此，在一个可选的实施例中，所述方法还包括：对所述数据流中的每个报文进行加密，得到加密后的各报文。

这里，所述发送端可以按照与所述接收端进行 IPSec SA 协商时确定的加密算法对所述数据流的各报文进行加密。

步骤 402：针对所述数据流中的每个加密后的报文，用虚拟 SPI 标识封装。

这里，为了提高 IPSec 隧道的处理性能，所述发送端可以使用多个加密单元对所述数据流的各报文分别进行加密并封装虚拟 SPI 标识。

步骤 403：通过所述 IPSec 隧道，向接收端传输所述数据流；所述虚拟 SPI 标识用于供所述接收端将所述数据流的各报文送入同一个解密单元进行解密处理。

本申请实施例提供了一种数据传输方法，应用于接收端，如图 5 所示，所述方法包括：

步骤 501：接收发送端通过 IPSec 隧道发送的数据流。所述数据流的各报文中携带有虚拟 SPI 标识。

其中，所述虚拟 SPI 标识是所述发送端基于所述数据流的流标识以及传输所述数据流的 IPSec 隧道的 SPI 标识确定的。

这里，所述发送端和接收端之间可建立多条 IPSec 隧道，并用 SPI 标识进行唯一标识。其中，所述接收端为每条 IPSec 隧道分配多个解密单元。

步骤 502：利用虚拟 SPI 标识，将所述数据流的各报文送入同一个解密单元进行解密处理。

这里，所述接收端利用虚拟 SPI 标识，将所述数据流的各报文送入多个解密单元中的同一个解密单元进行解密处理。

实际应用时，为了提高 IPSec 隧道的处理性能，所述接收端可以包括多个解密单元。所述接收端可以根据虚拟 SPI 标识将具有相同虚拟 SPI 标识的报文送入同一个解密单元进行解密处理，以避免因为多解密单元处理加剧报文乱序。其中，具有相同虚拟 SPI 标识的报文，表示属于同一条数据流，由同一个解密单元处理。

基于此，在一个可选的实施例中，所述利用虚拟 SPI 标识，将所述数据的各报文送入同一个解密单元进行解密处理，包括：将具有相同虚拟 SPI 标识的报文送入同一个解密单元，以进行解密处理。

可选地，可以将所述数据流的各报文的虚拟 SPI 标识进行比较，具备相同

虚拟 SPI 标识的各报文送入多个解密单元中的同一个解密单元，以进行解密处理。

采用本申请实施例的方案，所述发送端将携带有虚拟 SPI 标识的各报文发送至所述接收端，这样，所述接收端可以基于各报文携带的虚拟 SPI 标识，将具有相同虚拟 SPI 标识的各报文送入同一个解密单元进行解密处理。如此，可避免因为属于同一 IPSec 隧道的多个解密单元同时处理报文而加剧报文乱序的发生。

本申请实施例还提供了一种数据传输方法，应用于发送端，如图 6 所示，所述方法包括:

步骤 601: 确定数据流的区分标识。

其中，所述数据流的区分标识可以由五元组及以下信息至少之一组成: L2 层的信息、L3 层的信息、L4 层的信息、L5 层的信息、L6 层的信息、L7 层的信息。所述区分标识能够唯一区分所述数据流。

这里，所述五元组可以包括: 源 IP 地址、目的 IP 地址，源端口号、目的端口号以及协议号。L2 至 L7 层为开放系统互联（OSI，Open System Interconnection）参考模型定义的各层。L2 层信息可以包括与链路相关的信息; L3 层信息可以包括 IP 地址; L4 层信息可以包括协议信息，比如 TCP 协议、UDP 协议; L5 层信息可以包括与会话层相关的信息，比如服务质量参数; L6 层信息可以包括数据格式，比如 ASCII 格式等等; L7 层信息可以包括所述数据流的应用类型。所述应用类型包括但不限于 HTTP 应用类型、RTP 应用类型等等。

可选地，可以将五元组放置在前面，将 L2 层至 L7 层中至少一个信息放置在后面，得到所述数据流的区分标识。

步骤 602: 利用数据流的区分标识与子 IPSec 隧道的 SPI 标识的映射关系，确定与所述数据流传输所使用的子 IPSec 隧道。

实际应用时，为了满足 5G 数据传输速率的需求，可以在所述发送端和接收端之间建立多条子 IPSec 隧道，并用 SPI 标识进行唯一标识。一条子 IPSec 隧道在所述接收端分配一个解密单元。

这里，所述发送端对所述数据流进行传输前，所述发送端与所述接收端还

需要进行 IKE SA、Child SA 的协商，以确定数据流传输所使用的子 IPSec 隧道，即建立子 IPSec 安全策略，包含所述数据流的区分标识与子 IPSec 隧道的 SPI 标识的映射关系。

基于此，在一个可选的实施例中，所述方法还包括：与所述接收端进行 Child SA 协商；建立子 IPSec 隧道；其中，在建立子 IPSec 隧道的过程中，建立子 IPSec 隧道安全策略，在所述子 IPSec 隧道安全策略中包含所述数据流的区分标识和子 IPSec 隧道的 SPI 标识的映射关系。

这里，所述发送端与所述接收端进行 Child SA 协商的内容可以包括隧道两端使用的封装模式、加密算法、加密密钥、验证算法、验证密钥等等。

步骤 603：利用确定的子 IPSec 隧道，向接收端传输所述数据流。

这里，通过所述确定的子 IPSec 隧道将所述数据流中加密后的各报文传输至所述接收端的与所述子 IPSec 隧道对应的解密单元进行解密处理。

本申请实施例提供了一种数据传输方法，应用于接收端，如图 7 所示，所述方法包括：

步骤 701：接收发送端通过子 IPSec 隧道发送的数据流。

其中，所述子 IPSec 隧道是所述发送端基于所述数据流的区分标识与子 IPSec 隧道的 SPI 标识的映射关系确定的。

步骤 702：将通过子 IPSec 隧道传输的所述数据流发送至与所述子 IPSec 隧道对应的解密单元进行解密处理。

这里，为了满足 5G 数据传输速率的需求，可以在所述发送端和接收端之间建立多条子 IPSec 隧道，并用 SPI 标识进行唯一标识。一条子 IPSec 隧道在所述接收端分配一个解密单元。

这里，所述发送端与所述接收端关于建立子 IPSec 隧道进行协商的过程已在上文详述，这里不再赘述。

采用本申请实施例的方案，一条子 IPSec 隧道在所述接收端分配一个解密单元，这样，所述接收端可以将所述数据流的各报文送入与子 IPSec 隧道对应的解密单元进行解密处理。如此，可避免因为报文经过 IPSec 传输引发的报文乱序。另外，所述接收端与所述发送端之间建立多条子 IPSec 隧道，可以同对多个数据流进行处理，从而提高了 IPSec 隧道的处理能力，进而能够满足 5G 数

据传输速率的需求。

下面结合应用实施例对本申请再作进一步详细的描述。

应用实施例一

本应用实施例中，接收端通过虚拟 SPI 标识，将具有相同虚拟 SPI 标识的 GTP 报文送入多个解密单元中的同一个解密单元进行解密处理。

另外，本应用实施例中，为一条 IPSec 隧道在所述接收端分配多个解密单元。发送端用网关 A 表示，接收端用网关 B 表示。在 5G 网络中，以 DU 侧部署网关 A，CU 侧部署网关 B 为例。

GTP 协议是电信网络中常用的协议，GTP 报文在 5G 网络的传输过程中对保序有很高要求，如果传输过程中加剧报文乱序，则会导致处理性能下降，甚至严重影响业务体验。所述网关 A 与所述网关 B 进行 IPSec 隧道协商的过程，以及关于是否支持虚拟 SPI 的能力进行协商的过程可以参考上述描述，在此不再赘述。

图 8 为网关 A 使用 IPSec 隧道发送数据报文之前封装虚拟 SPI 标识的示意图。在此之前假设网关 A 和网关 B 已经经过虚拟 SPI 能力协商，都支持所述能力。如图 8 所示，假设有三条 GTP 数据流，对应的流标识分别用 TEID_1、TEID_2、TEID_3 表示。网关 A 接收到 GTP 数据流后，首先，根据 IPSec 安全策略确定承载所述 GTP 数据流的 IPSec 隧道的 SPI 标识。第二，网关 A 对 TEID_1 使用 HASH 算法，取末四位哈希值，得出 0001，利用 0001 对 TEID_1 对应的 SPI 标识的末四位进行设置，得到虚拟 SPI 标识（用 SPI-1 表示），对属于 TEID_1 标识的报文进行加密处理后使用 SPI-1 封装；对 TEID_2 使用 HASH 算法，得出哈希值 0010，利用哈希值 0010 对 TEID_2 对应的 SPI 标识的末四位进行设置，得到虚拟 SPI 标识（用 SPI-2 表示），对属于 TEID_2 标识的报文进行加密处理后使用 SPI-2 封装；对 TEID_3 使用 HASH 算法，得出哈希值 1001，利用哈希值 1001 对 TEID_3 对应的 SPI 标识的末四位进行设置，得到虚拟 SPI 标识（用 SPI-3 表示），对属于 TEID_3 标识的报文进行加密处理后使用 SPI-3 封装。网关 A 将封装后的上述加密报文发送给网关 B。

图 9 为网关 B 接收到上述加密报文后进行解密处理的示意图，如图 9 所示，网关 B 通过 IPSec 隧道接收网关 A 发送的三条 GTP 数据流，将具有相同虚拟 SPI 标识的 GTP 报文分配到同一个解密单元进行解密处理。

可选地，将“0001”的报文 A 和报文 B 分配给解密单元 1 进行解密处理；将“0010”的报文 C 和报文 D 分配给解密单元 2 进行解密处理；将“1001”的报文 E 分配给解密单元 3 进行解密处理。每个解密单元对解密后的报文按照目的地址发送给目的地。

这里，每个加密报文均携带虚拟 SPI 标识，这样，网关 B 可以将携带相同虚拟 SPI 标识的加密报文由多个解密单元中同一个解密单元进行处理，能够避免属于同一 IPSec 隧道的多个解密处理单元同时处理报文，引发乱序加剧的问题，还提高了单 IPSec 隧道的处理性能。

应用实施例二

本应用实施例中，接收端将接收数据流的各报文送入与子 IPSec 隧道对应的解密单元进行解密处理。

另外，本应用实施例中，为一条子 IPSec 隧道在所述接收端分配一个解密单元。发送端用网关 A 表示，接收端用网关 B 表示。在 5G 网络中，以 DU 侧部署网关 A，CU 侧部署网关 B 为例。

所述网关 A 与所述网关 B 关于建立子 IPSec 隧道进行协商的过程参考上述描述，在此不再赘述。网关 A 和网关 B 之间部署两条子 IPSec 隧道（用 SA1 和 SA2 表示），对地址段为 10.41.128.0/20 的设备与地址段为 10.42.144.0/20 的设备之间的数据通信进行安全传输保护。其中，数据流的区分标识用五元组及 L7 层信息表示，数据流的区分标识与两条子 IPSec 隧道的映射关系为：五元组及 HTTP 应用类型对应 SA1，五元组及 RTP 应用类型对应 SA2。

这里，网关 A 与网关 B 进行 Child SA1 协商，建立子 IPSec 隧道 SA1，协商过程参考 IPSec 协商过程，协商过程中包括建立所述子 IPSec 隧道 SA1 的安全策略，将所述数据流的区分标识，即五元组及 HTTP 应用类型和 SA1 的 SPI 建立映射关系。网关 A 与网关 B 进行 Child SA2 协商，建立子 IPSec 隧道 SA2，协商过程中包括建立所述子 IPSec 隧道 SA2 的安全策略，将所述数据流的区分标识，即五元组及 RTP 应用类型和 SA2 的 SPI 建立映射关系。

图 10 为通过子 IPSec 隧道传输数据流的示意图，如图 10 所示，当网关 A 接收到数据流时，通过深度数据包检测（DPI，Deep Packet Inspection）检测识别所述数据流的报文的应用类型，如果识别的应用类型为 HTTP 应用类型，则根据安全策略选择 SA1，将所述数据流的加密后的各报文发送给网关 B；网关

B 通过与 SA1 对应的解密单元对所述数据流的加密后的各报文进行解密处理，并向目的 IP 地址转发。如果使用 DPI 检测识别所述数据流的报文的应用类型为 RTP 应用类型，则根据安全策略选择 SA2，将所述数据流的加密后的各报文发送给网关 B。网关 B 通过与 SA2 对应的解密单元对所述数据流的各报文进行解密处理，并向目的 IP 地址转发。

这里，通过子 IPSec 隧道，网关 B 可以将流标识相同的各报文送入与子 IPSec 隧道对应的解密单元进行解密处理。如此，可避免因为报文使用 IPSec 传输引发的报文乱序问题的发生。

另外，通过建立多条子 IPSec 隧道，同对多个数据流进行处理，从而提高了 IPSec 隧道的处理能力，进而能够满足 5G 数据传输速率的需求。

为了实现本申请实施例的方法，本申请实施例还提供了一种数据传输装置，设置在发送端上，如图 11 所示，包括：

第一确定单元 111，设置为利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识；

加密单元 112，设置为针对所述数据流中的每个加密后的报文，将虚拟 SPI 标识携带于相应报文中；

第一传输单元 113，设置为通过所述 IPSec 隧道，向接收端传输所述数据流；所述虚拟 SPI 标识用于供所述接收端将所述数据流的各报文送入同一个解密单元进行解密处理。

这里，为了保证数据传输的安全性，可以在所述发送端和接收端之间建立多条 IPSec 隧道，并用 SPI 标识进行唯一标识。其中，所述接收端为每条 IPSec 隧道分配多个解密单元。

实际应用时，如果所述发送端确定所述接收端具备支持虚拟 SPI 的能力，则所述发送端向所述接收端传输所述数据流之前，可以将所述数据流的流标识经过哈希得到的哈希值填入 SPI 的字段中，得到虚拟 SPI 标识。

所述第一确定单元 111，具体设置为：对所述数据流的流标识进行哈希运算处理，得到哈希值；利用得到的哈希值设置所述 SPI 标识的字段，得到虚拟 SPI 标识。

这里，可以利用得到的哈希值，设置所述 SPI 标识中特定位置的字段。比

如，假设所述 SPI 标识可以用 26 比特表示，则所述特定位置可以是指 26 比特中的末四位比特等等。

这里，在确定虚拟 SPI 标识之前，所述发送端还需要针对虚拟 SPI 支持能力与所述接收端进行协商，以确定所述接收端是否具有支持虚拟 SPI 的能力。

基于此，在一个可选的实施例中，所述装置还包括：判断单元，设置为判断所述接收端是否具有支持虚拟 SPI 的能力；当确定所述接收端具有支持虚拟 SPI 的能力时，利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识。

这里，在对所述接收端是否具有支持虚拟 SPI 的能力进行确认之前，所述发送端与所述接收端还需要进行 IKE SA、IPSec SA 的协商，以确定数据流传输所使用的 IPSec 隧道，即建立 IPSec 安全策略，IPSec 安全策略包含所述数据流的流标识与 IPSec 隧道的 SPI 标识的映射关系。

基于此，在一个可选的实施例中，所述装置还包括：第一协商单元，设置为与所述接收端进行 IPSec SA 协商；建立 IPSec 隧道。

其中，在建立 IPSec 隧道的过程中，建立 IPSec 安全策略，在所述 IPSec 安全策略中包含所述数据流的流标识和所述 IPSec 隧道的 SPI 标识的映射关系。

可选地，为所述数据流建立 ACL，ACL 中包含所述数据流的流标识，并建立所述数据流的流标识和 IPSec 隧道的 SPI 标识的映射关系。

这里，所述发送端与所述接收端进行 IPSec SA 协商的内容可以包括隧道两端使用的封装模式、加密算法、加密密钥、验证算法、验证密钥等等。

实际应用时，所述发送端将所述数据流发送至所述接收端之前，还需要对所述数据流的各报文进行加密。

基于此，在一个可选的实施例中，所述加密单元 112，具体设置为对所述数据流中的每个报文进行加密，得到加密后的各报文。

实际应用时，所述第一确定单元 111、加密单元 112、第一传输单元 113、判断单元、第一协商单元可由数据传输装置中的处理器实现。

为了实现本申请实施例的方法，本申请实施例还提供了一种数据传输装置，设置在接收端上，如图 12 所示，包括：

第一接收单元 121，设置为接收发送端通过 IPSec 隧道发送的数据流；所述

数据流的各报文中携带有相应的虚拟 SPI 标识；所述虚拟 SPI 标识是所述发送端基于所述数据流的流标识以及传输所述数据流的 IPSec 隧道的 SPI 标识确定的；

第一解密单元 122，设置为利用虚拟 SPI 标识，将所述数据的各报文送入多个解密单元中的同一个解密单元进行解密处理。

这里，所述发送端和接收端之间可建立多条 IPSec 隧道，并用 SPI 标识进行唯一标识。其中，所述接收端为每条 IPSec 隧道分配多个解密单元。

实际应用时，为了提高 IPSec 隧道的处理性能，所述接收端可以包括多个解密单元。所述接收端可以根据虚拟 SPI 标识将具有相同虚拟 SPI 标识的报文送入同一个解密单元进行解密处理，以避免因为多解密单元处理加剧报文乱序。其中，具有相同虚拟 SPI 标识的报文，表示属于同一条数据流，由同一个解密单元处理。

基于此，在一个可选的实施例中，所述第一解密单元 122，具体设置为：将具有相同虚拟 SPI 标识的报文送入同一个解密单元，以进行解密处理。

可选地，所述第一解密单元 122，可以将所述数据流的各报文的虚拟 SPI 标识进行比较，具备相同虚拟 SPI 标识的各报文送入同一个解密单元，以进行解密处理。

实际应用时，所述第一接收单元 121、第一解密单元 122 可由数据传输装置中的处理器实现。

为了实现本申请实施例的方法，本申请实施例还提供了一种数据传输装置，设置在发送端上，如图 13 所示，包括：

第二确定单元 131，设置为确定数据流的区分标识；还设置为利用数据流的区分标识与子 IPSec 隧道的 SPI 标识的映射关系，确定与所述数据流使用的子 IPSec 隧道；

第二传输单元 132，设置为利用确定的子 IPSec 隧道，向接收端传输所述数据流。

其中，所述数据流的区分标识可以由五元组及以下信息至少之一组成：L2 层的信息、L3 层的信息、L4 层的信息、L5 层的信息、L6 层的信息、L7 层的信息。所述区分标识能够唯一区分所述数据流。

这里，所述五元组可以包括：源 IP 地址、目的 IP 地址，源端口号、目的端口号以及协议号。L2 至 L7 层为 OSI 参考模型定义的各层。L2 层信息可以包括与链路相关的信息；L3 层信息可以包括 IP 地址；L4 层信息可以包括协议信息，比如 TCP 协议、UDP 协议；L5 层信息可以包括与会话层相关的信息，比如服务质量参数；L6 层信息可以包括数据格式，比如 ASCII 格式等等；L7 层信息可以包括所述数据流的应用类型。所述应用类型包括但不限于 HTTP 应用类型、RTP 应用类型等等。

实际应用时，为了满足 5G 数据传输速率的需求，可以在所述发送端和接收端之间建立多条子 IPSec 隧道，并用 SPI 标识进行唯一标识。一条子 IPSec 隧道在所述接收端分配一个解密单元。

这里，所述发送端对所述数据流进行传输前，所述发送端与所述接收端还需要进行 IKE SA、Child SA 的协商，以确定数据流传输所使用的子 IPSec 隧道，即建立子 IPSec 安全策略，包含所述数据流的区分标识与子 IPSec 隧道的 SPI 标识的映射关系。

基于此，在一个可选的实施例中，所述装置还包括：第二协商单元，设置为与所述接收端进行 Child SA 协商；建立子 IPSec 隧道；

其中，在建立子 IPSec 隧道的过程中，建立子 IPSec 隧道安全策略，在所述子 IPSec 隧道安全策略中包含所述数据流的区分标识和子 IPSec 隧道的 SPI 标识的映射关系。

这里，所述发送端与所述接收端进行 Child SA 协商的内容可以包括隧道两端使用的封装模式、加密算法、加密密钥、验证算法、验证密钥等等。

这里，通过所述确定的子 IPSec 隧道将所述数据流传输至所述接收端的与所述子 IPSec 隧道对应的解密单元进行解密处理。

实际应用时，所述第二确定单元 131、第二传输单元 132、第二协商单元可由数据传输装置中的处理器实现。

为了实现本申请实施例的方法，本申请实施例还提供了一种数据传输装置，设置在接收端上，如图 14 所示，包括：

第二接收单元 141，设置为接收发送端通过子 IPSec 隧道发送的数据流。

其中，所述子 IPSec 隧道是所述发送端基于所述数据流的区分标识与子

IPSec 隧道的 SPI 标识的映射关系确定的。

第二解密单元 142，设置为将通过子 IPSec 隧道传输的所述数据流发送至与所述子 IPSec 隧道对应的解密单元进行解密处理。

这里，为了满足 5G 数据传输速率的需求，可以在所述发送端和接收端之间建立多条子 IPSec 隧道，并用 SPI 进行唯一标识。一条子 IPSec 隧道在所述接收端分配一个解密单元。

实际应用时，所述第二接收单元 141 可由数据传输装置中的通信接口实现。第二解密单元 142 可由数据传输装置中的处理器实现。

基于上述程序模块的硬件实现，且为了实现本申请实施例发送端侧的方法，本申请实施例还提供了一种发送设备，如图 15 所示，该智能设备 150 包括：第一通信接口 151、第一处理器 152、第一存储器 153；其中，

第一通信接口 151，能够与其它设备进行信息交互；

第一处理器 152，与所述第一通信接口 151 连接，以实现与无线网络接入设备进行信息交互，设置为运行计算机程序时，执行上述智能设备侧一个或多个技术方案提供的方法。而所述计算机程序存储在第一存储器 153 上。

当然，实际应用时，智能设备 150 中的各个组件通过总线系统 154 耦合在一起。可理解，总线系统 154 设置为实现这些组件之间的连接通信。总线系统 154 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 15 中将各种总线都标为总线系统 154。

本申请实施例中的第一存储器 153 设置为存储各种类型的数据以支持智能设备 150 的操作。这些数据的示例包括：用于在智能设备 150 上操作的任何计算机程序。

上述本申请实施例揭示的方法可以应用于所述第一处理器 152 中，或者由所述第一处理器 152 实现。所述第一处理器 152 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，上述方法的各步骤可以通过所述第一处理器 152 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的所述第一处理器 152 可以是通用处理器、数字信号处理器（DSP，Digital Signal Processor），或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。所述第一处理器 152 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。软件模块可以位于存储介质中，该存储介质位于第一存储器 153，所述第一处理器 152 读取第一存储器 153 中的信息，结合其硬件完成前述方法的步骤。

在示例性实施例中，发送设备 150 可以被一个或多个应用专用集成电路（ASIC，Application Specific Integrated Circuit）、DSP、可编程逻辑器件（PLD，Programmable Logic Device）、复杂可编程逻辑器件（CPLD，Complex Programmable Logic Device）、现场可编程门阵列（FPGA，Field-Programmable Gate Array）、通用处理器、控制器、微控制器（MCU，Micro Controller Unit）、微处理器（Microprocessor）、或者其他电子元件实现，用于执行前述方法。

基于上述程序模块的硬件实现，且为了实现本申请实施例接收端侧的方法，如图 16 所示，该接收设备 160 包括：

第二通信接口 161，能够与其它设备进行信息交互；

第二处理器 162，与所述第二通信接口 161 连接，以实现与智能设备进行信息交互，设置为运行计算机程序时，执行上述无线网络接入设备侧一个或多个技术方案提供的方法。而所述计算机程序存储在所述第二存储器 163 上。

当然，实际应用时，无线网络接入设备 160 中的各个组件通过总线系统 164 耦合在一起。可理解，总线系统 164 设置为实现这些组件之间的连接通信。总线系统 164 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 16 中将各种总线都标为总线系统 164。

本申请实施例中的第二存储器 163 设置为存储各种类型的数据以支持无线网络接入设备 160 的操作。这些数据的示例包括：用于在无线网络接入设备 160 上操作的任何计算机程序。

上述本申请实施例揭示的方法可以应用于所述第二处理器 162 中，或者由所述第二处理器 162 实现。所述第二处理器 162 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，上述方法的各步骤可以通过所述第二处理器 162 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的所述第二处理器 162 可以是通用处理器、DSP，或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。所述第二处理器 162 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。软件模块可以位于存储介质中，该存储介质位于第二存储器 163，所述第二处理器 162 读取第二存储器 163 中的信息，结合其硬件完成前述方法的步骤。

在示例性实施例中，接收设备 160 可以被一个或多个 ASIC、DSP、PLD、CPLD、FPGA、通用处理器、控制器、MCU、Microprocessor、或其他电子元件实现，用于执行前述方法。

可以理解，本申请实施例的存储器（第一存储器 153、第二存储器 163）可以是易失性存储器或者非易失性存储器，也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（ROM，Read Only Memory）、可编程只读存储器（PROM，Programmable Read-Only Memory）、可擦除可编程只读存储器（EPROM，Erasable Programmable Read-Only Memory）、电可擦除可编程只读存储器（EEPROM，Electrically Erasable Programmable Read-Only Memory）、磁性随机存取存储器（FRAM，ferromagnetic random access memory）、快闪存储器（Flash Memory）、磁表面存储器、光盘、或只读光盘（CD-ROM，Compact Disc Read-Only Memory）；磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器（RAM，Random Access Memory），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（SRAM，Static Random Access Memory）、同步静态随机存取存储器（SSRAM，Synchronous Static Random Access Memory）、动态随机存取存储器（DRAM，Dynamic Random Access Memory）、同步动态随机存取存储器（SDRAM，Synchronous Dynamic Random Access Memory）、双倍数据速率同步动态随机存取存储器（DDRSDRAM，Double Data Rate Synchronous Dynamic Random Access Memory）、增强型同步动态随机存取存储器（ESDRAM，Enhanced Synchronous Dynamic Random Access Memory）、同步连接动态随机存取存储器（SLDRAM，SyncLink Dynamic Random Access Memory）、直接内存总线随机存取存储器（DRRAM，Direct Rambus Random Access Memory）。本申请实施例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。

需要说明的是：“第一”、“第二”等是用于区别类似的对象，而不必用于描

述特定的顺序或先后次序。

另外，本申请实施例所记载的技术方案之间，在不冲突的情况下，可以任意组合。

以上所述，仅为本申请的较佳实施例而已，并非用于限定本申请的保护范围。

工业实用性

如上所述，本申请实施例提供的一种数据传输方法、装置、相关设备及存储介质具有以下有益效果：发送端将携带有虚拟 SPI 标识的各报文发送给接收端，这样，所述接收端可以将具有相同虚拟 SPI 标识的报文送入同一个解密单元进行解密处理。如此，可避免报文乱序问题的发生，同时还能提高 IPSec 隧道的处理性能。

权 利 要 求 书

1、一种数据传输方法，应用于发送端，所述方法包括:

利用数据流的流标识，以及传输所述数据流的网络协议安全 IPSec 隧道的安全参数索引 SPI 标识，确定虚拟 SPI 标识;

针对所述数据流中的每个加密后的报文，将虚拟 SPI 标识携带于相应报文中;

通过所述 IPSec 隧道，向接收端传输所述数据流; 所述虚拟 SPI 标识用于供所述接收端将所述数据流的各报文送入同一个解密单元进行解密处理。

2、根据权利要求 1 所述的方法，其中，所述利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识，包括:

对所述数据流的流标识进行哈希运算处理，得到哈希值;

利用得到的哈希值设置所述 SPI 标识的字段，得到虚拟 SPI 标识。

3、根据权利要求 1 所述的方法，其中，所述利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识之前，所述方法还包括:

判断所述接收端是否具有支持虚拟 SPI 的能力;

当确定所述接收端具有支持虚拟 SPI 的能力时，利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识。

4、根据权利要求 1 所述的方法，其中，所述利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识之前，所述方法还包括:

与所述接收端进行 IPsec 安全联盟 SA 协商，建立 IPSec 隧道; 其中，

在建立 IPSec 隧道的过程中，建立 IPSec 安全策略，在所述 IPSec 安全策略中包含所述数据流的流标识和所述 IPSec 隧道的 SPI 标识的映射关系。

5、一种数据传输方法，应用于接收端，所述方法包括:

接收发送端通过 IPSec 隧道发送的数据流; 所述数据流的各报文中携带有虚拟 SPI 标识; 所述虚拟 SPI 标识是所述发送端基于所述数据流的流标识以及传输所述数据流的 IPSec 隧道的 SPI 标识确定的;

利用虚拟 SPI 标识，将所述数据流的各报文送入同一个解密单元进行解密处理。

6、根据权利要求 5 所述的方法，其中，所述利用虚拟 SPI 标识，将所述数据流的各报文送入同一个解密单元进行解密处理，包括:

将具有相同虚拟 SPI 标识的报文送入同一个解密单元，以进行解密处理。

7、一种数据传输方法，应用于发送端，所述方法包括:

确定数据流的区分标识;

利用数据流的区分标识与子 IPSec 隧道的 SPI 标识的映射关系，确定所述数据流传输所使用的子 IPSec 隧道;

利用确定的子 IPSec 隧道，向接收端传输所述数据流；通过所述确定的子 IPSec 隧道将所述数据流传输至所述接收端的与所述子 IPSec 隧道对应的解密单元进行解密处理。

8、根据权利要求 7 所述的方法，其中，所述数据流的区分标识由五元组及以下信息至少之一组成:

L2 层的信息；L3 层的信息；L4 层的信息；L5 层的信息；L6 层的信息；L7 层的信息。

9、根据权利要求 7 所述的方法，其中，所述方法还包括:

与所述接收端进行子 Child SA 协商，建立子 IPSec 隧道；其中，

在建立子 IPSec 隧道的过程中，建立子 IPSec 隧道安全策略，在所述子 IPSec 隧道安全策略中包含所述数据流的区分标识和子 IPSec 隧道的 SPI 标识的映射关系。

10、一种数据传输方法，应用于接收端，所述方法包括:

接收发送端通过子 IPSec 隧道发送的数据流;

将通过子 IPSec 隧道传输的所述数据流发送至所述子 IPSec 隧道对应的解密单元进行解密处理。

11、根据权利要求 10 所述的方法，其中，所述方法还包括:

与所述发送端进行 Child SA 协商，建立子 IPSec 隧道。

12、一种数据传输装置，应用于发送端，所述装置包括:

第一确定单元，设置为利用数据流的流标识，以及传输所述数据流的 IPSec 隧道的 SPI 标识，确定虚拟 SPI 标识；

加密单元，设置为针对所述数据流中的每个加密后的报文，将虚拟 SPI 标识携带于相应报文中；

第一传输单元，设置为通过所述 IPSec 隧道，向接收端传输所述数据流；所述虚拟 SPI 标识用于供所述接收端将所述数据流的各报文送入同一个解密单元进行解密处理。

13、一种数据传输装置，应用于接收端，所述装置包括：

第一接收单元，设置为接收发送端通过 IPSec 隧道发送的数据流；所述数据流的各报文中携带有虚拟 SPI 标识；所述虚拟 SPI 标识是所述发送端基于所述数据流的流标识以及传输所述数据流的 IPSec 隧道的 SPI 标识确定的；

第一解密单元，设置为利用虚拟 SPI 标识，将所述数据流的各报文送入同一个解密单元进行解密处理。

14、一种数据传输装置，应用于发送端，所述装置包括：

第一确定单元，设置为确定数据流的区分标识；还设置为利用数据流的区分标识与子 IPSec 隧道的 SPI 标识的映射关系，确定所述数据流传输所使用的子 IPSec 隧道；

第二传输单元，设置为利用确定的子 IPSec 隧道，向接收端传输所述数据流；通过所述确定的子 IPSec 隧道将所述数据流传输至所述接收端的与所述子 IPSec 隧道对应的解密单元进行解密处理。

15、一种数据传输装置，应用于接收端，所述装置包括：

第二接收单元，设置为接收发送端通过子 IPSec 隧道发送的数据流；

第二解密单元，设置为将通过子 IPSec 隧道传输的所述数据流发送至与所述子 IPSec 隧道对应的解密单元进行解密处理。

16、一种发送设备，包括：第一处理器和设置为存储能够在处理器上运行的计算机程序的第一存储器，

其中，所述第一处理器设置为运行所述计算机程序时，执行权利要求 1 至 4 任一项所述方法的步骤，或者，执行权利要求 7 至 9 任一项所述方法的步骤。

17、一种接收设备，包括：第二处理器和设置为存储能够在处理器上运行

的计算机程序的第二存储器，

其中，所述第一处理器设置为运行所述计算机程序时，执行权利要求 5 或 6 所述方法的步骤，或者，执行权利要求 10 或 11 所述方法的步骤。

18、一种存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现权利要求 1 至 4 任一项所述方法的步骤，或者，执行权利要求 5 至 6 任一项所述方法的步骤，或者，执行权利要求 7 至 9 任一项所述方法的步骤，或者，执行权利要求 10 或 11 所述方法的步骤。

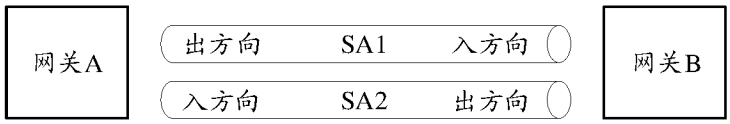
网关A
出方向 SA1 入方向
入方向 SA2 出方向
网关B

图 1

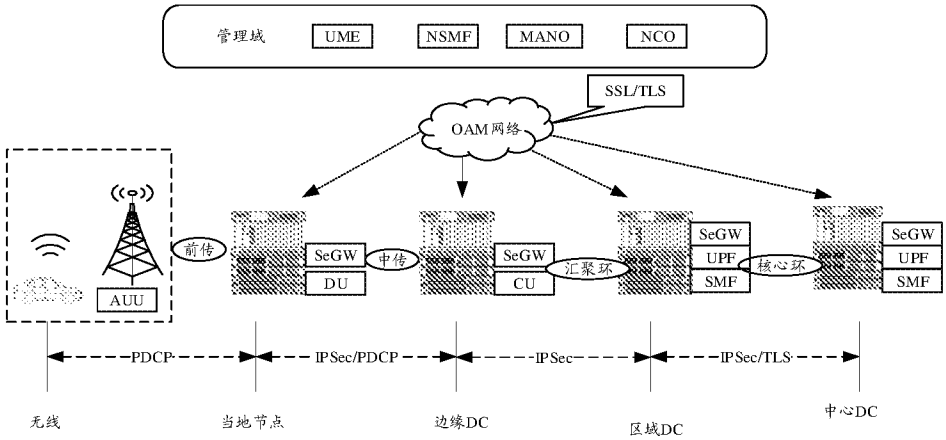
管理域
UME
NSMF
MANO
NCO
SSL/TLS
OAM网络
前传
AUU
SeGW
DU
中传
SeGW
CU
汇聚环
SeGW
UPF
SMF
核心环
SeGW
UPF
SMF
PDCP
IPSec/PDCP
IPSec
IPSec/TLS
无线
当地节点
边缘DC
区域DC
中心DC

图 2

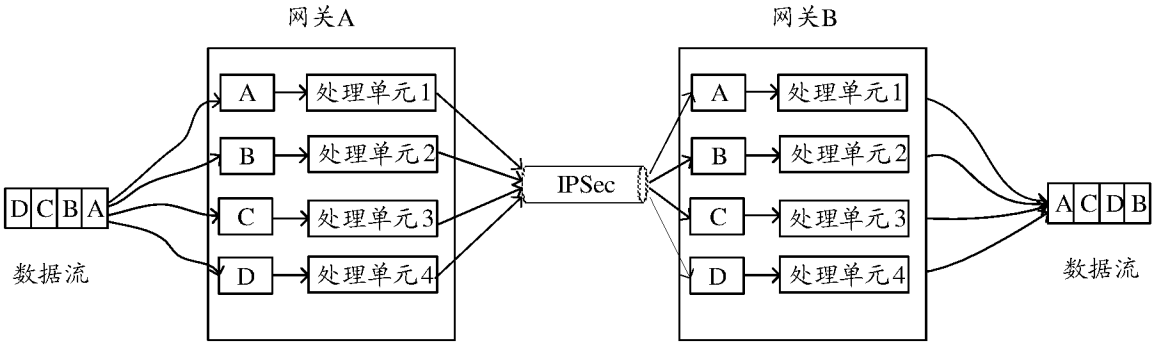
网关A
网关B
D C B A
数据流
A
B
C
D
处理单元1
处理单元2
处理单元3
处理单元4
IPSec
A
B
C
D
处理单元1
处理单元2
处理单元3
处理单元4
A C D B
数据流

图 3

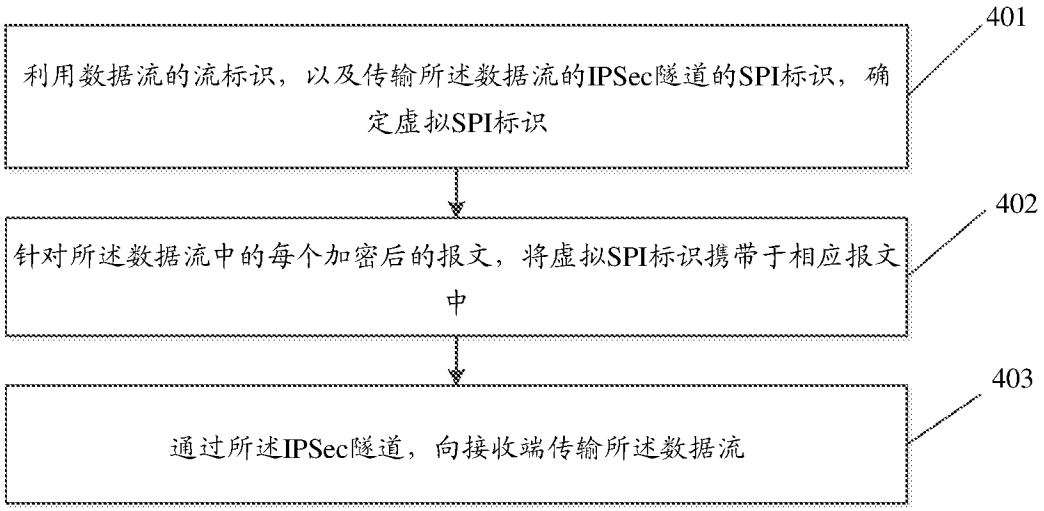
401
利用数据流的流标识，以及传输所述数据流的IPSec隧道的SPI标识，确定虚拟SPI标识
402
针对所述数据流中的每个加密后的报文，将虚拟SPI标识携带于相应报文中
403
通过所述IPSec隧道，向接收端传输所述数据流

图 4

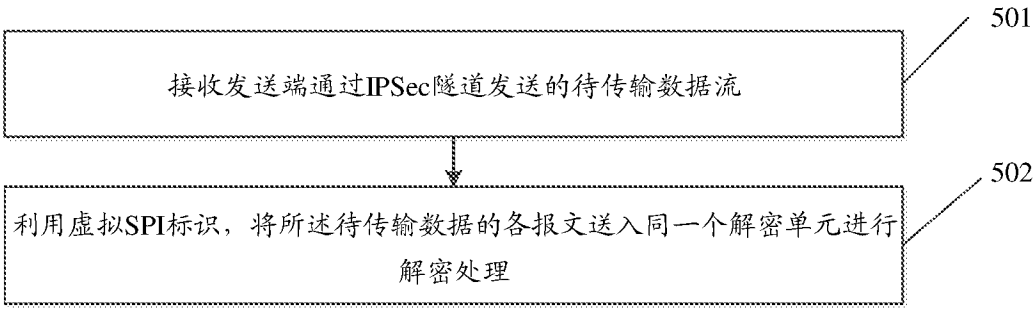
501
接收发送端通过IPSec隧道发送的待传输数据流
502
利用虚拟SPI标识，将所述待传输数据的各报文送入同一个解密单元进行解密处理

图 5

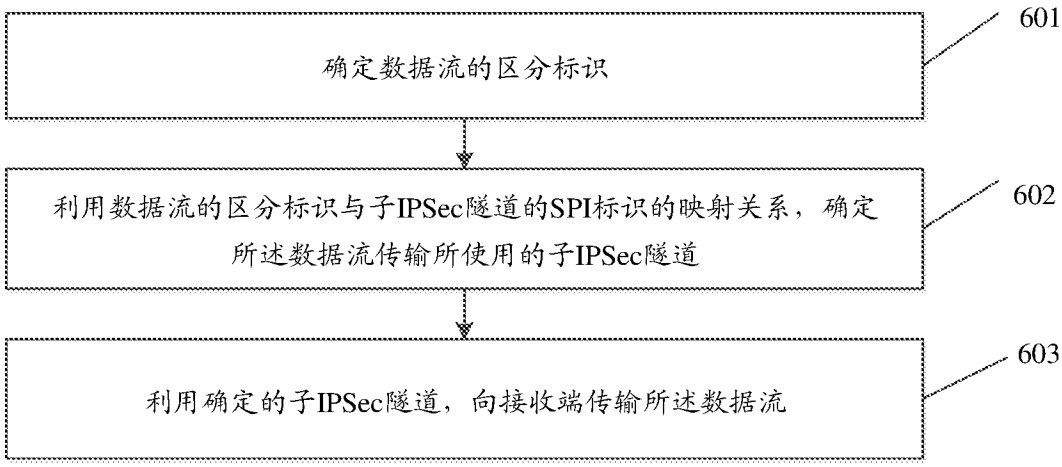
601
确定数据流的区分标识
602
利用数据流的区分标识与子IPSec隧道的SPI标识的映射关系，确定所述数据流传输所使用的子IPSec隧道
603
利用确定的子IPSec隧道，向接收端传输所述数据流

图 6

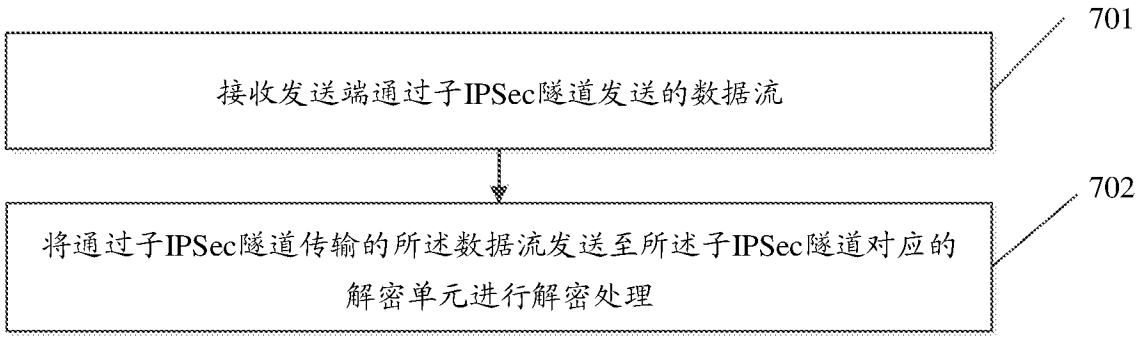
701
接收发送端通过子IPSec隧道发送的数据流
702
将通过子IPSec隧道传输的所述数据流发送至所述子IPSec隧道对应的解密单元进行解密处理

图 7

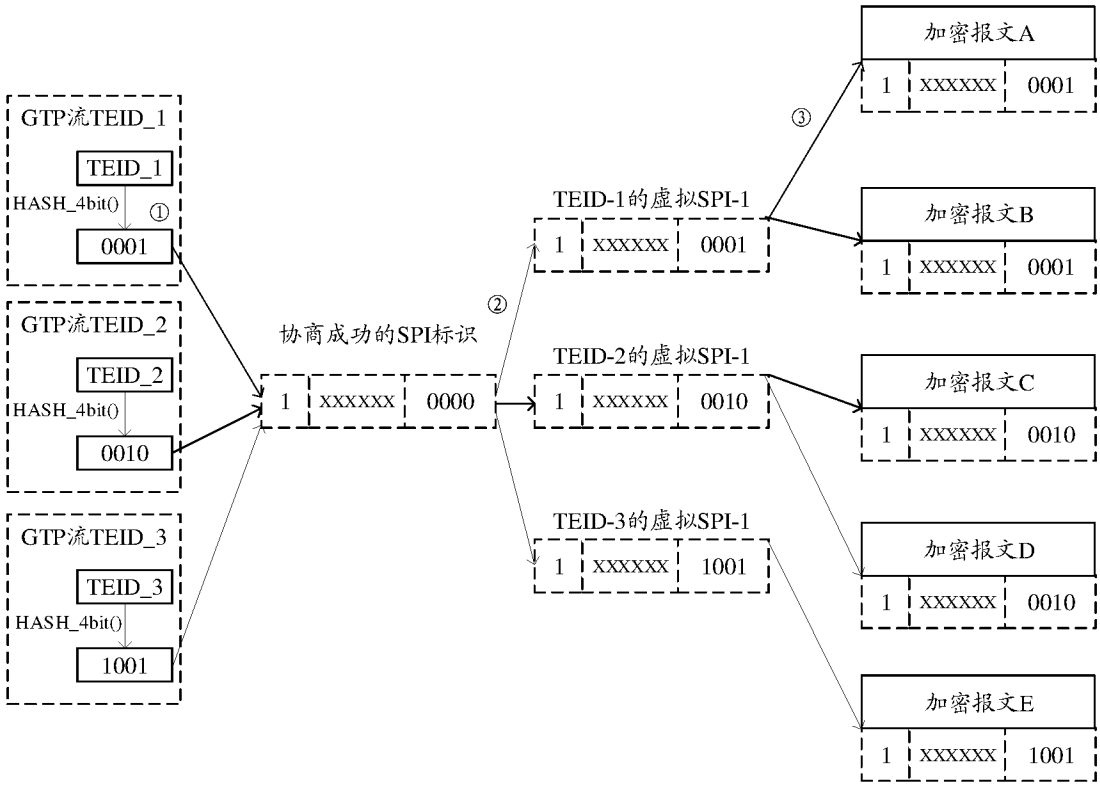
GTP流TEID_1
TEID_1
HASH_4bit()
①
0001
GTP流TEID_2
TEID_2
HASH_4bit()
0010
GTP流TEID_3
TEID_3
HASH_4bit()
1001
协商成功的SPI标识
1 XXXXXX 0000
②
TEID-1的虚拟SPI-1
1 XXXXXX 0001
TEID-2的虚拟SPI-1
1 XXXXXX 0010
TEID-3的虚拟SPI-1
1 XXXXXX 1001
③
加密报文A
1 XXXXXX 0001
加密报文B
1 XXXXXX 0001
加密报文C
1 XXXXXX 0010
加密报文D
1 XXXXXX 0010
加密报文E
1 XXXXXX 1001

图 8

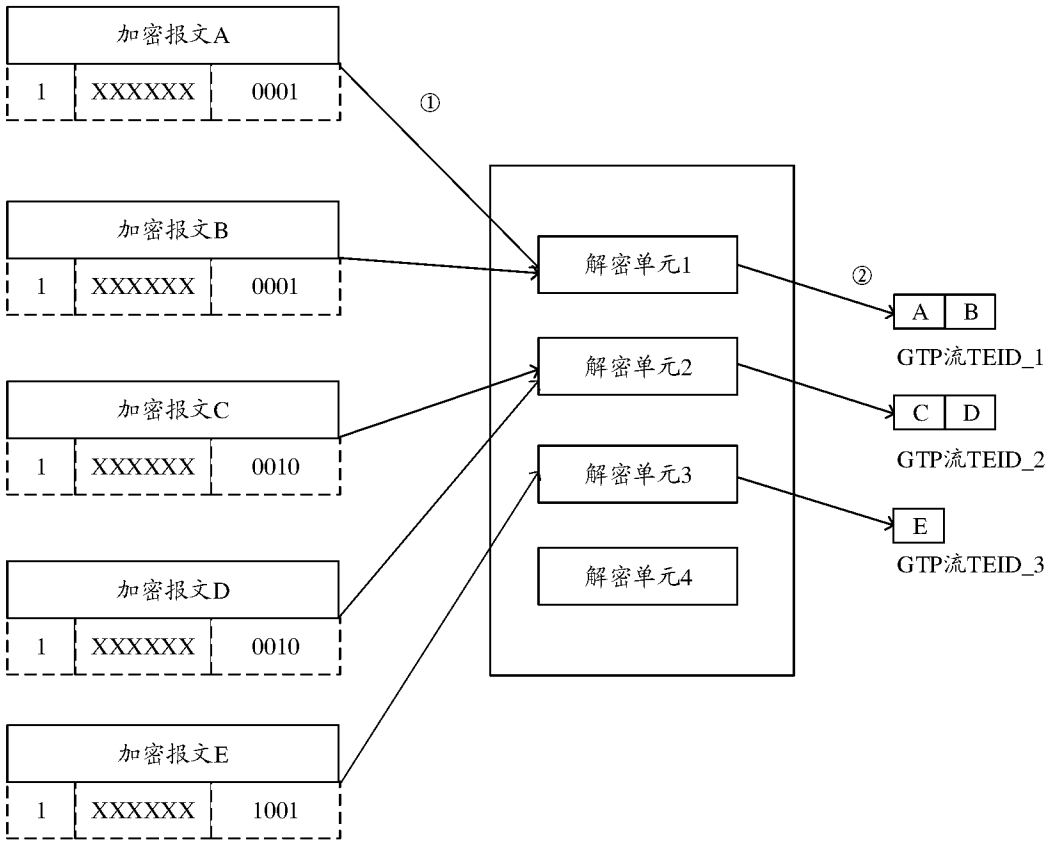
加密报文A
1
XXXXXX
0001
加密报文B
1
XXXXXX
0001
加密报文C
1
XXXXXX
0010
加密报文D
1
XXXXXX
0010
加密报文E
1
XXXXXX
1001
①
解密单元1
解密单元2
解密单元3
解密单元4
②
A
B
GTP流TEID_1
C
D
GTP流TEID_2
E
GTP流TEID_3

图 9

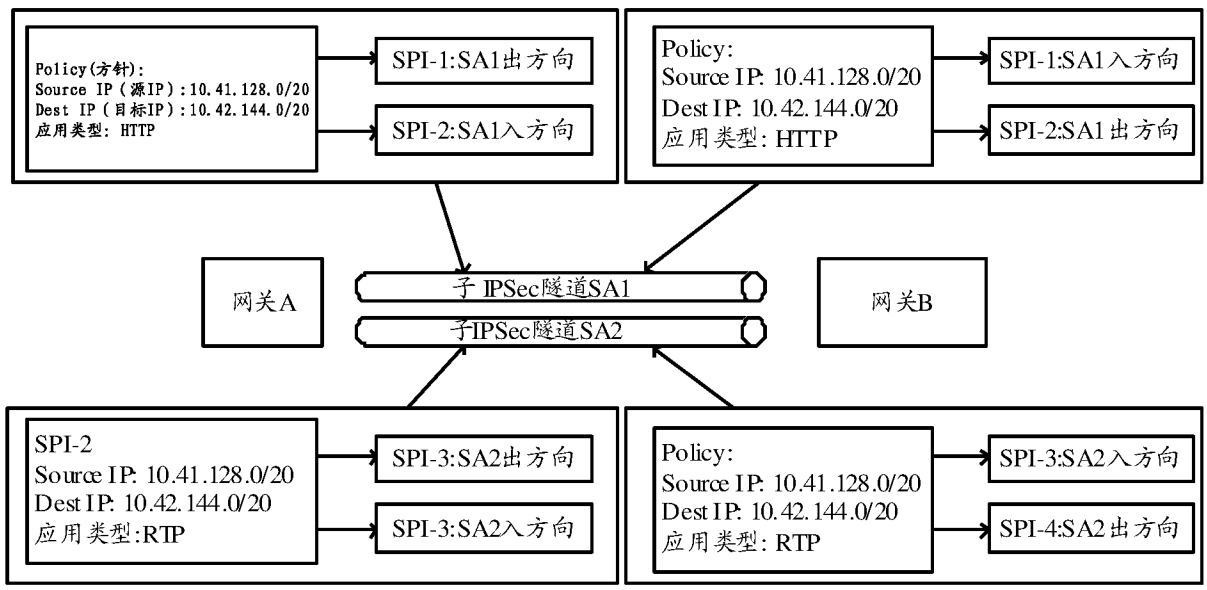
Policy(方针):
Source IP(源IP):10.41.128.0/20
Dest IP(目标IP):10.42.144.0/20
应用类型: HTTP
SPI-1:SA1出方向
SPI-2:SA1入方向
Policy:
Source IP: 10.41.128.0/20
Dest IP: 10.42.144.0/20
应用类型: HTTP
SPI-1:SA1入方向
SPI-2:SA1出方向
网关A
子IPSec隧道SA1
子IPSec隧道SA2
网关B
SPI-2
Source IP: 10.41.128.0/20
Dest IP: 10.42.144.0/20
应用类型:RTP
SPI-3:SA2出方向
SPI-3:SA2入方向
Policy:
Source IP: 10.41.128.0/20
Dest IP: 10.42.144.0/20
应用类型: RTP
SPI-3:SA2入方向
SPI-4:SA2出方向

图 10

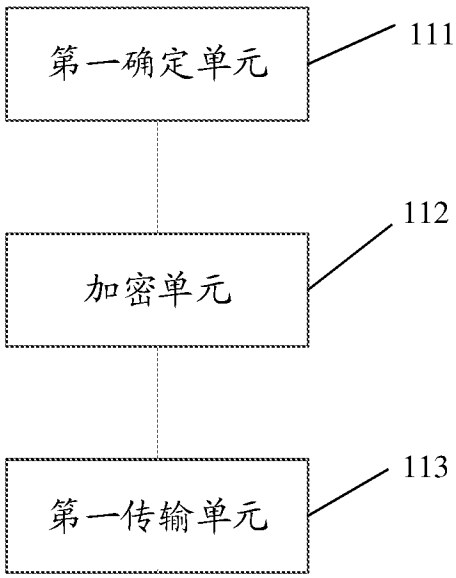
第一确定单元
111
加密单元
112
第一传输单元
113

图 11

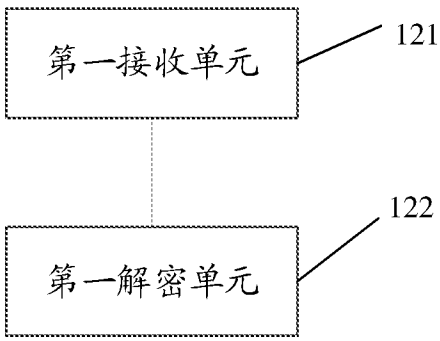
第一接收单元
121
第一解密单元
122

图 12

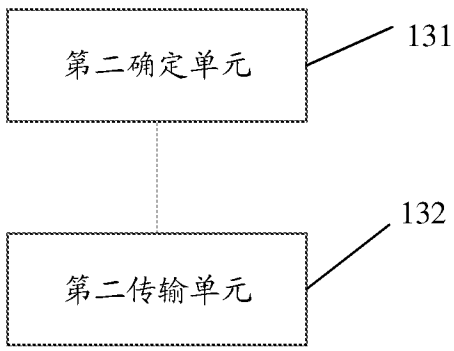
第二确定单元
131
第二传输单元
132

图 13

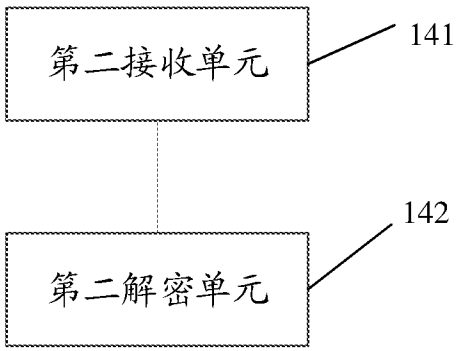
第二接收单元
141
142
第二解密单元

图 14

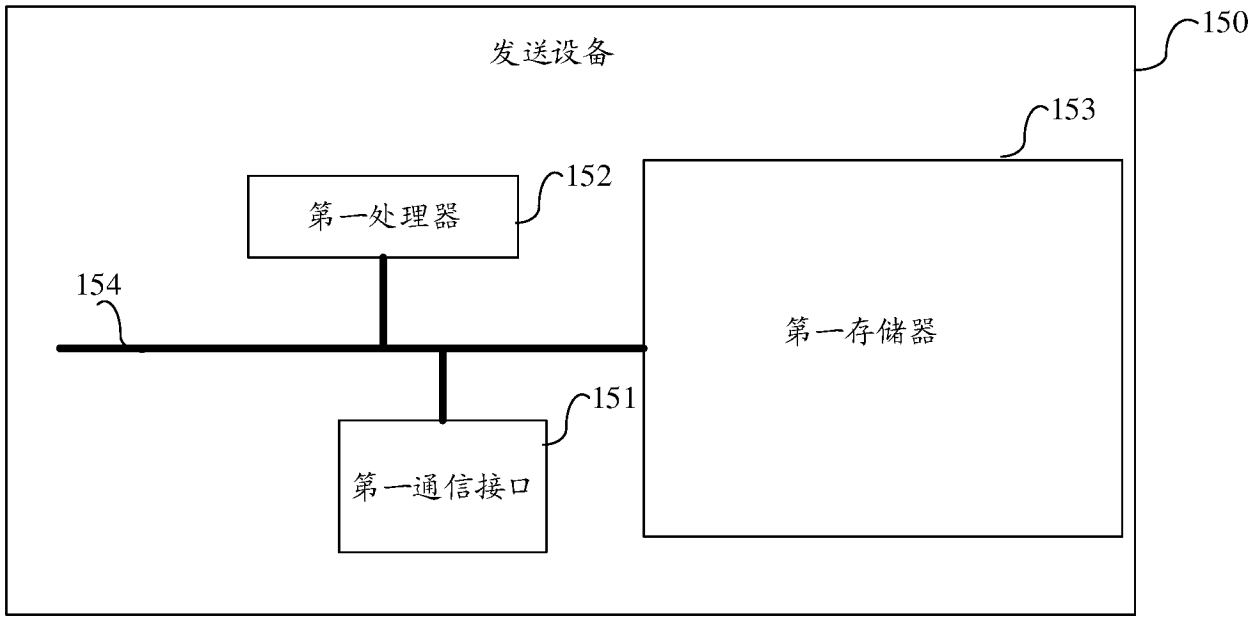
发送设备
150
153
152
第一处理器
154
第一存储器
151
第一通信接口

图 15

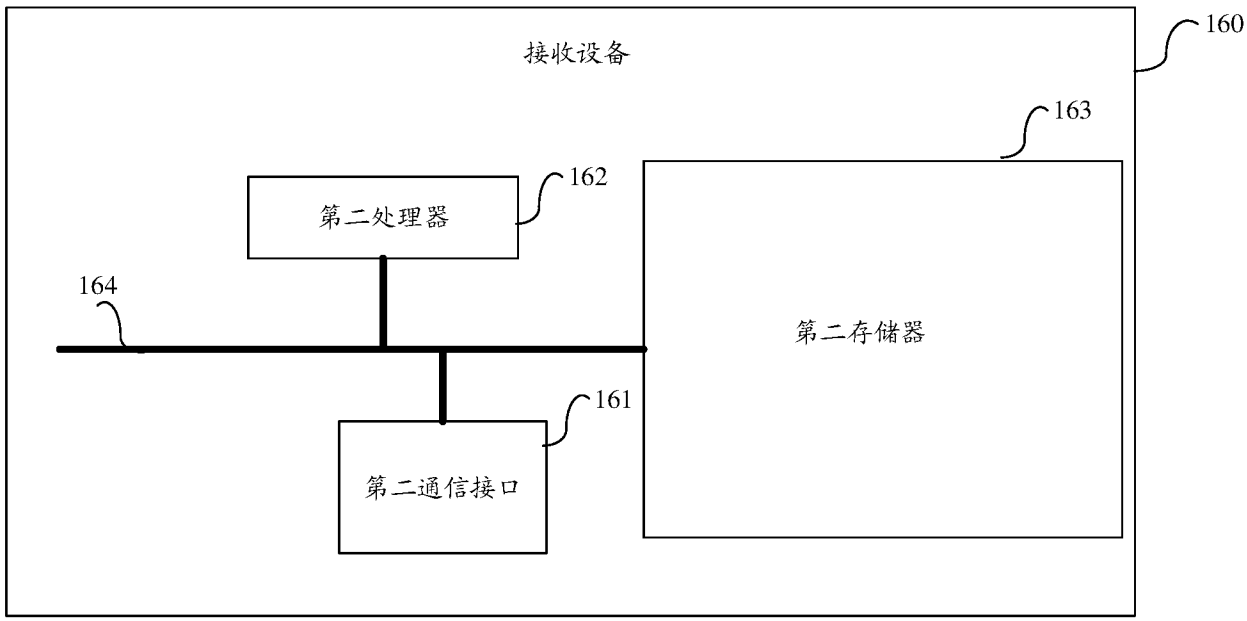

图 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/112548

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, 3GPP: 隧道, 安全, 参数, 索引, 标识, 加密, 解密, 子隧道, 映射, 对应, 相同, 同一, IPSec, SA, safe, security, parameter, index, id, identifier, cipher, encrypt, decrypt, sub-tunnel, tunnel, map, correspond, same

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 108989194 A (MICROSOFT TECHNOLOGY LICENSING LLC.) 11 December 2018 (2018-12-11) description, paragraphs [0025]-[0049]	1-6, 12-13, 16-18
Y	CN 108989194 A (MICROSOFT TECHNOLOGY LICENSING LLC.) 11 December 2018 (2018-12-11) description, paragraphs [0025]-[0049]	7-11, 14-15
Y	CN 104247367 A (HUAWEI TECHNOLOGIES CO., LTD.) 24 December 2014 (2014-12-24) claims 1-18, and description, paragraphs [0020]-[0044]	7-11, 14-15
A	CN 102907056 A (HUAWEI TECHNOLOGIES CO., LTD.) 30 January 2013 (2013-01-30) entire document	1-18
A	CN 106998549 A (ZTE CORPORATION) 01 August 2017 (2017-08-01) entire document	1-18
A	US 2010217971 A1 (CISCO TECHNOLOGY, INC.) 26 August 2010 (2010-08-26) entire document	1-18

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 January 2019	**23 January 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/112548

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MOTOROLA MOBILITY-LENOVO; NOKIA; NOKIA SHANGHAI BELL. "Changing Transport Mode to Tunnel Mode for IPsec Tunnel" *3GPP TSG-CT WG1 Meeting #111bis C1-184265,* 13 July 2018 (2018-07-13), pp. 1-10	1-18

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/112548

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	108989194	A	11 December 2018	WO	2018222323	A1	06 December 2018
CN	104247367	A	24 December 2014	JP	2015515210	A	21 May 2015
				EP	2823620	A1	14 January 2015
				US	2013263249	A1	03 October 2013
				WO	2013149041	A1	03 October 2013
				JP	2017028740	A	02 February 2017
CN	102907056	A	30 January 2013	WO	2012097523	A1	26 July 2012
CN	106998549	A	01 August 2017		None		
US	2010217971	A1	26 August 2010	EP	2401853	A1	04 January 2012
				CN	102549998	A	04 July 2012
				WO	2010126634	A1	04 November 2010

国际检索报告

国际申请号
PCT/CN2019/112548

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, CNKI, WPI, EPODOC,3GPP：隧道，安全，参数，索引，标识，加密，解密，子隧道，映射，对应，相同，同一，IPSec,SA, safe, security, parameter, index, id, identifier, cipher, encrypt, decrypt, sub-tunnel, tunnel, map, correspond, same

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 108989194 A (微软技术许可有限责任公司) 2018年 12月 11日 (2018-12-11) 说明书第[0025]-[0049]段	1-6，12-13，16-18
Y	CN 108989194 A (微软技术许可有限责任公司) 2018年 12月 11日 (2018-12-11) 说明书第[0025]-[0049]段	7-11，14-15
Y	CN 104247367 A (华为技术有限公司) 2014年 12月 24日 (2014-12-24) 权利要求1-18、说明书第[0020]-[0044]段	7-11，14-15
A	CN 102907056 A (华为技术有限公司) 2013年 1月 30日 (2013-01-30) 全文	1-18
A	CN 106998549 A (中兴通讯股份有限公司) 2017年 8月 1日 (2017-08-01) 全文	1-18
A	US 2010217971 A1 (CISCO TECHNOLOGY, INC.) 2010年 8月 26日 (2010-08-26) 全文	1-18
A	MOTOROLA MOBILITY - LENOVO, NOKIA, NOKIA SHANGHAI BELL. "Changing Transport Mode to Tunnel Mode for IPsec Tunnel" 3GPP TSG-CT WG1 Meeting #111bis C1-184265, 2018年 7月 13日 (2018-07-13), 第1-10页	1-18

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 1月 10日	2020年 1月 23日

ISA/CN的名称和邮寄地址	受权官员
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	李燕
传真号 (86-10)62019451	电话号码 53961771

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/112548

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	108989194	A	2018年 12月 11日	WO	2018222323	A1	2018年 12月 6日
CN	104247367	A	2014年 12月 24日	JP	2015515210	A	2015年 5月 21日
				EP	2823620	A1	2015年 1月 14日
				US	2013263249	A1	2013年 10月 3日
				WO	2013149041	A1	2013年 10月 3日
				JP	2017028740	A	2017年 2月 2日
CN	102907056	A	2013年 1月 30日	WO	2012097523	A1	2012年 7月 26日
CN	106998549	A	2017年 8月 1日		无		
US	2010217971	A1	2010年 8月 26日	EP	2401853	A1	2012年 1月 4日
				CN	102549998	A	2012年 7月 4日
				WO	2010126634	A1	2010年 11月 4日