(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2018 年 1 月 11 日 (11.01.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/006627 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 9/08* (2006.01)
H04L 9/30 (2006.01)

(21) 国际申请号: PCT/CN2017/077952

(22) 国际申请日: 2017 年 3 月 23 日 (23.03.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610526350.0 2016年7月6日 (06.07.2016) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 王海光 (WANG, Haiguang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 刘斐 (LIU, Fei); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 康鑫 (KANG, Xin); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 广州三环专利代理有限公司 (GUANGZHOU SCIHEAD PATENT AGENT CO., LTD.); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (CN)。

(54) **Title:** PROTECTION SYSTEM, METHOD AND DEVICE FOR TRANSMISSION DATA

(54) **发明名称**: 一种传输数据的保护系统、方法及装置

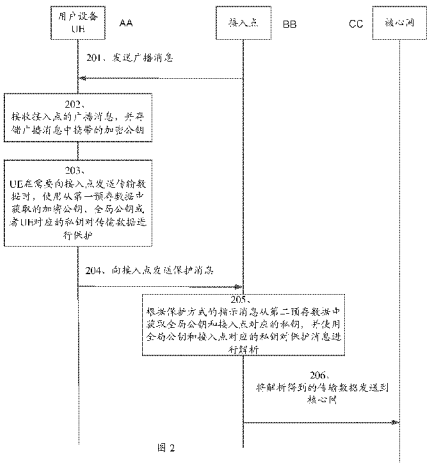


图 2

201 Sending a broadcast message
202 Receiving the broadcast message from an access point, and storing an encrypted public key carried in the broadcast message
203 A UE using, when transmission data needs to be sent to the access point, the encrypted public key and a global public key acquired from first pre-stored data or a private key corresponding to the UE to protect the transmission data
204 Sending a protection message to the access point
205 Acquiring, from second pre-stored data, the global public key and a private key corresponding to the access point according to an indication message of a protection method, and using the global public key and the private key corresponding to the access point to parse the protection message
206 Sending parsed transmission data to a core network
AA User equipment (UE)
BB Access point
CC Core network

(57) **Abstract:** Disclosed are a protection system, method and device for transmission data. The system comprises: a user equipment (UE) and an access point; the access point sending a broadcast message with an encrypted public key carried therein; the UE receiving and storing the encrypted public key; the UE acquiring, from first pre-stored data, a global public key or a private key corresponding to the UE, and using the encrypted public key and the global public key or the private key corresponding to the UE to protect transmission data; the UE sending a protection message to the access point, the protection message carrying an indication message of a protection method for the transmission data; the access point, after receiving the protection message, acquiring, from second pre-stored data, the global public key and a private key corresponding to the access point according to the indication message of the protection method, and using the global public key and the private key corresponding to the access point to parse the protection message; and the access point sending parsed transmission data to a core network. By means of the embodiments of the present invention, protection is performed on transmission data, so that insecure data is filtered, thereby improving the security of a network.

(57) **摘要**: 本发明实施例公开了一种传输数据的保护系统、方法及装置，所述系统包括：用户设备UE和接入点；接入点发送广播消息，其中携带加密公钥；UE接收并存储加密公钥；UE从第一预存数据中获取全局公钥或者UE对应的私钥，并使用加密公钥和全局公钥或者UE对应的私钥对传输数据进行保护；UE向接入点发送保护消息，保护消息中携带传输数据的保护方式的指示消息；接入点在接收到保护消息之后，根据保护方式的指示消息从其第二预存数据中获取全局公钥和接入点对应的私钥，并使用全局公钥和接入点对应的私钥对保护消息进行解析；接入点将解析得到的传输数据发送到核心网。采用本发明实施例，具有可对传输数据进行保护，过滤不安全数据，从而提高网络的安全性。

WO 2018/006627 A1

[见续页]

(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, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, 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))。

一种传输数据的保护系统、方法及装置

技术领域

本发明涉及通信技术领域，尤其涉及一种传输数据的保护系统、方法及装置。

背景技术

在 4G 网络中，在用户设备（英文：user equipment，UE）与网络交互认证完成之前，UE 与网络之间没有建立共享密钥。UE 与网络的数据传输采用的是明文传输，攻击者容易通过空口信令监听到 UE 的身份信息，造成 UE 的隐私泄露。在 5G 网络中也同样存在上述数据传输的安全隐患。

在 4G 网络的现有技术中，为了保护身份信息，UE 需要在向网络发送附着请求（英文：attachment request）中携带 UE 的非永久身份信息，例如，移动用户伪标识（英文：pseudo mobile subscriber informaiton，PMSI）。网络侧接收到 UE 的 PMSI 之后，给 UE 分配一个新的 PMSI 并通过认证向量传递给 UE。UE 接收到新的 PMSI 之后，在下一次入网时可采用新的 PMSI 给网络侧发送附着请求，避免使用 UE 的永久身份信息（例如，移动用户身份（英文：international mobile subscriber identity，IMSI））发送附着请求，进而避免了攻击者通过空口窃听 UE 的 IMSI，造成 UE 的隐私泄露。然而，UE 每次都使用新的 PMSI 向 HSS 发送附着请求，网络侧需要维护 UE 临时身份的更新，增加了网络侧服务器的复杂度，实现成本高，在 5G 网络的数据传输中适用性低。

此外，在 5G 网络中，为了更好地支撑物联网（英文：internet of things，IOT）设备的数据传输，还需要对无连接数据的传输进行保护。在 3GPP TR 22.799 中，针对无连接数据（英文：connection less data）的发送是在 UE 与网络认证并建立连接后，网络侧为 UE 生成包含安全上下文的 Cookie 并发送给 UE。UE 接收由网络侧发送的带有安全上下文的 Cookie 并保存。当 UE 需要发送数据时，UE 使用 Cookie 中包含的安全上下文信息对数据进行加密，将 Cookie 连同安全上下文发送到网络侧。基站或者网络侧接受到包含安全上下文的 Cookie 后，使用该 Cookie 提供的信息重建安全上下文并解密数据包。由于 Cookie 的内容可能较大，增加了数据传输的信令开销，同时 Cookie 中也包含了用户身份等隐私信息，无法保护 Cookie 中的用户身份等敏感信息，因而存在安全方面的隐患。

发明内容

本申请提供了一种传输数据的保护系统、方法及装置，可对传输数据进行保护，过滤不安全数据，提高了网络的安全性。

第一方面，提供了一种传输数据的保护系统，其可包括：用户设备 UE 和接入点；

所述接入点用于发送广播消息，所述广播消息中携带加密公钥；

所述 UE 用于接收所述接入点的所述广播消息，并存储所述加密公钥；

所述 UE 还用于在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息；

所述 UE 还用于向所述接入点发送所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息；

所述接入点还用于在接收到所述保护消息之后，根据所述保护方式的指示消息从其第二预存数据中获取所述全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据；

所述接入点还用于将解析得到的所述 UE 发送的传输数据发送到核心网中。

在本申请中，UE 向接入点发送上行数据时，可使用接入点的身份等信息作为加密公钥，并使用 IBC 技术的全局公钥对上传传输数据进行加密，可以有效解决网络中对空口信令及其数据的保护，防止用户隐私、信令内容的泄露。接入点对 UE 发送的消息进行解密和签名、完整性校验码等验证，过滤非法信令和数据，保护核心网的安全。

结合第一方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述接入点对应的私钥包括第一私钥和第二私钥；

所述接入点还用于在发送广播消息之前，从网络或者密钥管理系统 KMS 中获取系统参数，并将所述系统参数存储为所述接入点的第二预存数据；

其中，所述系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第一私钥，或者第二全局公钥和第二私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第一私钥为 IBC 技术的所述接入点对应的数据加密私钥 $SK_{BS_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第二私钥为 IBC 技术的所述接入点对应的数据签名私钥 $SK_{BS_ID_Sig}$。

结合第一方面第一种可能的实现方式，在第二种可能的实现方式中，所述加密公钥为基站 BS 的身份 BS_ID，或者所述加密公钥包含 BS_ID；或者

所述加密公钥包括无线保真 Wi-Fi 切入点 AP 的介质控制子层 MAC 地址，或者 Wi-Fi AP 的服务集标识 SSID；或者

所述加密公钥包括热点 UE 的身份 UE_ID，或者热点 UE 的移动用户身份 IMSI。

结合第一方面，在第三种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述 UE 还用于在接收所述接入点的广播消息之前，从网络或者 KMS 中获取所述 UE 用于处理传输数据的处理参数，并将所述处理参数存储为所述 UE 的第一预存数据；

其中，所述处理参数包括 UE 所属运营商的身份 operator ID1 以及以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

结合第一方面第二种可能的实现方式或者第一方面第三种可能的实现方式，在第四种可能的实现方式中，所述第二预存数据中包括所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$；

所述接入点还用于使用所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$ 对所述广播消息进行签名以得到

所述广播消息的签名 Sig1，并在所述广播消息中携带所述接入点具有数据签名功能的指示信息或者所述广播消息的签名 Sig1。

结合第一方面第四种可能的实现方式，在第五种可能的实现方式中，所述第一预存数据中包括所述 operator ID1 和所述 GPK_{Sig};

所述 UE 具体用于:

根据接收到的所述广播消息中携带的指示信息确定所述接入点具有数据签名功能，并根据所述广播消息对应的接入点的标识信息确定所述接入点所属的运营商的身份 operator ID2;

将所述 operator ID2 与所述 operator ID1 进行匹配，从所述第一预存数据中查找所述接入点对应的第三全局公钥 $GPK_{Sig}1$;

当所述广播消息中携带签名 Sig1 时，使用所述 $GPK_{Sig}1$ 和所述接入点的标识信息对所述广播消息进行验证;

当所述广播消息验证通过时，确定将所述广播消息携带的所述加密公钥添加至所述第一预存数据中。

结合第一方面第五种可能的实现方式，在第六种可能的实现方式中，所述第一预存数据中包括所述 GPK_{enc};

所述 UE 具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc};

使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密。

结合第一方面第六种可能的实现方式，在第七种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$、所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$;

所述接入点具体用于:

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息;

执行将所述解密消息中携带的所述 UE 发送的传输数据发送到核心网的步骤。

结合第一方面第五种可能的实现方式，在第八种可能的实现方式中，所述第一预存数据中包括所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$;

所述 UE 具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$;

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成第一对称钥 K1，并将所述传输数据和所述 K1 输入系统函数以获取第三完整性校验码 MAC2;

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据以及所述 UE 的标识信息、所述 MAC2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息以及所述 MAC2 进行加密。

结合第一方面第八种可能的实现方式，在第九种可能的实现方式中，所述第二预存数据中包括加密公钥、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$；

所述接入点具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息；

所述接入点还用于：

从所述解密消息中获取所述保护消息携带的所述 MAC2、UE 的标识信息以及所述传输数据；

使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$ 生成对称钥 K2；

使用所述对称钥 K2、所述 UE 的标识信息和解密得到的传输数据计算第四完整性校验码 MAC3，并当所述 MAC3 与所述 MAC2 相匹配时，执行将所述 UE 发送的传输数据发送到核心网的步骤。

结合第一方面第五种可能的实现方式，在第十种可能的实现方式中，所述第一预存数据中包括所述所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$；

所述 UE 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$；

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig2，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息和所述 Sig2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述 Sig2 进行加密。

结合第一方面第十种可能的实现方式，在第十一种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$ 和所述 GPK_{Sig}；

所述接入点具体用于：

根据所述加密方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以获取所述传输数据；

所述接入点还用于：

从所述保护消息解密得到的解密消息中获取所述 UE 的标识信息和所述签名 Sig2；

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{sig}；

使用所述 UE 的标识信息以及所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，执行将所述 UE 发送的传输数据发送到核心网的步骤。

第二方面，提供了一种传输数据的保护系统，其可包括：用户设备 UE、接入点和核心网节点；

所述 UE 用于在需要发送传输数据时，从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息；

所述 UE 还用于向所述接入点发送所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息；

所述接入点用于向所述核心网节点发送所述保护消息；

所述核心网节点用于在接收到所述保护消息之后，根据所述保护方式的指示消息从其第二预存数据中获取所述全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据。

在本申请中，UE 向核心网节点发送上行数据时，可使用核心网节点的身份等信息作为加密公钥，并使用 IBC 技术的全局公钥和核心网节点对应的私钥对上传传输数据进行加密，可以有效解决网络中对空口信令及其数据的保护，防止用户隐私、信令内容的泄露。核心网节点对 UE 发送的消息进行解密和签名、完整性校验码等验证，过滤非法信令和数据，保护核心网的安全。

结合第二方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥；

所述核心网节点还用于从密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据；

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

结合第二方面第一种可能的实现方式，在第二种可能的实现方式中，所述加密公钥为核心网认证节点的身份，或者所述加密公钥包含所述核心网节点的身份。

结合第二方面，在第三种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述 UE 还用于从核心网中获取加密公钥、所述 UE 用于处理传输数据的核心网处理参数，并将所述加密公钥和所述核心网处理参数存储为所述 UE 的第一预存数据；

其中，所述核心网处理参数包括以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

结合第二方面第二种可能的实现方式或者第二方面第三种可能的实现方式，在第四种可能的实现方式中，所述第一预存数据中包括所述加密公钥和所述 GPK_{enc}；

所述 UE 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc}；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密。

结合第二方面第四种可能的实现方式，在第五种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述核心网节点具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到所述 UE 的传输数据。

结合第二方面第二种可能的实现方式或者第二方面第三种可能的实现方式，在第六种可能的实现方式中，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述 UE 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$；

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成对称钥 K3，并将所述传输数据和所述 K3 输入系统函数以获取第四完整性校验码 MAC3；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密。

结合第二方面第六种可能的实现方式，在第七种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述核心网节点具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$，对所述保护消息进行解密以得到解密消息；

使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$ 生成对称钥 K4；

使用所述 K4、所述 UE 的标识信息和所述解密消息生成第五完整性校验码 MAC4，并当所述 MAC4 与所述 MAC3 相匹配时，获取所述传输数据。

结合第二方面第三种可能的实现方式或者第二方面第三种可能的实现方式，在第八种可能的实现方式中，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$；

所述 UE 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$；

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig3，并使用

所述加密公钥、所述 GPK_{enc} 对所述传输数据和所述签名 Sig2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述签名进行加密。

结合第二方面第八种可能的实现方式，在第九种可能的实现方式中，所述第二预存数据中包括所述加密公钥、所述 GPK_{enc}、所述 $SK_{CP_ID_enc}$ 和所述 GPK_{Sig};

所述核心网节点具体用于:

根据所述加密方式的指示消息确定所述传输数据的保护方式，并使用从所述第二预存数据中获取的所述 GPK_{enc}、所述加密公钥和所述 $SK_{CP_ID_enc}$ 对所述保护消息进行解密;

从所述保护消息解密得到的解密消息中获取所述签名 Sig3，并使用所述 UE 的标识信息和所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，获取所述传输数据。

第三方面，提供了一种传输数据的保护系统，其可包括: 用户设备 UE、接入点和核心网节点;

所述核心网节点用于接收用户面网关下发的传输数据，并从其第二预存数据中获取所述 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥;

所述核心网节点还用于使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述传输数据进行保护以得到保护消息，并将所述保护消息发送给所述接入点;

所述接入点用于将所述保护消息发送给所述 UE;

所述 UE 从其第一预存数据中获取所述所述核心网节点的标识，所述全局公钥和所述 UE 对应的私钥对所述保护消息进行解析以得到所述传输数据。

在本申请中，UE 和核心网节点可使用基于 IBC 的技术对下行数据进行加密和验证保护，增强了网络传输数据的安全性。

结合第三方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥;

所述核心网节点还用于从网络或者密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据;

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组: 第一全局公钥和第五私钥，或者第二全局公钥和第六私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

结合第三方面，在第二种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥;

所述 UE 还用于从核心网中获取其标识信息、所述 UE 用于处理传输数据的核心网处理参数，并将所述标识信息和所述核心网处理参数存储为所述 UE 的第一预存数据;

其中，所述核心网处理参数包括以下两组数据中至少一组: 第一全局公钥和第三私钥，

或者第二全局公钥和第四私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

结合第三方面第一种可能的实现方式或者第三方面第二种可能的实现方式，在第三种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述核心网节点具体用于:

在接收到所述传输数据之后，从所述第二预存数据中获取所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$;

根据所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$ 生成对称钥 K5，并将所述传输数据和所述 K5 输入系统函数以获取第六完整性校验码 MAC5;

使用所述 K5 对所述传输数据加密得到保护消息。

结合第三方面第三种可能的实现方式，在第四种可能的实现方式中，所述第一预存数据中包括所述 UE 的标识信息、所述核心网节点的标识、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$;

所述 UE 具体用于:

从所述第一预存数据中获取所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$，并使用所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 对所述保护消息进行解密以得到解密消息;

使用所述核心网节点的标识信息、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 生成对称钥 K6;

使用所述 K6 对所述保护消息进行解密以得到解密消息;

使用所述 K6 和所述解密消息生成第七完整性校验码 MAC6，并当所述 MAC6 与所述解密消息中携带的 MAC5 相匹配时，获取所述传输数据。

第四方面，提供了一种传输数据的保护方法，其可包括:

用户设备 UE 接收接入点发送的广播消息，并存储所述广播消息中携带的加密公钥;

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息;

所述 UE 向所述接入点发送所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息。

结合第四方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥;

所述 UE 接收所述接入点的广播消息之前，所述方法还包括:

所述 UE 从网络或者 KMS 中获取所述 UE 用于处理传输数据的处理参数，并将所述处理参数存储为所述 UE 的第一预存数据;

其中，所述处理参数包括 UE 所属运营商的身份 operator ID1 以及以下三组数据中至少一组: 第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

结合第四方面第一种可能的实现方式，在第二种可能的实现方式中，所述第一预存数据中包括所述 operator ID1 和所述 GPK_{Sig};

所述 UE 存储所述广播消息中携带的加密公钥之前，所述方法还包括:

所述 UE 根据接收到的所述广播消息中携带的指示信息确定所述接入点具有数据签名功能，并根据所述广播消息对应的接入点的标识信息确定所述接入点所属的运营商的身份 operator ID2;

将所述 operator ID2 与所述 operator ID1 进行匹配，从所述第一预存数据中查找所述接入点对应的第三全局公钥 $GPK_{Sig}1$;

当所述广播消息中携带签名 Sig1 时，使用所述 $GPK_{Sig}1$ 和所述接入点的标识信息对所述广播消息进行验证;

当所述广播消息验证通过时，确定将所述广播消息携带的所述加密公钥添加至所述第一预存数据中。

结合第四方面第二种可能的实现方式，在第三种可能的实现方式中，所述第一预存数据中包括所述 GPK_{enc};

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥，并使用所述加密公钥和所述全局公钥对所述传输数据进行保护包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc};

使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密。

结合第四方面第二种可能的实现方式，在第四种可能的实现方式中，所述第一预存数据中包括所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$;

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$;

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成第一对称钥 K1，并将所述传输数据和所述 K1 输入系统函数以获取第三完整性校验码 MAC2;

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据以及所述 UE 的标识信息、所述 MAC2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息以及所述 MAC2 进行加密。

结合第四方面第二种可能的实现方式，在第五种可能的实现方式中，所述第一预存数据中包括所述所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$；

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息包括：

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$；

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig2，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息和所述 Sig2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述 Sig2 进行加密。

第五方面，提供了一种传输数据的保护方法，其可包括：

接入点发送广播消息，所述广播消息中携带加密公钥；

所述接入点接收用户设备 UE 发送的根据所述加密公钥对传输数据进行保护得到的保护消息，所述保护消息中携带所述 UE 发送的传输数据的保护方式的指示消息；

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据；

所述接入点将解析得到的所述 UE 发送的传输数据发送到核心网中。

结合第五方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述接入点对应的私钥包括第一私钥和第二私钥；

所述接入点发送广播消息之前，所述方法还包括：

所述接入点从网络或者密钥管理系统 KMS 中获取系统参数，并将所述系统参数存储为所述接入点的第二预存数据；

其中，所述系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第一私钥，或者第二全局公钥和第二私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第一私钥为 IBC 技术的所述接入点对应的数据加密私钥 $SK_{BS_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第二私钥为 IBC 技术的所述接入点对应的数据签名私钥 $SK_{BS_ID_Sig}$。

结合第五方面第一种可能的实现方式，在第二种可能的实现方式中，所述加密公钥为基站 BS 的身份 BS_ID，或者所述加密公钥包含 BS_ID；或者

所述加密公钥包括无线保真 Wi-Fi 切入点 AP 的介质控制子层 MAC 地址，或者 Wi-Fi AP 的服务集标识 SSID；或者

所述加密公钥包括热点 UE 的身份 UE_ID，或者热点 UE 的移动用户身份 IMSI。

结合第五方面第二种可能的实现方式，在第三种可能的实现方式中，所述第二预存数

据中包括所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$;

所述接入点发送广播消息之前，所述方法还包括:

所述接入点使用所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$ 对所述广播消息进行签名以得到所述广播消息的签名 Sig1，并在所述广播消息中携带所述接入点具有数据签名功能的指示信息或者所述广播消息的签名 Sig1。

结合第五方面第二种可能的实现方式，在第四种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$、所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$;

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析包括:

所述接入点根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息。

结合第五方面第二种可能的实现方式，在第五种可能的实现方式中，所述第二预存数据中包括加密公钥、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$;

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析包括:

所述接入点根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息;

所述接入点将解析得到的所述 UE 发送的传输数据发送到核心网中包括:

所述接入点从所述解密消息中获取所述保护消息携带的第三完整性保护码 MAC2、UE 的标识信息以及所述传输数据;

使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$ 生成对称钥 K2;

使用所述对称钥 K2、所述 UE 的标识信息和解密得到的传输数据计算第四完整性校验码 MAC3，并当所述 MAC3 与所述 MAC2 相匹配时，将所述 UE 发送的传输数据发送到核心网。

结合第五方面第二种可能的实现方式，在第六种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$ 和所述 GPK_{Sig};

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析包括:

根据所述加密方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以获取所述传输数据;

所述接入点将解析得到的所述 UE 发送的传输数据发送到核心网中包括:

从所述保护消息解密得到的解密消息中获取所述 UE 的标识信息和所述签名 Sig2;

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{sig};

使用所述 UE 的标识信息以及所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，将所述 UE 发送的传输数据发送到核心网。

第六方面，提供了一种传输数据的保护方法，其可包括:

用户设备 UE 在需要发送传输数据时，从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息;

所述 UE 向接入点发送所述保护消息，以通过所述接入点将所述保护消息发送给核心网节点，所述保护消息中携带所述传输数据的保护方式的指示消息。

结合第六方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥;

所述 UE 发送传输数据之前，所述方法还包括:

所述 UE 从核心网中获取加密公钥、所述 UE 用于处理传输数据的核心网处理参数，并将所述加密公钥和所述核心网处理参数存储为所述 UE 的第一预存数据;

其中，所述核心网处理参数包括以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

结合第六方面第一种可能的实现方式，在第二种可能的实现方式中，所述第一预存数据中包括所述加密公钥和所述 GPK_{enc};

所述 UE 从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥，并使用所述加密公钥，以及所述全局公钥对所述传输数据进行保护包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc};

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密。

结合第六方面第一种可能的实现方式，在第三种可能的实现方式中，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$;

所述 UE 从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$;

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成对称钥 K3，并将所述传输数据和所述 K3 输入系统函数以获取第四完整性校验码 MAC3;

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密。

结合第六方面第二种可能的实现方式，在第四种可能的实现方式中，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$;

所述 UE 从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$;

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig3，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据和所述签名 Sig2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述签名进行加密。

第七方面，提供了一种传输数据的保护方法，其可包括:

核心网节点接收接入点发送的保护消息，所述保护消息中携带用户设备 UE 发送的所述传输数据的保护方式的指示消息;

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据。

结合第七方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥;

所述核心网节点接收接入点发送的保护消息之前，所述方法还包括:

所述核心网节点从密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据;

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

结合第七方面第一种可能的实现方式，在第二种可能的实现方式中，所述加密公钥为核心网认证节点的身份，或者所述加密公钥包含所述核心网节点的身份。

结合第七方面第二种可能的实现方式，在第三种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析包括:

所述核心网节点根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到所述 UE 的传输数据。

结合第七方面第二种可能的实现方式，在第四种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析包括:

所述核心网节点根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$，对所述保护消息进行解密以得到解密消息;

获取所述解密消息中携带的第四完整性校验码 MAC3，并使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$ 生成对称钥 K4;

使用所述 K4、所述 UE 的标识信息和所述解密消息生成第五完整性校验码 MAC4，并当所述 MAC4 与所述 MAC3 相匹配时，获取所述传输数据。

结合第七方面第二种可能的实现方式，在第五种可能的实现方式中，所述第二预存数据中包括所述加密公钥、所述 GPK_{enc}、所述 $SK_{CP_ID_enc}$ 和所述 GPK_{Sig};

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析包括:

所述核心网节点根据所述加密方式的指示消息确定所述传输数据的保护方式，并使用从所述第二预存数据中获取的所述 GPK_{enc}、所述加密公钥和所述 $SK_{CP_ID_enc}$ 对所述保护消息进行解密;

从所述保护消息解密得到的解密消息中获取所述签名 Sig3，并使用所述 UE 的标识信息和所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，获取所述传输数据。

第八方面，提供了一种传输数据的保护方法，其可包括:

核心网节点接收用户面网关下发的传输数据，并从其第二预存数据中获取用户设备 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥;

所述核心网节点使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述传输数据进行保护以得到保护消息，并将所述保护消息发送给接入点。

结合第八方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥;

所述核心网节点接收用户面网关下发的传输数据之前，所述方法还包括:

所述核心网节点从网络或者密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据；

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

结合第八方面第一种可能的实现方式，在第二种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述核心网节点从其第二预存数据中获取用户设备 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥包括：

所述核心网节点从所述第二预存数据中获取所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$；

所述核心网节点使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述传输数据进行保护以得到保护消息包括：

所述核心网节点根据所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$ 生成对称钥 K5，并将所述传输数据和所述 K5 输入系统函数以获取第六完整性校验码 MAC5；

使用所述 K5 对所述传输数据加密得到保护消息。

第九方面，提供了一种传输数据的保护方法，其可包括：

用户设备 UE 接收接入点发送的保护消息；

所述 UE 从其第一预存数据中获取核心网节点的标识，基于身份的密码 IBC 技术的全局公钥和所述 UE 对应的私钥对所述保护消息进行解析以得到所述传输数据。

结合第九方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述 UE 接收接入点发送的保护消息之前，所述方法还包括：

所述 UE 从核心网中获取其标识信息、所述 UE 用于处理传输数据的核心网处理参数，并将所述标识信息和所述核心网处理参数存储为所述 UE 的第一预存数据；

其中，所述核心网处理参数包括以下两组数据中至少一组：第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

结合第九方面第一种可能的实现方式，在第二种可能的实现方式中，所述第一预存数据中包括所述 UE 的标识信息、所述核心网节点的标识、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述 UE 从其第一预存数据中获取核心网节点的标识，基于身份的密码 IBC 技术的全

局公钥和所述 UE 对应的私钥对所述保护消息进行解析以得到所述传输数据包括:

所述 UE 从所述第一预存数据中获取所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$，并使用所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 对所述保护消息进行解密以得到解密消息;

使用所述核心网节点的标识信息、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 生成对称钥 K6;

使用所述 K6 对所述保护消息进行解密以得到解密消息;

使用所述 K6 和所述解密消息生成第七完整性校验码 MAC6，并当所述 MAC6 与所述解密消息中携带的第六完整性校验码 MAC5 相匹配时，获取所述传输数据。

第十方面，提供了一种传输数据的保护装置，其可包括:

接收单元，用于接收接入点发送的广播消息，并存储所述广播消息中携带的加密公钥;

处理单元，用于在需要向所述接入点发送传输数据时，从用户设备 UE 的第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述接收单元接收的所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息;

发送单元，用于向所述接入点发送所述处理单元处理的所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息。

结合第十方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥;

所述处理单元还用于:

从网络或者 KMS 中获取所述 UE 用于处理传输数据的处理参数，并将所述处理参数存储为所述 UE 的第一预存数据;

其中，所述处理参数包括 UE 所属运营商的身份 operator ID1 以及以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

结合第十方面第一种可能的实现方式，在第二种可能的实现方式中，所述第一预存数据中包括所述 operator ID1 和所述 GPK_{Sig};

所述接收单元具体用于:

根据接收到的所述广播消息中携带的指示信息确定所述接入点具有数据签名功能，并根据所述广播消息对应的接入点的标识信息确定所述接入点所属的运营商的身份 operator ID2;

将所述 operator ID2 与所述 operator ID1 进行匹配，从所述第一预存数据中查找所述接入点对应的第三全局公钥 $GPK_{Sig}1$;

当所述广播消息中携带签名 Sig1 时，使用所述 $GPK_{Sig}1$ 和所述接入点的标识信息对所述广播消息进行验证;

当所述广播消息验证通过时，确定将所述广播消息携带的所述加密公钥添加至所述第

一预存数据中。

结合第十方面第二种可能的实现方式，在第三种可能的实现方式中，所述第一预存数据中包括所述 GPK_{enc};

所述处理单元具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc};

使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密。

结合第十方面第二种可能的实现方式，在第四种可能的实现方式中，所述第一预存数据中包括所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$;

所述处理单元具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$;

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成第一对称钥 K1，并将所述传输数据和所述 K1 输入系统函数以获取第三完整性校验码 MAC2;

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据以及所述 UE 的标识信息、所述 MAC2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息以及所述 MAC2 进行加密。

结合第十方面第二种可能的实现方式，在第五种可能的实现方式中，所述第一预存数据中包括所述所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$;

所述处理单元具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$;

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig2，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息和所述 Sig2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述 Sig2 进行加密。

第十一方面，提供了一种传输数据的保护装置，其可包括:

发送单元，用于发送广播消息，所述广播消息中携带加密公钥;

接收单元，用于接收用户设备 UE 发送的根据所述发送单元发送的所述加密公钥对传输数据进行保护得到的保护消息，所述保护消息中携带所述 UE 发送的传输数据的保护方式的指示消息;

解析单元，用于根据所述接收单元接收的所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公

钥和所述接入点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据;

所述发送单元，还用于将所述解析单元解析得到的所述 UE 发送的传输数据发送到核心网中。

结合第十一方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述接入点对应的私钥包括第一私钥和第二私钥;

所述解析单元还用于:

从网络或者密钥管理系统 KMS 中获取系统参数，并将所述系统参数存储为所述接入点的第二预存数据;

其中，所述系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第一私钥，或者第二全局公钥和第二私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第一私钥为 IBC 技术的所述接入点对应的数据加密私钥 $SK_{BS_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第二私钥为 IBC 技术的所述接入点对应的数据签名私钥 $SK_{BS_ID_Sig}$。

结合第十一方面第一种可能的实现方式，在第二种可能的实现方式中，所述加密公钥为基站 BS 的身份 BS_ID，或者所述加密公钥包含 BS_ID; 或者

所述加密公钥包括无线保真 Wi-Fi 切入点 AP 的介质控制子层 MAC 地址，或者 Wi-Fi AP 的服务集标识 SSID; 或者

所述加密公钥包括热点 UE 的身份 UE_ID，或者热点 UE 的移动用户身份 IMSI。

结合第十一方面第二种可能的实现方式，在第三种可能的实现方式中，所述第二预存数据中包括所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$;

所述发送单元具体用于:

使用所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$ 对所述广播消息进行签名以得到所述广播消息的签名 Sig1，并在所述广播消息中携带所述接入点具有数据签名功能的指示信息或者所述广播消息的签名 Sig1。

结合第十一方面第二种可能的实现方式，在第四种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$、所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$;

所述解析单元具体用于:

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息。

结合第十一方面第二种可能的实现方式，在第五种可能的实现方式中，所述第二预存数据中包括加密公钥、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$;

所述解析单元具体用于:

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息;

所述发送单元具体用于:

从所述解析单元解析得到的所述解密消息中获取所述保护消息携带的第三完整性保护码 MAC2、UE 的标识信息以及所述传输数据;

使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$ 生成对称钥 K2;

使用所述对称钥 K2、所述 UE 的标识信息和解密得到的传输数据计算第四完整性校验码 MAC3，并当所述 MAC3 与所述 MAC2 相匹配时，将所述 UE 发送的传输数据发送到核心网。

结合第十一方面第二种可能的实现方式，在第六种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$ 和所述 GPK_{Sig};

所述解析单元具体用于:

根据所述加密方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以获取所述传输数据;

所述发送单元具体用于:

从所述保护消息解密得到的解密消息中获取所述 UE 的标识信息和所述签名 Sig2;

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{sig};

使用所述 UE 的标识信息以及所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，将所述 UE 发送的传输数据发送到核心网。

第十二方面，提供了一种传输数据的保护装置，其可包括:

保护单元，用于在需要发送传输数据时，从用户设备的第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息;

发送单元，用于向接入点发送所述保护单元处理得到的所述保护消息，以通过所述接入点将所述保护消息发送给核心网节点，所述保护消息中携带所述传输数据的保护方式的指示消息。

结合第十二方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥;

所述保护单元还用于:

从核心网中获取加密公钥、所述 UE 用于处理传输数据的核心网处理参数，并将所述加密公钥和所述核心网处理参数存储为所述 UE 的第一预存数据;

其中，所述核心网处理参数包括以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

结合第十二方面第一种可能的实现方式，在第二种可能的实现方式中，所述第一预存

数据中包括所述加密公钥和所述 GPK_{enc};

所述保护单元具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc};

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密。

结合第十二方面第一种可能的实现方式，在第三种可能的实现方式中，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$;

所述保护单元具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$;

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成对称钥 K3，并将所述传输数据和所述 K3 输入系统函数以获取第四完整性校验码 MAC3;

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密。

结合第十二方面第一种可能的实现方式，在第四种可能的实现方式中，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$;

所述保护单元具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$;

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig3，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据和所述签名 Sig2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述签名进行加密。

第十三方面，提供了一种传输数据的保护装置，其可包括:

接收单元，用于接收接入点发送的保护消息，所述保护消息中携带用户设备 UE 发送的所述传输数据的保护方式的指示消息;

解析单元，用于根据所述接收单元接收的所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据。

结合第十三方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥;

所述解析单元还用于:

从密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核

心网接入点的第二预存数据;

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

结合第十三方面，第一种可能的实现方式，在第二种可能的实现方式中，所述加密公钥为核心网认证节点的身份，或者所述加密公钥包含所述核心网节点的身份。

结合第十三方面，第二种可能的实现方式，在第三种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述解析单元具体用于:

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到所述 UE 的传输数据。

结合第十三方面，第二种可能的实现方式，在第四种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述解析单元具体用于:

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$，对所述保护消息进行解密以得到解密消息;

获取所述解密消息中携带的第四完整性校验码 MAC3，并使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$ 生成对称钥 K4;

使用所述 K4、所述 UE 的标识信息和所述解密消息生成第五完整性校验码 MAC4，并当所述 MAC4 与所述 MAC3 相匹配时，获取所述传输数据。

结合第十三方面，第二种可能的实现方式，在第五种可能的实现方式中，所述第二预存数据中包括所述加密公钥、所述 GPK_{enc}、所述 $SK_{CP_ID_enc}$ 和所述 GPK_{Sig};

所述解析单元具体用于:

根据所述加密方式的指示消息确定所述传输数据的保护方式，并使用从所述第二预存数据中获取的所述 GPK_{enc}、所述加密公钥和所述 $SK_{CP_ID_enc}$ 对所述保护消息进行解密;

从所述保护消息解密得到的解密消息中获取所述签名 Sig3，并使用所述 UE 的标识信息和所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，获取所述传输数据。

第十四方面，提供了一种传输数据的保护装置，其可包括:

接收单元，用于接收用户面网关下发的传输数据;

处理单元，用于从核心网节点的第二预存数据中获取用户设备 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥，并使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述接收单元接收的所述传输数据进行保护以得到保护

消息。

发送单元，用于将所述处理单元处理得到的所述保护消息发送给接入点。

结合第十四方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥；

所述处理单元还用于：

从网络或者密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据；

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

结合第十四方面第一种可能的实现方式，在第二种可能的实现方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述处理单元具体用于：

从所述第二预存数据中获取所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$；

根据所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$ 生成对称钥 K5，并将所述传输数据和所述 K5 输入系统函数以获取第六完整性校验码 MAC5；

使用所述 K5 对所述传输数据加密得到保护消息。

第十五方面，提供了一种传输数据的保护装置，其可包括：

接收单元，用于接收接入点发送的保护消息；

解析单元，用于从用户设备的第一预存数据中获取核心网节点的标识，基于身份的密码 IBC 技术的全局公钥和所述 UE 对应的私钥对所述保护消息进行解析以得到所述传输数据。

结合第十五方面，在第一种可能的实现方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述解析单元还用于：

从核心网中获取其标识信息、所述 UE 用于处理传输数据的核心网处理参数，并将所述标识信息和所述核心网处理参数存储为所述 UE 的第一预存数据；

其中，所述核心网处理参数包括以下两组数据中至少一组：第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

结合第十五方面第一种可能的实现方式，在第二种可能的实现方式中，所述第一预存数据中包括所述 UE 的标识信息、所述核心网节点的标识、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述解析单元具体用于:

从所述第一预存数据中获取所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$，并使用所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 对所述保护消息进行解密以得到解密消息;

使用所述核心网节点的标识信息、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 生成对称钥 K6;

使用所述 K6 对所述保护消息进行解密以得到解密消息;

使用所述 K6 和所述解密消息生成第七完整性校验码 MAC6，并当所述 MAC6 与所述解密消息中携带的 MAC5 相匹配时，获取所述传输数据。

第十六方面提供了一种用户设备，其可包括：存储器和处理器，所述存储器和所述处理器相连;

所述存储器用于存储一组程序代码;

所述处理器用于调用所述存储器中存储的程序代码，执行如上述第四方面提供的传输数据的保护方法。

第十七方面提供了一种接入点，其可包括：存储器和处理器，所述存储器和所述处理器相连;

所述存储器用于存储一组程序代码;

所述处理器用于调用所述存储器中存储的程序代码，执行如上述第五方面提供的传输数据的保护方法。

第十八方面提供了一种用户设备，其可包括：存储器和处理器，所述存储器和所述处理器相连;

所述存储器用于存储一组程序代码;

所述处理器用于调用所述存储器中存储的程序代码，执行如上述第六方面提供的传输数据的保护方法。

第十九方面提供了一种核心网节点，其可包括：存储器和处理器，所述存储器和所述处理器相连;

所述存储器用于存储一组程序代码;

所述处理器用于调用所述存储器中存储的程序代码，执行如上述第七方面提供的传输数据的保护方法。

第二十方面提供了一种核心网节点，其可包括：存储器和处理器，所述存储器和所述处理器相连;

所述存储器用于存储一组程序代码;

所述处理器用于调用所述存储器中存储的程序代码，执行如上述第八方面提供的传输数据的保护方法。

第二十一方面提供了一种用户设备，其可包括：存储器和处理器，所述存储器和所述处理器相连;

所述存储器用于存储一组程序代码;

所述处理器用于调用所述存储器中存储的程序代码，执行如上述第九方面提供的传输数据的保护方法。

由上可知，本申请公开了一种传输数据的保护系统、方法及装置，上述系统包括：用户设备 UE 和接入点；接入点发送广播消息，其中携带加密公钥；UE 接收并存储加密公钥；UE 从第一预存数据中获取全局公钥或者 UE 对应的私钥，并使用加密公钥和全局公钥或者 UE 对应的私钥对传输数据进行保护；UE 向接入点发送保护消息，保护消息中携带传输数据的保护方式的指示消息；接入点在接收到保护消息之后，根据保护方式的指示消息从其第二预存数据中获取全局公钥和接入点对应的私钥，并使用全局公钥和接入点对应的私钥对保护消息进行解析；接入点将解析得到的传输数据发送到核心网。采用本申请，具有可对传输数据进行保护，过滤不安全数据，从而提高网络的安全性。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明实施例提供的数据传输的一传输架构图；

图 2 是本发明实施例提供的传输数据的保护系统进行数据传输的一交互示意图；

图 3 是本发明实施例提供的保护系统在场景一中的一交互示意图；

图 4 是本发明实施例提供的保护系统在场景一中的另一交互示意图；

图 5 是本发明实施例提供的保护系统在场景二中的一交互示意图；

图 6 是本发明实施例提供的保护系统在场景二中的另一交互示意图；

图 7 是本发明实施例提供的保护系统在场景三中的交互示意图；

图 8 是本发明实施例提供的保护系统在场景四中的交互示意图；

图 9 是本发明实施例提供的数据传输的另一传输架构图；

图 10 是本发明实施例提供的传输数据的保护系统进行数据传输的另一交互示意图；

图 11 是本发明实施例提供的保护系统在场景五中的一交互示意图；

图 12 是本发明实施例提供的保护系统在场景五中的另一交互示意图；

图 13 是本发明实施例提供的保护系统在场景五中的另一交互示意图；

图 14 是本发明实施例提供的数据传输的另一传输架构图；

图 15 是本发明实施例提供的传输数据的保护系统进行下行数据传输的交互示意图；

图 16 是本发明实施例提供的保护系统在场景六中的交互示意图；

图 17 是本发明实施例提供的传输数据的保护方法的一流程示意图；

图 18 是本发明实施例提供的传输数据的保护方法的另一流程示意图；

图 19 是本发明实施例提供的传输数据的保护方法的另一流程示意图；

图 20 是本发明实施例提供的传输数据的保护方法的另一流程示意图；

图 21 是本发明实施例提供的传输数据的保护方法的另一流程示意图；

图 22 是本发明实施例提供的传输数据的保护方法的另一流程示意图；

图 23 是本发明实施例提供的传输数据的保护装置的一结构示意图；

图 24 是本发明实施例提供的传输数据的保护装置的另一结构示意图；

图 25 是本发明实施例提供的传输数据的保护装置的另一结构示意图;
图 26 是本发明实施例提供的传输数据的保护装置的另一结构示意图;
图 27 是本发明实施例提供的传输数据的保护装置的另一结构示意图;
图 28 是本发明实施例提供的传输数据的保护装置的另一结构示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

基于身份的密码（英文：Identity Based Cryptography，IBC）技术提供一种基于身份的加密（英文：Identity Based Encryption，IBE）技术和基于身份的签名（英文：Identity Based Signature，IBS）技术等。IBC技术属于一种公钥技术。首先密钥的产生是基于一对全局参数，包括全局公钥（英文：Global Public Key，GPK）和全局私钥（英文：Global Secret Key，GSK）。其中，密钥产生方根据用户提供的身份（英文：Identity，ID）信息，使用上述全局参数进行运算，为用户产生一个对应于该用户的ID的私钥SK_{ID}。例如，密钥产生方可根据UE提供的身份（如，UE_ID），使用上述全局参数进行运算得到UE对应的私钥SK_{UE_ID}。进一步的，可将上述用户的ID、私钥SK_{ID}和全局公钥GPK通过可靠手段分发给用户，具体手段可根据实际应用场景确定。

在使用IBC技术加密时，加密方需要获得加密公钥（具体可为接收方的ID）和全局公钥GPK。加密方使用接收方的ID和全局公钥加密用户的明文数据M，形成密文E(M)，并发送给接收方。接收方接收到密文E(M)，首先根据自身的ID获得该ID相对应的用于解密的私钥SK_{ID}和全局公钥GPK，并使用SK_{ID}和GPK解密密文E(M)，获得相应的明文M。

在使用IBC技术签名时，签名方需要拥有自身的ID，用于签名的私钥SK_{ID}和全局公钥GPK。签名方使用全局公钥和私钥SK_{ID}对用户的明文数据M签名，形成签名Sig（SK_{ID}, M），并把签名后的消息{ID, M, Sig(SK_{ID}, M)}发送给接收方。接收方接收到带有签名的消息后，首先根据消息中携带的ID获得相对应的全局公钥GPK，并使用ID和GPK验证消息中携带的签名Sig（SK_{ID}，M），以验证消息的完整性。

IBC 技术与现有的基于公钥基础设施（英文：Public Key Infrastructure， PKI）的公钥技术不同之处在于，现有 PKI 技术中的公钥是一串随机数字，不具有身份意义特征，而 IBC 技术弥补了这方面的的缺陷。在 IBC 技术中，公钥可以是任意一串有意义的字符，通常是我们现实生活中的身份信息，如 email 地址 abc@xyz.com 等，也可以使用电话号码或者 IMSI 等信息，便于记忆和验证。

本发明实施例可使用 IBC 技术保护空口信令或者低频小数据的传输，即本发明中所描述的传输数据可包括空口信令或者无连接的低频小数据等，具体可根据实际应用场景确定，在此不做限制。

参见图 1，是本发明实施例提供的数据传输的一传输架构图。在图 1 所示的传输架构中，可包括 UE、接入点和核心网等数据传输端。其中，接入点可包括基站（英文：Base Station，

BS），无线保真（英文：Wireless-Fidelity，Wi-Fi）网络中的接入点（英文：Access Point，AP）或者作为网络热点的热点 UE。其中，上述 BS 可为 3G 网络中的基站（英文：Node B，NB），也可为 4G 网络中的演进性基站（英文：Evolved Node B，eNB），或者更早前的网络时代中的基站，在此不做限制。

参见图 2，图 2 是本发明实施例提供的传输数据的保护系统进行数据传输的一交互示意图。本发明实施例提供的保护系统中各个数据传输端进行数据传输的过程可包括步骤：

S201，接入点向 UE 发送广播消息。

在一些可行的实施方式中，接入点发送广播消息之前，可预先从网络或者密钥管理系统（英文：Key Management System，KMS）获取系统参数，并将获取的系统参数存储在接入点的指定存储空间，即可将获取的系统参数存储为接入点的预存数据（即第二预存数据）。其中，接入点从网络或者 KMS 中获取的系统参数可包括加密公钥，或者第一全局公钥和私钥，或者第二全局公钥和私钥等。其中，接入点从网络或者 KMS 中获取的系统参数具体包含的信息可根据接入点在实际应用场景中执行的数据传输操作的需求确定，在此不做限制。

具体实现中，上述加密公钥可为接入点的标识。若具体应用场景中，上述接入点为 BS，则上述加密公钥可为 BS 的身份（即 BS_ID），或者上述加密公钥包含 BS_ID。其中，上述加密公钥包含 BS_ID 表示上述加密公钥由 BS_ID 和其他数据构成，BS_ID 只是加密公钥的长串数据中的一部分数据，具体可根据时间采用的加密公钥的数据形式确定，在此不做限制。

若具体应用场景中，上述接入点为 Wi-Fi AP，则上述加密公钥可为 Wi-Fi AP 的介质控制子层（英文：Media Access Control，MAC）地址，或者 Wi-Fi AP 的服务集标识（英文：Service Set Identifier，SSID）。具体实现中，接入点为 WiFi AP 时，加密公钥的具体组成形式可根据实际应用场景确定，在此不做限制。

若具体应用场景中，上述接入点为热点 UE，则上述加密公钥可为热点 UE 的 UE_ID，或者热点 UE 的移动用户身份（英文：International Mobile Subscriber Identity，IMSI）。具体实现中，接入点为热点 UE 时，加密公钥的具体组成形式可根据实际应用场景确定，在此不做限制。

进一步的，具体实现中，上述接入点从网络或者 KMS 中获取的第一全局公钥可为 IBC 技术的数据加密全局公钥 GPK_{enc}。第一私钥可使用 IBC 技术根据接入点的 ID 和上述 GPK_{enc} 生成的接入点对应的数据加密私钥 $SK_{BS_ID_enc}$。其中，上述接入点 BS、Wi-Fi AP 和热点 UE 在数据传输中都作为基站，上述生成数据加密私钥时使用的接入点的 ID 包括 BS 的 ID、WiFi AP 的 ID 或者热点 UE 的 ID，因此接入点对应的数据加密私钥均表示为 $SK_{BS_ID_enc}$。上述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}。第二私钥为使用 IBC 技术根据接入点的 ID 和上述 GPK_{Sig} 生成的接入点对应的数据签名私钥 $SK_{BS_ID_Sig}$。同理，上述接入点 BS、Wi-Fi AP 和热点 UE 在数据传输中都作为基站，上述生成数据签名私钥时使用的接入点的 ID 包括 BS 的 ID、WiFi AP 的 ID 或者热点 UE 的 ID，因此接入点对应的数据签名私钥均表示为 $SK_{BS_ID_Sig}$。

在一些可行的实施方式中，UE 也可从网络或者上述 KMS 中获取用于处理传输数据的处理参数。其中，上述处理参数可包括 UE 所属运营商的身份、全局公钥或者 UE 对应的私

钥等。其中，上述 UE 所属运营商的身份可表示为 operator ID1，例如 UE 所属运营商为运营商 A 时，上述 operator ID1 则为运营商 A 的身份。上述全局公钥包括第一全局公钥和第二全局公钥，上述私钥包括第三私钥和第四私钥。其中，上述第一全局公钥为与接入点获取的第一全局公钥相同的数据加密全局公钥 GPK_{enc}。上述第二全局公钥为与接入点获取的第二全局公钥相同的数据签名全局公钥 GPK_{sig}。上述第三私钥可使用 IBC 技术根据 UE_ID 和上述 GPKenc 生成的 UE 对应的数据加密私钥 $SK_{UE_ID_enc}$。上述第四私钥为使用 IBC 技术根据 UE_ID 和上述 GPK_{sig} 生成的 UE 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

具体实现中，接入点可周期性向 UE 发送广播消息，并在上述广播消息中携带上述加密公钥，以供 UE 根据上述加密公钥进行数据保护。

进一步的，在一些可行的实施方式中，接入点可使用第二预存数据中存储的 GPK_{Sig} 和 $SK_{BS_ID_Sig}$ 对所述广播消息进行签名以得到广播消息的签名（表示为 Sig1），并在广播消息中携带接入点具有数据签名功能的指示信息。进一步的，也可在上述广播消息中携带上述 Sig1。

S202，UE 接收接入点的广播消息，并存储广播消息中携带的加密公钥。

在一些可行的实施方式中，UE 接收到接入点发送的广播消息之后，可根据上述广播消息中携带的信息确定接入点是否支持基于加密公钥的数据加密或者数据签名，以及加密公钥的类型。其中，上述加密公钥的类型可包括 IBC 技术的加密公钥，或者 PKI 技术的公钥。本发明实施例将具体支持对 IBC 技术的加密公钥的数据传输进行描述。具体实现中，若接入点发送的广播消息不携带加密公钥，则可确定接入点不支持加密公钥的数据加密，UE 可向该接入点发送数据时无需加密，对此类应用场景，本发明实施例不具体描述。若上述广播消息中携带加密公钥，但是不包含接入点是否具有数据签名功能的指示信息，UE 则可直接存储上述广播消息中携带的加密公钥，以根据上述加密公钥对后续需要向接入点发送的数据进行加密处理。

在一些可行的实施方式中，若 UE 接收到上述接入点发送的广播消息，并且确定上述广播消息中携带指示信息，则可根据上述指示信息确定接入点是否具有数据签名功能。UE 还可验证上述广播消息中携带的时间戳（英文：timestamp）或者序列号（英文：sequence number）是否合法，若上述时间戳或者序列号合法，则可进一步直接存储上述广播消息中携带的信息，包括加密公钥、时间戳和序列号等信息。

进一步的，在一些可行的实施方式中，若 UE 根据广播消息中携带的指示信息确定接入点具有数据签名功能，则可根据上述广播消息中携带的签名验证广播消息的合法性。具体的，UE 可根据广播消息中携带的接入点的标识信息（例如接入点的 ID 等）确定接入点所属的运营商的身份 operator ID2。将上述 operator ID2 与 operator ID1 进行匹配，若上述 operator ID2 与 operator ID1 相同，则可确定上述接入点和 UE 同属一个运营商。进一步的，UE 确定接入点与其同属一个运营商之后，则可根据 operator ID1（此时 operator ID2 与 operator ID1 相同）从其第一预存数据中查找 operator ID1 对应的数据签名全局公钥（设定为第三全局公钥），即接入点对应的第三全局公钥 $GPK_{Sig}1$。进一步的，若上述广播消息中携带签名 Sig1，UE 可则使用上述 $GPK_{Sig}1$ 和接入点的 ID 等信息对广播消息进行验证。当广播消息验证通过时，确定将广播消息携带的加密公钥、时间戳或者序列号等信息添加至

UE 的第一预存数据中，以备后续传输数据处理时使用。若上述广播消息验证不通过，则丢弃该广播消息。UE 需要发送传输数据时，则可根据第一存储数据中存储的目标接入点的信息进行数据处理并发送给目标接入点。

S203，UE 在需要向接入点发送传输数据时，使用从第一预存数据中获取的加密公钥、全局公钥或者 UE 对应的私钥对传输数据进行保护以得到保护消息。

具体实现中，上述全局公钥可包括 GPK_{enc} 或者 GPK_{Sig}，具体可根据 UE 对传输数据的具体处理方式确定。上述 UE 对应的私钥可包括 $SK_{UE_ID_enc}$ 或者 $SK_{UE_ID_Sig}$，具体可根据 UE 对传输数据的具体处理方式确定。下面将结合步骤 S204-S206 对数据传输的实现方式进行具体描述。

S204，UE 向接入点发送保护消息。

具体实现中，上述保护消息中携带传输数据的保护方式的指示消息。其中，上述保护方式可包括加密、或者加密和签名、或者加密使用的密钥，以及签名使用的密钥等信息。下面将结合步骤 S205-S206 对数据传输的实现方式进行具体描述。

S205，接入点根据保护方式的指示消息从第二预存数据中获取全局公钥和接入点对应的私钥，并使用全局公钥和接入点对应的私钥对保护消息进行解析。

S206，接入点将解析得到的传输数据发送到核心网中。

在一些可行的实施方式中，UE 可在需要向目标接入点发送传输数据时，可根据目标接入点的 ID 等标识信息从第一预存数据中获取目标接入点对应的加密公钥和 GPK_{enc}。其中，上述目标接入点可为 UE 的第一预存数据中包含的一个或者多个接入点信息中的某一个接入点。例如，若上述目标接入点为目标 BS（简称 BS），则可根据 BS_ID 从第一预存数据中获取加密公钥，其中，加密公钥可为 BS_ID，或者加密公钥包含 BS_ID。进一步的，UE 还可在其第一预存数据中获取自身的标识信息，例如 UE_ID 等信息。UE 可将需要发送的传输数据和 UE_ID 等信息输入系统函数以获取第一完整性校验码（英文 Message Authentication Code，MAC）（如 MAC0），并使用加密公钥、GPK_{enc} 对传输数据和 MAC0 进行加密以得到保护消息。其中，上述保护消息可携带传输数据的保护方式的指示信息。上述传输数据的保护方式为使用加密公钥和 GPK_{enc} 对传输数据和 MAC0 进行加密。

进一步的，在一些可行的实施方式中，UE 生成完整性校验码时也可将存储在第一预存数据中的时间戳和序列号等信息，连同需要发送的传输数据、UE_ID 等信息输入系统函数，通过系统函数生成 MAC0。将时间戳和序列号等信息添加到生成 MAC0 的数据中，可供接入点更好地验证消息的完整性，增强数据传输的安全性。下面各个应用场景中完整性校验码的生成也可根据实际应用场景需求添加时间戳和序列号到输入系统函数的数据中，增强各个应用场景中数据传输的安全性，下面不再赘述。

具体实现中，UE 对传输数据进行加密得到保护消息之后，则可将上述保护消息发送给接入点。其中，上述保护消息可包含一个指示位，上述指示位用于传输上述指示信息，用于告知接入点上述传输数据的保护方式。

在一些可行的实施方式中，接入点接到上述保护消息之后，可首先根据上述保护消息确定传输数据的保护方式，进而可根据保护方式从第二预存数据中获取相关的数据对传输数据进行解析。其中，若上述传输数据的保护方式为使用加密公钥和 GPK_{enc} 对传输数据和

MAC0进行加密，接入点则可从第二预存数据中获取$SK_{BS_ID_enc}$和GPK_{enc}，并使用$SK_{BS_ID_enc}$和GPK_{enc}对保护消息进行解密以得到解密消息。进一步的，接入点还可从解密消息中获取保护消息携带的 MAC0。接入点解密得到上述解密消息之后，还可将解密消息输入到一个系统函数，获得一个完整性校验码（具体可设定为第二完整性校验码 MAC1）。其中，上述生成 MAC1 的数据中也可包含时间戳和序列号等信息。具体的，若接入点的广播消息中携带时间戳和序列号等信息，UE 生成完整性校验码时可将时间戳和序列号添加到生成完整性校验码的数据中。相对应的，接入点验证 UE 发送的保护消息时，也可将时间戳和序列号等信息添加在生成用于验证保护消息的完整性校验码的数据中，具体可根据实际应用场景确定。下述各个应用场景中完整性校验码的生成也可根据实际应用场景需求确定是否添加时间戳和完整性校验码，在此不再赘述。当 MAC1 与 MAC0 相匹配时，则可获取上述保护消息中携带的传输数据，进而可将上述传输数据发送到核心网。

进一步的，在一些可行的实施方式中，UE 需要向目标接入点（下面简称接入点）发送传输数据时，还可对传输数据进行签名。具体的，UE 可在需要向接入点发送传输数据时，从第一预存数据中获取加密公钥、GPK_{enc}、GPK_{sig} 以及 $SK_{UE_ID_Sig}$。进而可根据 GPK_{sig} 和 $SK_{UE_ID_Sig}$ 对传输数据进行签名以得到签名 Sig2，并使用上述加密公钥、GPK_{enc} 对传输数据、UE 的标识信息和上述 Sig2 进行加密以得到保护消息。其中，上述保护消息可携带传输数据的保护方式的指示信息。上述传输数据的保护方式为使用加密公钥、GPK_{enc} 对传输数据以及上述 Sig2 进行加密。

具体实现中，UE 对传输数据进行加密得到保护消息之后，则可将上述保护消息发送给接入点。其中，上述保护消息可包含一个指示位，上述指示位用于传输上述指示信息，用于告知接入点上述传输数据的保护方式。

在一些可行的实施方式中，接入点接到上述保护消息之后，可首先根据上述保护消息确定传输数据的保护方式，进而可根据保护方式从第二预存数据中获取相关的数据对传输数据进行解析。其中，上述传输数据的保护方式为使用使用加密公钥、GPK_{enc} 对传输数据以及上述 Sig2 进行加密。接入点根据加密方式的指示消息确定传输数据的保护方式为使用使用加密公钥、GPK_{enc} 对传输数据以及上述 Sig2 进行加密之后，可从第二预存数据中获取 GPK_{enc} 和 $SK_{BS_ID_enc}$，并使用 $SK_{BS_ID_enc}$ 和 GPK_{enc} 对保护消息进行解密以获取传输数据。进一步的，接入点还可从保护消息解密得到的解密消息中获取 UE 的标识信息（如 UE_ID）和上述 Sig2。具体实现中，UE 向接入点发送保护消息时，可在上述保护消息中携带 UE_ID 等标识，以供接入点根据 UE_ID 等标识对保护消息中的签名进行验证，以确定是否将传输数据发送到核心网。

具体实现中，接入点根据加密方式的指示消息确定传输数据的保护方式为使用使用加密公钥、GPK_{enc} 对传输数据以及上述 Sig2 进行加密之后，可从第二预存数据中获取上述 GPK_{sig}，并使用 UE_ID 和上述 GPK_{sig} 对上述保护消息中携带的 Sig2 进行验证。若上述当保护消息中的 Sig2 验证成功，接入点则可将传输数据发送到核心网。

在本发明实施例中，UE 向接入点发送上行数据时，可使用接入点的身份等信息作为加密公钥，并使用 IBC 技术的全局公钥对上传传输数据进行加密，可以有效解决 5G 网络中对空口信令及其数据的保护，防止用户隐私、信令内容的泄露。接入点对 UE 发送的消息

进行解密和签名、完整性校验码等验证，过滤非法信令和数据，保护核心网的安全。

参见图 3，图 3 是本发明实施例提供的保护系统在场景一中的一交互示意图。下面将结合图 3，对本发明实施例提供的传输数据的保护系统中各个数据传输端在场景一中数据交互过程进行描述。其中，接入点为 BS。当接入点为 BS 时，加密公钥可为 BS_ID 或者加密公钥中包含 BS_ID。私钥 $SK_{BS_ID_enc}$ 和私钥 $SK_{BS_ID_Sig}$ 具体为 BS 对应的数据加密私钥和数据签名私钥。

在该应用场景中，UE 和接入网（英文：Radio Access Network，RAN）使用 IBE 的技术对从 UE 到 RAN 的上行数据的传输实施了加密，但是 UE 不对消息提供认证信息，因此 RAN 对用户消息无认证能力。其中，上述 RAN 为接入点所属的网络，RAN 可提供上述接入点的功能。在该应用场景中，RAN 侧将以基站为例进行说明，UE 和基站组成的系统执行数据传输包含的具体流程包括步骤：

31、基站获取 IBC 技术的系统参数。

具体实现中，基站可从网络中获取系统参数，其中，上述系统参数可包括加密公钥（如 BS_ID）、全局公钥 GPK，以及基站对应的加密或者签名的密钥 SK_{BS_ID}。当基站同时具有加密和签名的功能时，基站需要从网络中获取的系统参数包括两个全局公钥，分别为 GPK_{enc} 和 GPK_{Sig}，和两个私钥，分别为 $SK_{BS_ID_enc}$，$SK_{BS_ID_Sig}$。

32、基站存储 IBC 技术的系统参数。

其中，上述系统参数包括 BS_ID，GPK_{enc}、GPK_{Sig}，$SK_{BS_ID_enc}$ 和 $SK_{BS_ID_Sig}$ 等。

33、UE 获取 IBC 技术的处理参数。

具体实现中，UE 从网络中获取其所属运营商的 operator ID 和基于 IBC 技术的公钥 GPK。GPK 可以是两个，分别对应于加密和签名，如 GPK_{enc} 和 GPK_{Sig}。

34、基站发送广播消息。

具体实现中，广播消息中包含一个指示位（英文：indicator），该指示位（如 indicator1）可用于标明消息中是否包含 PKI 技术的公钥，或者 IBC 技术的公钥，或者还可用于指明基站的身份（即 BS_ID），或者用于表明基站是否支持 IBE 技术的加密，基站是否具有签名的能力等信息。广播消息中还可能携带时间戳或者一个消息序列号。

进一步的，基站可以使用 GPK_{Sig} 和私钥 $SK_{BS_ID_Sig}$ 对该消息进行签名得到 Sig1。

35、UE 验证消息并存储广播消息中携带的相关数据。

具体实现中，UE 接收到基站发送的广播消息后，首先根据广播消息中包含的 indicator1，确认基站是否支持基于公钥的加密及公钥的类型，其中，公钥的类型包括 PKI 公钥或者 IBC 公钥，本发明实施例将对 IBC 公钥进行描述，对 PKI 公钥不做限制。UE 还可进一步确认消息中的 Timestamp 或者 sequence number 是否合法。UE 还要确定消息中是否携带了签名。如果广播消息中包含一个签名（如上述 Sig1），UE 根据基站所属运营商获得相应的 operator ID（例如上述 operator ID2），并进一步确认 operator ID2 相对应的全局公钥 GPK_{Sig}。UE 使用基站的标识信息（如 BS_ID）和 GPK_{Sig} 验证消息的合法性。如果消息合法，则存储广播消息中包含的加密公钥（如 BS_ID，其中 BS_ID 也为基站的标识信息）、Timestamp 以及 Sequence number 等信息。否则，UE 丢弃该消息。具体实现中，上述签名和广播消息的

验证可参见上述 S201-S206 中各个步骤的相关描述，在此不再赘述。

36、UE 生成完整性校验码，并对传输数据进行加密以得到保护消息。

具体实现中，当 UE 需要向 RAN 发送信令或者无连接的小数据时， UE 首先根据接收方的 ID（如 BS_ID）从第一预存数据中获取 BS_ID 相对应的加密公钥（加密公钥具体可为 BS_ID 或者包含 BS_ID 的密钥）及 BS_ID 相对应的系统参数（如 Timestamp，Sequence number 和 GPK_{enc}）。UE 把用户要加密的消息输入到一个系统函数（具体可为哈希函数（Hash））中获取一个完整性校验码 (如 MAC0)。其中，上述用户要加密的消息可为信令（或者无连接的小数据），进一步的，上述用户要加密的消息也可包括信令（或者无连接的小数据）、Timestamp 和 Sequence number 等。其中，timestamp 或者 Sequence number 可以是 UE 最近接收到的数值。UE 使用 BS 对应的加密公钥（BS_ID）或者全局公钥 GPKenc 对要发送的信令（或者无连接的小数据）及其 MAC0 进行加密操作以得到保护消息。

37、UE 向基站发送由上述第 36 步加密的保护消息。

具体实现中，上述保护消息中包含一个指示位（如 indicator2），标明该保护消息是否被加密，或者该保护消息的保护方式，例如是否使用了 BS_ID 进行了消息的加密等。

38、基站验证 UE 发送的消息。

具体实现中，基站接收到 UE 发送的保护消息后，首先根据保护消息中携带的指示位（如 indicator2）确定保护消息的保护方式。如果保护消息是使用 BS_ID 和 GPK_{enc} 进行了加密，基站则可从其预存数据中获取 BS_ID 及其相对应的私钥 $SK_{BS_ID_enc}$、全局公钥 GPK_{enc}。进而基站可使用获取的参数（$SK_{BS_ID_enc}$ 及其全局公钥 GPK_{enc}）对接收到的保护消息进行解密。如果消息中还包含了完整性校验码（MAC0），基站进一步根据解密得到的消息生成另一个完整性校验码（MAC1），通过 MAC0 和 MAC1 的比对来验证消息的完整性。

39、基站将解密后的消息发送到核心网。

具体实现中，若基站通过 MAC0 和 MAC1 的比对确定了保护消息的完整性，则可将保护消息中携带的传输数据发送到核心网。进一步的，完成消息验证后，基站可更新相关用户的计费信息，并发送到核心网的计费单元。

具体实现中，上述各个步骤的更多详细实现方式可参见上述 S201-S206 中各个步骤的相关描述，在此不再赘述。

参见图 4，图 4 是本发明实施例提供的保护系统在场景一中的另一交互示意图。下面将结合图 4，对本发明实施例提供的传输数据的保护系统中各个数据传输端在场景一中数据交互过程进行描述。其中，接入点为 Wi-Fi AP。当接入点为 Wi-Fi AP 时，加密公钥可为 Wi-Fi AP 的 MAC 地址或者 SSID。私钥 $SK_{BS_ID_enc}$ 和私钥 $SK_{BS_ID_Sig}$ 具体为 Wi-Fi AP 对应的数据加密私钥和数据签名私钥。

在该应用场景中，UE 和 Wi-Fi AP 使用 IBE 的技术对从 UE 到 RAN 的数据实施了加密，但是 UE 不对消息提供认证信息，因此 Wi-Fi AP 对用户消息无认证能力。其中，上述 RAN 为接入点所属的网络，RAN 可提供上述接入点的功能。在该应用场景中，RAN 侧将以 Wi-Fi AP 为例进行说明，UE 和 Wi-Fi AP 组成的系统执行数据传输包含的具体流程包括步骤：

41、Wi-Fi AP 获取 IBC 技术的系统参数。

具体实现中，Wi-Fi AP 可从网络中获取系统参数，其中，上述系统参数可包括加密公钥(如MAC地址或者SSID)、全局公钥GPK，以及基站对应的加密或者签名的密钥SK_{BS_ID}。当 Wi-Fi AP 同时具有加密和签名的功能时，Wi-Fi AP 需要从网络中获取的系统参数包括两个全局公钥，分别为GPK_{enc}和GPK_{Sig}，和两个私钥，分别为$SK_{BS_ID_enc}$，$SK_{BS_ID_Sig}$。

42、Wi-Fi AP 存储 IBC 技术的系统参数。

其中，上述系统参数包括 MAC 地址或者 SSID、GPK_{enc}、GPK_{Sig}，$SK_{BS_ID_enc}$和$SK_{BS_ID_Sig}$等。

43、UE 获取 IBC 技术的处理参数。

具体实现中，UE从网络中获取其所属运营商的operator ID和基于IBC技术的公钥GPK。GPK 可以是两个，分别对应于加密和签名，如GPK_{enc}和GPK_{Sig}。

44、Wi-Fi AP 发送广播消息或者单播消息。

具体实现中，上述广播消息可为 Beacon，单播消息可为 Probe response，下面将以广播消息为例进行说明。广播消息中包含一个指示位(英文: indicator)，该指示位(如 indicator1)可用于标明消息中是否包含 PKI 技术的公钥，或者 IBC 技术的公钥，或者还可用于指明 Wi-Fi AP 的身份（即 MAC 地址或者 SSID），或者用于表明 Wi-Fi AP 是否支持 IBE 技术的加密，Wi-Fi AP 是否具有签名的能力等信息。广播消息中还可能携带时间戳或者消息序列号。

进一步的，Wi-Fi AP 可以使用 MAC 地址或者 SSID 和私钥$SK_{BS_ID_Sig}$对该消息进行签名得到 Sig1。

45、UE 验证消息并存储广播消息或者单播消息中携带的相关数据。

具体实现中，UE 接收到 Wi-Fi AP 发送的广播消息后，首先根据广播消息中包含的 indicator1，确认 Wi-Fi AP 是否支持基于公钥的加密及公钥的类型，其中，公钥的类型包括 PKI 公钥或者 IBC 公钥，本发明实施例将对 IBC 公钥进行描述，对 PKI 公钥不做限制。UE 还可进一步确认消息中的 Timestamp 或者 sequence number 是否合法。UE 还要确定消息中是否携带了签名。如果广播消息中包含一个签名（如上述 Sig1），UE 根据 Wi-Fi AP 的 MAC 地址或者 SSID 进一步确认 MAC 地址或者 SSID 相对应的全局公钥GPK_{Sig}。UE 使用 Wi-Fi AP 的标识信息（如 MAC 地址或者 SSID）和GPK_{Sig}验证消息的合法性。如果消息合法，则存储广播消息中包含的加密公钥（如 MAC 地址或者 SSID，其中，MAC 地址或者 SSID 也为 Wi-Fi AP 的标识信息）、Timestamp 以及 Sequence number 等信息。否则，UE 丢弃该消息。具体实现中，上述签名和广播消息的验证可参见上述 S201-S206 中各个步骤的相关描述，在此不再赘述。

46、UE 生成完整性校验码，并对传输数据进行加密以得到保护消息。

具体实现中，当 UE 需要向 RAN 发送信令或者无连接的小数据时，UE 首先根据接收方的 ID（如 MAC 地址或者 SSID）从第一预存数据中获取 MAC 地址或者 SSID 相对应的加密公钥(加密公钥具体可为MAC地址或者SSID或者包含MAC地址或者SSID的密钥)，以及MAC地址或者SSID相对应的系统参数(如Timestamp，Sequence number 和GPK_{enc})。UE 把用户要加密的消息输入到一个系统函数（具体可为哈希函数（Hash））中获取一个完整性校验码 (如 MAC0)。其中，上述用户要加密的消息可为信令(或者无连接的小数据)，

进一步的，上述用户要加密的消息也可包括信令（或者无连接的小数据）、Timestamp 和 Sequence number 等。其中，timestamp 或者 Sequence number 可以是 UE 最近接收到的数值。UE 使用 Wi-Fi AP 对应的加密公钥（如 MAC 地址或者 SSID）或者全局公钥 GPK_{enc} 对要发送的信令（或者无连接的小数据）及其 MAC0 进行加密操作以得到保护消息。

47、UE 向 Wi-Fi AP 发送由上述第 46 步加密的保护消息。该保护消息中包含一个指示位（如 indicator2），标明该保护消息是否被加密，或者该保护消息的保护方式，例如是否使用了 Wi-Fi AP 的 MAC 地址或者 SSID 进行了消息的加密等。

48、Wi-Fi AP 进行消息验证。

具体实现中，Wi-Fi AP 接受到 UE 发送的保护消息后，首先根据保护消息中携带的指示位（如 indicator2）确定保护消息的保护方式。如果保护消息是使用 MAC 地址或者 SSID 和 GPK_{enc} 进行了加密，Wi-Fi AP 则可从其预存数据中获取 MAC 地址或者 SSID 及其相对应的私钥 $SK_{BS_ID_enc}$ 和全局公钥 GPK_{enc}。进而 Wi-Fi AP 可使用获取的参数（$SK_{BS_ID_enc}$ 及其全局公钥 GPK_{enc}）对接收到的保护消息进行解密。如果消息中还包含了完整性校验码（MAC0），Wi-Fi AP 进一步根据解密得到的消息生成另一个完整性校验码（MAC1），通过 MAC0 和 MAC1 的比对来验证消息的完整性。

49、Wi-Fi AP 将解密后的消息发送到核心网。

具体实现中，若 Wi-Fi AP 通过 MAC0 和 MAC1 的比对确定了保护消息的完整性，则可将保护消息中携带的传输数据发送到核心网。具体实现中，上述各个步骤的更多详细实现方式可参见上述 S201-S206 中各个步骤的相关描述，在此不再赘述。

进一步的，在一些可行的实施方式中，UE 需要向接入点发送传输数据时，还可根据加密公钥、全局公钥以及 UE 对应的数据加密私钥等数据生成对称钥，进而可使用对称钥对传输数据进行保护。具体的，UE 可在需要向接入点发送传输数据时，从第一预存数据中获取加密公钥、GPK_{enc} 以及 $SK_{UE_ID_enc}$。进一步的，UE 可根据上述加密公钥、GPK_{enc} 以及 $SK_{UE_ID_enc}$ 生成对称钥（设定为第一对称钥 K1），并将上述传输数据和上述 K1 输入系统函数以获取一个完整性校验码（设定为第三完整性校验码 MAC2）。需要说明的是，本发明实施例中所描述的系统函数具体可为哈希函数，也可为其他可实现完整性校验码的生成的系统函数，具体可根据实际应用场景确定，在此不再做限制。

具体实现中，UE 根据加密公钥、GPK_{enc} 以及 $SK_{UE_ID_enc}$ 生成 K1 之后，可使用上述加密公钥和上述 GPK_{enc} 对传输数据、UE_ID 等 UE 标识信息以及上述生成的 MAC2 进行加密以得到保护消息。进一步的，UE 可在上述保护消息中携带上述传输数据的保护方式的指示信息，上述指示信息用于指示传输数据的保护方式为使用加密公钥和 GPK_{enc} 对传输数据、UE_ID 以及 MAC2 进行加密。

具体实现中，UE 对传输数据进行加密得到保护消息之后，则可将上述保护消息发送给接入点。其中，上述保护消息可包含一个指示位，上述指示位用于传输上述指示信息，用于告知接入点上述传输数据的保护方式。

在一些可行的实施方式中，接入点接到上述保护消息之后，可首先根据上述保护消息确定传输数据的保护方式，进而可根据保护方式从第二预存数据中获取相关的数据对传输

数据进行解析。其中，上述传输数据的保护方式为使用加密公钥和 GPK_{enc} 对传输数据、UE_ID 以及 MAC2 进行加密。接入点可根据上述保护方式的指示消息确定传输数据的保护方式为使用加密公钥和 GPK_{enc} 对传输数据、UE_ID 以及 MAC2 进行加密，进而可从上述第二预存数据中获取 GPK_{enc} 和 $SK_{BS_ID_enc}$，并使用上述 $SK_{BS_ID_enc}$ 和 GPK_{enc} 对保护消息进行解密以得到解密消息。进一步的，接入点还可从上述解密消息中获取保护消息携带的 MAC2、UE_ID 以及传输数据，并使用上述加密公钥、UE_ID、GPK_{enc} 和 $SK_{BS_ID_enc}$ 生成对称钥 K2。接入点生成上述 K2 之后，则可使用上述 K2、UE_ID 和解密得到的传输数据计算一个完整性校验码（设定为第四完整性校验码 MAC3）。若上述 MAC3 与保护消息中携带的上述 MAC2 相匹配，接入点则可将上述保护消息中携带的 UE 发送的传输数据发送到核心网中。

需要说明的是，在本发明实施例中，同一个应用场景中，UE 进行数据加密使用的加密公钥与接入点进行数据解密或者验证使用的加密公钥相同，进而可实现加密数据在接收方的正确解密。加密公钥通过广播消息等方式从传输数据接收方（即接入点）传递给传输数据发送方（即 UE），传输数据发送方使用传输数据接收方提供的公钥进行数据保护，进而可避免在数据传输中携带数据加密密钥等信息造成信息泄露，增强了网络的安全性。

参见图 5，图 5 是本发明实施例提供的保护系统在场景二中的一交互示意图。下面将结合图 5，对本发明实施例提供的传输数据的保护系统中各个数据传输端在场景二中数据交互过程进行描述。其中，接入点为 BS。当接入点为 BS 时，加密公钥可为 BS_ID 或者加密公钥中包含 BS_ID。私钥 $SK_{BS_ID_enc}$ 和私钥 $SK_{BS_ID_Sig}$ 具体为 BS 对应的数据加密私钥和数据签名私钥。

在该应用场景中，与上述图 3 所示的应用场景提供的实现方式不同的是，UE 和 RAN 使用 IBE 的技术对从 UE 到 RAN 的上行数据的传输实施了加密，并且 UE 对消息提供认证信息，因此 RAN 对用户消息有认证能力。其中，上述 RAN 为接入点所属的网络，RAN 可提供上述接入点的功能。在该应用场景中，RAN 侧将以基站为例进行说明，UE 和基站组成的系统执行数据传输包含的具体流程包括步骤:

51、基站获取 IBC 技术的系统参数。

具体实现中，基站可从网络中获取系统参数，其中，上述系统参数可包括加密公钥（如 BS_ID）、全局公钥 GPK，以及基站对应的加密或者签名的密钥 SK_{BS_ID}。当基站同时具有加密和签名的功能时，基站需要从网络中获取的系统参数包括两个全局公钥，分别为 GPK_{enc} 和 GPK_{Sig}，和两个私钥，分别为 $SK_{BS_ID_enc}$，$SK_{BS_ID_Sig}$。

52、基站存储 IBC 技术的系统参数。

其中，上述系统参数包括 BS_ID，GPK_{enc}、GPK_{Sig}，$SK_{BS_ID_enc}$ 和 $SK_{BS_ID_Sig}$ 等。

53、UE 获取 IBC 技术的处理参数。

具体实现中，UE 从网络中获取其所属运营商的 operator ID1 和基于 IBC 技术的公钥 GPK 以及私钥。GPK 可以是两个，分别对应于加密和签名，如 GPK_{enc} 和 GPK_{Sig}。私钥也可以是两个，分别对应于加密和签名，如 $SK_{UE_ID_enc}$ 和 $SK_{UE_ID_sig}$。

54、基站发送广播消息。

具体实现中，广播消息中包含一个指示位，该指示位（如 indicator1）可用于标明消息中是否包含 PKI 技术的公钥，或者 IBC 技术的公钥，或者还可用于指明基站的身份（即 BS_ID），或者用于表明基站是否支持 IBE 技术的加密，基站是否具有签名的能力等信息。广播消息中还可能携带时间戳或者一个消息序列号。

进一步的，基站可以使用 BS_ID 和私钥 $SK_{BS_ID_Sig}$ 对该消息进行签名得到 Sig1。

55、UE 验证消息并存储广播消息中携带的相关数据。

UE 接收到基站发送的广播消息后，首先根据广播消息中包含的 indicator1，确认基站是否支持基于公钥的加密及公钥的类型，其中，公钥的类型包括 PKI 公钥或者 IBC 公钥，本发明实施例将对 IBC 公钥进行描述，对 PKI 公钥不做限制。UE 还可进一步确认消息中的 Timestamp 或者 sequence number 是否合法。 UE 还要确定消息中是否携带了签名。如果广播消息中包含一个签名（如上述 Sig1），UE 根据基站所属运营商获得相应的 operator ID（例如上述 operator ID2），并进一步确认 operator ID2 相对应的全局公钥 GPK_{Sig}。UE 使用基站的标识信息（如 BS_ID）和 GPK_{Sig} 验证消息的合法性。如果消息合法，则存储广播消息中包含的加密公钥（如 BS_ID，其中 BS_ID 也为基站的标识信息）、Timestamp 以及 Sequence number 等信息。否则，UE 丢弃该消息。具体实现中，上述签名和广播消息的验证可参见上述 S201-S206 中各个步骤的相关描述，在此不再赘述。

56、UE 生成认证码，并使用加密公钥和全局公钥对传输数据进行加密以得到保护消息。

具体实现中，当 UE 需要向 RAN 发送信令或者无连接的小数据时， UE 首先根据接收方的 ID（如 BS_ID）从第一预存数据中获取 BS_ID 相对应的加密公钥（加密公钥具体可为 BS_ID 或者包含 BS_ID 的密钥）及 BS_ID 相对应的系统参数（如 Timestamp，Sequence number 和 GPK_{enc}）。进一步的，UE 可为需要发送的消息生成一个认证码。其中，生成认证码的方式可包括两种:

其一，UE 使用私钥 SK_{UE_ID}、以及全局公钥 GPK_{enc}，以及加密公钥（即 BS_ID）等数据生成一个对称钥（设定为 K1）。UE 把用户要加密的消息（即传输数据，例如信令或者无连接的小数据，进一步的还可包括一个时间戳或者序列号，时间戳或者序列号可以是 UE 最近接收到的数值，以及使用上述方法生成的 K1）输入到一个系统函数中获取一个具有认证能力的完整性校验码 (设定为 MAC2)。

其二，UE 直接使用 GPK_{sig} 和 $SK_{UE_ID_sig}$ 对要发送的消息（即传输数据，例如信令或者无连接的小数据，进一步的还可包括一个时间戳或者序列号等）进行签名得到签名 Sig2。

UE 使用 BS 对应的加密公钥（BS_ID）和全局公钥 GPK_{enc} 对要发送的信令（或者无连接的小数据）及其 MAC2 进行加密操作以得到保护消息。进一步的，UE 也可 UE 使用 BS 对应的加密公钥（BS_ID）和全局公钥 GPK_{enc} 对要发送的信令（或者无连接的小数据）及其 Sig2 进行加密操作以得到保护消息。

57、UE 向基站发送由上述第 56 步加密的保护消息。

该保护消息中包含一个指示位（如 indicator2），标明该保护消息是否被加密，或者该保护消息的保护方式，例如是否使用了 BS_ID 进行了消息的加密等。

58、基站对保护消息进行验证。

具体实现中，基站接收到 UE 发送的保护消息后，首先根据保护消息中携带的指示位

（如 indicator2）确定保护消息的保护方式。如果保护消息是使用 BS_ID 和 GPK_{enc} 进行了加密，基站则可从其预存数据中获取 BS_ID 及其相对应的私钥 $SK_{BS_ID_enc}$、全局公钥 GPK_{enc}。进而基站可使用获取的参数（$SK_{BS_ID_enc}$ 及其全局公钥 GPK_{enc}）对接收到的保护消息进行解密。

如果消息中还包含了认证码（完整性校验码或者签名），基站则需进一步验证消息的完整性。如果消息使用了对称钥 K1 进行了完整性保护，则基站使用私钥 $SK_{BS_ID_enc}$、全局公钥 GPK_{enc}，以及 UE_ID 生成对称密钥 K2，然后使用 K2 和 UE_ID 以及对保护消息进行解密得到的传输数据计算一个完整性校验码 MAC3。通过 MAC3 和 MAC2 的比对来进行保护消息的验证。如果 UE 对该保护消息进行了签名，基站则使用消息中携带的 UE_ID，结合全局公钥 GPK_{sig}（进一步的，还可包括其他参数如时间戳或者序列号等）对保护消息进行认证。

59、基站将解密后的消息发送到核心网。

具体实现中，若基站通过 MAC3 和 MAC2 的比对或者 Sig2 的验证确定了保护消息的完整性，则可将保护消息中携带的传输数据发送到核心网。具体实现中，上述各个步骤的更多详细实现方式可参见上述 S201-S206 中各个步骤的相关描述，在此不再赘述。

参见图 6，图 6 是本发明实施例提供的保护系统在场景二中的另一交互示意图。下面将结合图 6，对本发明实施例提供的传输数据的保护系统中各个数据传输端在场景二中数据交互过程进行描述。其中，接入点为 Wi-Fi AP。当接入点为 Wi-Fi AP 时，加密公钥可为 Wi-Fi AP 的 MAC 地址或者 SSID。私钥 $SK_{BS_ID_enc}$ 和私钥 $SK_{BS_ID_Sig}$ 具体为 Wi-Fi AP 对应的数据加密私钥和数据签名私钥。

在该应用场景中，与上述图 3 所示的应用场景提供的实现方式不同的是，UE 和 RAN 使用 IBE 的技术对从 UE 到 RAN 的上行数据的传输实施了加密，并且 UE 对消息提供认证信息，因此 RAN 对用户消息有认证能力。其中，上述 RAN 为接入点所属的网络，RAN 可提供上述接入点的功能。在该应用场景中，RAN 侧将以 Wi-Fi AP 为例进行说明，UE 和 Wi-Fi AP 组成的系统执行数据传输包含的具体流程包括步骤：

61、Wi-Fi AP 获取 IBC 技术的系统参数。

具体实现中，Wi-Fi AP 可从网络中获取系统参数，其中，上述系统参数可包括加密公钥（如 MAC 地址或者 SSID）、全局公钥 GPK，以及 Wi-Fi AP 对应的加密或者签名的密钥 SK_{BS_ID}。当 Wi-Fi AP 同时具有加密和签名的功能时，Wi-Fi AP 需要从网络中获取的系统参数包括两个全局公钥，分别为 GPK_{enc} 和 GPK_{Sig}，和两个私钥，分别为 $SK_{BS_ID_enc}$，$SK_{BS_ID_Sig}$。

62、Wi-Fi AP 存储 IBC 技术的系统参数。

其中，上述系统参数包括 MAC 地址或者 SSID，GPK_{enc}、GPK_{Sig}，$SK_{BS_ID_enc}$ 和 $SK_{BS_ID_Sig}$ 等。

63、UE 获取 IBC 技术的处理参数。

具体实现中，UE 从网络中获取其 MAC 地址和基于 IBC 技术的公钥 GPK 以及私钥。GPK 可以是两个，分别对应于加密和签名，如 GPK_{enc} 和 GPK_{Sig}。私钥也可以是两个，分

别对应于加密和签名，如 SK_{MAC_enc} 和 SK_{MAC_sig}。

64、Wi-Fi AP 发送广播消息或者单播消息。

具体实现中，上述广播消息可为 Beacon，单播消息可为 Probe response，下面将以广播消息为例进行说明。广播消息中包含一个指示位(英文: indicator)，该指示位(如 indicator1)可用于标明消息中是否包含 PKI 技术的公钥，或者 IBC 技术的公钥，或者还可用于指明 Wi-Fi AP 的身份（即 MAC 地址或者 SSID），或者用于表明 Wi-Fi AP 是否支持 IBE 技术的加密，Wi-Fi AP 是否具有签名的能力等信息。广播消息中还可能携带时间戳或者消息序列号。

进一步的，Wi-Fi AP 可以使用 MAC 地址或者 SSID 和私钥 $SK_{BS_ID_Sig}$ 对该消息进行签名得到 Sig1。

65、UE 验证消息并存储广播消息中携带的相关数据。

具体实现中，UE 接收到 Wi-Fi AP 发送的广播消息后，首先根据广播消息中包含的 indicator1，确认 Wi-Fi AP 是否支持基于公钥的加密及公钥的类型，其中，公钥的类型包括 PKI 公钥或者 IBC 公钥，本发明实施例将对 IBC 公钥进行描述，对 PKI 公钥不做限制。UE 还可进一步确认消息中的 Timestamp 或者 sequence number 是否合法。UE 还要确定消息中是否携带了签名。如果广播消息中包含一个签名（如上述 Sig1），UE 根据 Wi-Fi AP 的 MAC 地址或者 SSID 进一步确认 MAC 地址或者 SSID 相对应的全局公钥 GPK_{Sig}。UE 使用 Wi-Fi AP 的标识信息（如 MAC 地址或者 SSID）和 GPK_{Sig} 验证消息的合法性。如果消息合法，则存储广播消息中包含的加密公钥(如 MAC 地址或者 SSID，其中 MAC 地址或者 SSID 也为基站的标识信息)、Timestamp 以及 Sequence number 等信息。否则，UE 丢弃该消息。具体实现中，上述签名和广播消息的验证可参见上述 S201-S206 中各个步骤的相关描述，在此不再赘述。

66、UE 生成认证码，并使用加密公钥和全局公钥对传输数据进行加密以得到保护消息。

具体实现中，当 UE 需要向 RAN 发送信令或者无连接的小数据时，UE 首先根据接收方的 ID（如 MAC 地址或者 SSID）从第一预存数据中获取 MAC 地址或者 SSID 相对应的加密公钥(加密公钥具体可为 MAC 地址或者 SSID，或者包含 MAC 地址或者 SSID 的密钥）及 MAC 地址或者 SSID 相对应的系统参数(如 Timestamp，Sequence number 和 GPK_{enc})。进一步的，UE 可为需要发送的消息生成一个认证码。其中，生成认证码的方式可包括两种:

其一，UE 使用私钥 SK_{MAC_enc}、以及全局公钥 GPK_{enc}，以及自己的 MAC 地址或者 SSID 等数据生成一个对称钥（设定为 K1）。UE 把用户要加密的消息（即传输数据，例如信令或者无连接的小数据，进一步的还可包括一个时间戳或者序列号，时间戳或者序列号可以是 UE 最近接收到的数值，以及使用上述方法生成的 K1）输入到一个系统函数中获取一个具有认证能力的完整性校验码 (设定为 MAC2)。

其二，UE 直接使用 GPK_{sig} 和 SK_{MAC_sig} 对要发送的消息（即传输数据，例如信令或者无连接的小数据，进一步的还可包括一个时间戳或者序列号等）进行签名得到签名 Sig2。

UE 使用 WiFi AP 对应的加密公钥（MAC 地址或者 SSID）和全局公钥 GPKenc 对要发送的信令（或者无连接的小数据）及其 MAC2 进行加密操作以得到保护消息。进一步的，UE 也可 UE 使用 WiFi AP 对应的加密公钥（MAC 地址或者 SSID）和全局公钥 GPK_{enc} 对

要发送的信令（或者无连接的小数据）及其 Sig2 进行加密操作以得到保护消息。

67、UE 向 Wi-Fi AP 发送由上述第 56 步加密的保护消息。

该保护消息中包含一个指示位（如 indicator2），标明该保护消息是否被加密，或者该保护消息的保护方式，例如是否使用了 WiFi AP 的 MAC 地址或者 SSID 进行了消息的加密等。

68、Wi-Fi AP 进行消息验证。

具体实现中，Wi-Fi AP 接收到 UE 发送的保护消息后，首先根据保护消息中携带的指示位（如 indicator2）确定保护消息的保护方式。如果保护消息是使用 WiFi AP 的 MAC 地址或者 SSID、和 GPK_{enc} 进行了加密，Wi-Fi AP 则可从其预存数据中获取 WiFi AP 的 MAC 地址或者 SSID 及其相对应的私钥 $SK_{BS_ID_enc}$、全局公钥 GPK_{enc}。进而基站可使用获取的参数（$SK_{BS_ID_enc}$ 及其全局公钥 GPKenc）对接收到的保护消息进行解密。

如果消息中还包含了认证码（完整性校验码或者签名），Wi-Fi AP 则需进一步验证消息的完整性。如果消息使用了对称钥 K1 进行了完整性保护，则 Wi-Fi AP 使用加密公钥（如 WiFi AP 的 MAC 地址或者 SSID）、私钥 $SK_{BS_ID_enc}$、全局公钥 GPK_{enc}，以及 UE_ID 生成对称密钥 K2，然后使用 K2 和 UE_ID 以及对保护消息进行解密得到的传输数据计算一个完整性校验码 MAC3。通过 MAC3 和 MAC2 的比对来进行保护消息的验证。如果 UE 对该保护消息进行了签名，Wi-Fi AP 则使用消息中携带的 UE_ID，结合全局公钥 GPK_{sig}（进一步的，还可包括其他参数如时间戳或者序列号等）对保护消息进行认证。

69、Wi-Fi AP 将解密后的消息发送到核心网。

具体实现中，若 Wi-Fi AP 通过 MAC3 和 MAC2 的比对或者 Sig2 的验证确定了保护消息的完整性，则可将保护消息中携带的传输数据发送到核心网。具体实现中，上述各个步骤的更多详细实现方式可参见上述 S201-S206 中各个步骤的相关描述，在此不再赘述。

参见图 7，图 7 是本发明实施例提供的保护系统在场景三中的交互示意图。下面将结合图 7，对本发明实施例提供的传输数据的保护系统中各个数据传输端在场景三中数据交互过程进行描述。其中，接入点为 BS。当接入点为 BS 时，加密公钥可为 BS_ID 或者加密公钥中包含 BS_ID。私钥 $SK_{BS_ID_enc}$ 和私钥 $SK_{BS_ID_Sig}$ 具体为 BS 对应的数据加密私钥和数据签名私钥。

在该应用场景中，与上述图 3 所示的应用场景提供的实现方式不同的是，UE 和 RAN 使用 IBE 的技术对从 UE 到 RAN 的上行数据的传输实施了加密，并且 UE 对消息提供认证信息，因此 RAN 对用户消息有认证能力。其中，上述 RAN 为接入点所属的网络，RAN 可提供上述接入点的功能。在该应用场景中，UE 和 RAN 组成的系统还可和核心网中的网元进行数据交互，其中，核心网中的网元包括：用户面网关（英文：User Plane Gateway，UP-GW）、KMS 和控制面认证单元（英文：Control Plane Authentication Unit ，CP-AU）等。下面 RAN 侧将以基站为例进行说明，UE 和基站组成的系统执行数据传输包含的具体流程包括步骤：

71、基站获取 IBC 技术的系统参数。

具体实现中，基站可从 KMS 中获取系统参数，其中，上述系统参数可包括加密公钥（如 BS_ID）、全局公钥 GPK，以及基站对应的加密或者签名的密钥 SK_{BS_ID}。当基站同时具有

加密和签名的功能时，基站需要从网络中获取的系统参数包括两个全局公钥，分别为 GPK_{enc} 和 GPK_{Sig}，两个私钥，分别为 $SK_{BS_ID_enc}$，$SK_{BS_ID_Sig}$。

72、基站存储 IBC 技术的系统参数。

其中，上述系统参数包括 BS_ID，GPK_{enc}、GPK_{Sig}，$SK_{BS_ID_enc}$ 和 $SK_{BS_ID_Sig}$ 等。

73、UP-GW 从 KMS 获取 IBC 技术的系统参数。

其中，上述 UP-GW 从 KMS 获取的系统参数包括 GPK_{enc} 和 GPK_{Sig}，分别用于加密和签名。

74、UE 与核心网进行交互认证。

其中，UE 与核心网进行交互认证时可核心网中的认证单元可为 3GPP TR 23.799 中定义的 CP-AU，具体认证方式可参见 3GPP TR 23.799 中描述的实现方式，在此不再赘述。

75、UE 通知核心网的 KMS 与核心网认证成功。

76、UE 获取 IBC 技术的处理参数。

具体实现中，UE 从 KMS 获取其所属运营商的 operator ID 和基于 IBC 技术的公钥 GPK 以及私钥。GPK 可以是两个，分别对应于加密和签名，如 GPK_{enc} 和 GPK_{Sig}。私钥也可以是两个，分别对应于加密和签名，如 $SK_{UE_ID_enc}$ 和 $SK_{UE_ID_sig}$。

77、基站发送广播消息。

具体实现中，广播消息中包含一个指示位，该指示位（如 indicator1）可用于标明消息中是否包含 PKI 技术的公钥，或者 IBC 技术的公钥，或者还可用于指明基站的身份（即 BS_ID），或者用于表明基站是否支持 IBE 技术的加密，基站是否具有签名的能力等信息。广播消息中还可能携带时间戳或者一个消息序列号。

进一步的，基站可以使用 BS_ID 和私钥 $SK_{BS_ID_Sig}$ 对该消息进行签名得到 Sig1。

78、UE 验证消息并存储广播消息中携带的相关数据。

具体实现中，UE 接收到基站发送的广播消息后，首先根据广播消息中包含的 indicator1，确认基站是否支持基于公钥的加密及公钥的类型，其中，公钥的类型包括 PKI 公钥或者 IBC 公钥，本发明实施例将对 IBC 公钥进行描述，对 PKI 公钥不做限制。UE 还可进一步确认消息中的 Timestamp 或者 sequence number 是否合法。UE 还要确定消息中是否携带了签名。如果广播消息中包含一个签名（如上述 Sig1），UE 根据基站所属运营商获得相应的 operator ID（例如上述 operator ID2），并进一步确认 operator ID2 相对应的全局公钥 GPK_{Sig}。UE 使用基站的标识信息（如 BS_ID）和 GPK_{Sig} 验证消息的合法性。如果消息合法，则存储广播消息中包含的加密公钥（如 BS_ID，其中 BS_ID 也为基站的标识信息）、Timestamp 以及 Sequence number 等信息。否则，UE 丢弃该消息。具体实现中，上述签名和广播消息的验证可参见上述 S201-S206 中各个步骤的相关描述，在此不再赘述。

79、UE 生成认证码，并使用加密公钥和全局公钥对传输数据进行加密以得到保护消息。

具体实现中，当 UE 需要向 RAN 发送信令或者无连接的小数据时，UE 首先根据接收方的 ID（如 BS_ID）从第一预存数据中获取 BS_ID 相对应的加密公钥（加密公钥具体可为 BS_ID 或者包含 BS_ID 的密钥）及 BS_ID 相对应的系统参数（如 Timestamp，Sequence number 和 GPK_{enc}）。进一步的，UE 可为需要发送的消息生成一个认证码。其中，生成认证码的方式可包括两种：

其一，UE 使用私钥 SK_{UE_ID}、以及全局公钥 GPK_{enc}，以及加密公钥（即 BS_ID）等数据生成一个对称钥（设定为 K1）。UE 把用户要加密的消息（即传输数据，例如信令或者无连接的小数据，进一步的还可包括一个时间戳或者序列号，时间戳或者序列号可以是 UE 最近接收到的数值，以及使用上述方法生成的 K1）输入到一个系统函数中获取一个具有认证能力的完整性校验码 (设定为 MAC2)。

其二，UE 直接使用 GPK_{sig} 和 $SK_{UE_ID_sig}$ 对要发送的消息（即传输数据，例如信令或者无连接的小数据，进一步的还可包括一个时间戳或者序列号等）进行签名得到签名 Sig2。

UE 使用 BS 对应的加密公钥（BS_ID）和全局公钥 GPK_{enc} 对要发送的信令（或者无连接的小数据）及其 MAC2 进行加密操作以得到保护消息。进一步的，UE 也可 UE 使用 BS 对应的加密公钥（BS_ID）和全局公钥 GPK_{enc} 对要发送的信令（或者无连接的小数据）及其 Sig2 进行加密操作以得到保护消息。

710、UE 向基站发送由上述第 79 步加密的保护消息。

具体实现中，上述保护消息中包含一个指示位（如 indicator2），标明该保护消息是否被加密，或者该保护消息的保护方式，例如是否使用了 BS_ID 进行了消息的加密，以及是否使用了 UE_ID 进行了消息的签名等。

711、基站验证 UE 发送的消息。

具体实现中，基站接收到 UE 发送的保护消息后，首先根据保护消息中携带的指示位（如 indicator2）确定保护消息的保护方式。如果保护消息是使用 BS_ID 和 GPK_{enc} 进行了加密，基站则可从其预存数据中获取 BS_ID 及其相对应的私钥 $SK_{BS_ID_enc}$、全局公钥 GPK_{enc}。进而基站可使用获取的参数（$SK_{BS_ID_enc}$ 及其全局公钥 GPK_{enc}）对接收到的保护消息进行解密。

如果消息中还包含了认证码（完整性校验码或者签名），基站则需进一步验证消息的完整性。如果消息使用了对称钥 K1 进行了完整性保护，则基站使用加密公钥（如 BS_ID）、私钥 $SK_{BS_ID_enc}$、全局公钥 GPK_{enc}，以及 UE_ID 生成对称密钥 K2，然后使用 K2 和 UE_ID 以及对保护消息进行解密得到的传输数据计算一个完整性校验码 MAC3。通过 MAC3 和 MAC2 的比对来进行保护消息的验证。如果 UE 对该保护消息进行了签名，基站则使用消息中携带的 UE_ID，结合全局公钥 GPK_{sig}（进一步的，还可包括其他参数如时间戳或者序列号等）对保护消息进行认证。

712、基站将解密后的消息发送到核心网。

具体实现中，基站对保护消息认证通过之后，可将解密后的消息发送给核心网的 UP-GW。其中，发送给 UP-GW 的消息中包含 UE_ID 和 UE 使用 $SK_{UE_ID_sig}$ 对消息产生的签名等信息。

713、UP-GW 验证消息。

具体实现中，UP-GW 接收到消息之后，可使用 GPK_{sig} 和 UE_ID 对消息中携带的签名进行验证。具体验证方式可参见上述各个应用场景中描述的签名的验证方式，在此不再赘述。验证通过后，则进一步转发给其它路由器或者服务器。

具体实现中，上述各个步骤的更多详细实现方式可参见上述 S201-S206 中各个步骤的相关描述，在此不再赘述。

参见图 8，图 8 是本发明实施例提供的保护系统在场景四中的交互示意图。下面将结合图 8，对本发明实施例提供的传输数据的保护系统中各个数据传输端在场景四中数据交互过程进行描述。其中，接入点为 BS。

在该应用场景中，数据的加密和解密是基于 PKI，密钥为基于 PKI 的公钥和私钥。UE 和 RAN 可使用 PKI 技术，结合上述使用 IBC 技术的相同原理的实现方式实现传输数据的保护。在该用于场景中，UE 和 RAN 使用 PKI 的技术对从 UE 到 RAN 的数据实施了加密，但是 UE 不对消息提供认证信息，因此 RAN 对用户消息无认证能力。 具体流程包括如下步骤:

81、基站获取基于 PKI 技术的系统参数。

具体实现中，上述系统参数包括基站的身份（如 BS_ID），基站用于加密的公钥 PK1 及其证书和解密的公钥 PK2 及其证书，用于加密的私钥 SK1 和用于解密的私钥 SK2 等。

82、基站存储基于 PKI 技术的系统参数。

具体实现中，上述系统参数包括 BS_ID，PK1、PK2、SK1 和 SK2 等。

83、UE 从网络获取运营商的 operator ID 和基于 PKI 技术的 PK1 和 PK2 等。

84、基站发送广播消息。

具体实现中，广播消息中包含一个指示位（如 indicator3），该指示位标明消息中是否包含基于 PKI 的公钥 PK（包括 PK1 和 PK2）及其证书。

85、UE 使用 PKI 密钥验证广播消息。

具体实现中，UE 接收到基站发送的广播消息后，首先根据广播消息中包含的 indicator3，确认基站是否支持基于 PKI 公钥的加密。UE 进一步确认消息中的 Timestamp 或者 sequence number 是否合法。UE 还要确定消息中是否携带了签名。如果广播消息中还包含一个签名，UE 使用 PK2 验证消息的合法性。如果消息合法，则存储 BS_ID，PK1 和 PK2，进一步的，还可存储 Timestamp，或者 Sequence number 等。否则，如果消息不合法，UE 丢弃该消息。

86、UE 进行传输数据的保护。

具体实现中，当 UE 需要向网络侧发送传输数据（包括信令或者是无连接的小数据）时， UE 首先根据基站的 BS_ID 获取相应的加密公钥 PK1，及其 Timestamp 和 Sequence number 等数据，并将获取的上述数据输入到一个系统函数中获取一个完整性校验码(设为 MAC8)。UE 使用 BS_ID 和 PK1 对要发送的消息及其 MAC8 进行加密操作。

87、UE 向基站发送由上述第 86 步加密的消息。

具体实现中，上述消息中包含一个指示位（如 indicator4），标明该消息是否被加密，或者是否使用了基站的基于 PKI 的公钥进行了加密。

88、基站验证消息。

具体实现中，基站接收到 UE 发送的消息后，首先根据消息中携带的指示位确定消息的加密方式。如果消息是使用 PKI 公钥 PK1 进行了加密，基站获取基站相对应的私钥 SK1 并使用获取的 SK1 等参数对接收到消息进行解密。如果消息中还包含了完整性保护码，基站进一步根据 SK1 等参数验证消息的完整性。

89、基站将解密后的消息发送到核心网。

具体实现中，上述各个步骤的更多详细实现方式可参见上述基于 IBS 技术的各个应用场景中各个步骤的相关描述，在此不再赘述。

参见图 9，是本发明实施例提供的数据传输的另一传输架构图。在图 9 所示的传输架构中，可包括 UE、接入点和核心网节点等数据传输端。其中，接入点可包括 BS， Wi-Fi AP 或者作为网络热点的热点 UE。其中，上述 BS 可为 3G 网络中的 NB，也可为 4G 网络中的 eNB，或者更前的网络时代中的基站，在此不做限制。本发明实施例将以 BS 为例进行说明。

其中，上述核心网节点可包括： CP-AU、HSS 、控制面功能（英文：Control Plane Function，CP-Function）或者 KMS 等。

参见图 10，图 10 是本发明实施例提供的传输数据的保护系统进行数据传输的另一交互示意图。本发明实施例提供的保护系统中各个数据传输端进行数据传输的过程可包括步骤：

S901， UE 在需要发送传输数据时，从其第一预存数据中获取加密公钥、全局公钥或者 UE 对应的私钥对传输数据进行保护以得到保护消息。

S902，UE 向接入点发送保护消息。

S903，接入点向核心网节点发送保护消息。

S904，核心网节点在接收到保护消息之后，根据保护方式的指示消息从其第二预存数据中获取全局公钥和核心网节点对应的私钥对保护消息进行解析。

在一些可行的实施方式中，UE 发送通过 BS 发送传输数据到核心网之前，可与核心网进行交互认证。具体的，核心网节点可预先从 KMS 获取系统参数，并将获取的系统参数存储在核心网节点的指定存储空间，即可将获取的系统参数存储为核心网节点的预存数据（设为第二预存数据）。其中，核心网节点从 KMS 获取的系统参数可包括加密公钥，或者第一全局公钥和第五私钥，或者第二全局公钥和第六私钥等。其中，核心网节点从 KMS 获取的系统参数具体包含的信息可根据核心网节点在实际应用场景中执行的数据传输操作的需求确定，在此不做限制。

具体实现中，上述加密公钥可为核心网节点的标识，如核心网节点的 ID，或者上述加密公钥包含核心网节点的 ID 等。若具体应用场景中，上述核心网节点为 CP_AU，则上述加密公钥可为 CP-AU 的身份（即 CP_AU_ID），或者上述加密公钥包含 CP_AU_ID。其中，上述加密公钥包含CP_AU_ID表示上述加密公钥由CP_AU_ID和其他数据构成，CP_AU_ID只是加密公钥的长串数据中的一部分数据，具体可根据时间采用的加密公钥的数据形式确定，在此不做限制。

若具体应用场景中，上述接入点为 HSS，则上述加密公钥可为 HSS_ID，或者上述加密公钥包含 HSS_ID。具体实现中，接入点为 HSS 时，加密公钥的具体组成形式可根据实际应用场景确定，在此不做限制。

进一步的，具体实现中，上述接入点从 KMS 获取的第一全局公钥可为 IBC 技术的数据加密全局公钥 GPK_{enc}。第五私钥可使用 IBC 技术根据核心网节点的 ID 和上述 GPK_{enc} 生成的核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$。其中，上述 CP-AU 和 HSS 在数据传输中都作为核心网节点，上述生成数据加密私钥时使用的核心网节点的 ID 包括 CP_AU_ID 和

HSS_ID，因此核心网节点对应的数据加密私钥均表示为 $SK_{CP_ID_enc}$。上述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}。第六私钥为使用 IBC 技术根据核心网节点的 ID 和上述 GPK_{Sig} 生成的核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

在一些可行的实施方式中，UE 可从核心网获取加密公钥和用于处理传输数据的核心网处理参数，并将上述加密公钥和核心网处理参数存储为 UE 的第一预存数据。其中，上述核心网处理参数可包括全局公钥或者 UE 对应的私钥等。其中，上述全局公钥包括第一全局公钥和第二全局公钥，上述私钥包括第三私钥和第四私钥。其中，上述第一全局公钥为与核心网节点获取的第一全局公钥相同的数据加密全局公钥 GPK_{enc}。上述第二全局公钥为与核心网节点获取的第二全局公钥相同的数据签名全局公钥 GPK_{sig}。上述第三私钥可使用 IBC 技术根据 UE_ID 和上述 GPK_{enc} 生成的 UE 对应的数据加密私钥 $SK_{UE_ID_enc}$。上述第四私钥为使用 IBC 技术根据 UE_ID 和上述 GPK_{sig} 生成的 UE 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

在一些可行的实施方式中，UE 可在需要向接入点发送传输数据时，可根据核心网节点的 ID 等标识信息从第一预存数据中获取核心网节点对应的加密公钥和 GPK_{enc}。例如，若上述核心网节点为 CP-AU，则可根据 CP_AU_ID 从第一预存数据中获取加密公钥，其中，加密公钥可为 CP_AU_ID，或者加密公钥包含 CP_AU_ID。进一步的，UE 可使用加密公钥、GPK_{enc} 对传输数据进行加密以得到保护消息。其中，上述保护消息可携带传输数据的保护方式的指示信息。上述传输数据的保护方式为使用加密公钥和 GPK_{enc} 对传输数据进行加密。

具体实现中，UE 对传输数据进行加密得到保护消息之后，则可将上述保护消息发送给接入点。其中，上述保护消息可包含一个指示位，上述指示位用于传输上述指示信息，用于告知核心网节点上述传输数据的保护方式。接入点接收到上述保护消息之后，可向核心网节点转发上述保护消息以及上述保护消息中携带的指示信息等。

在一些可行的实施方式中，核心网节点接到上述保护消息之后，可首先根据上述保护消息确定传输数据的保护方式，进而可根据保护方式从第二预存数据中获取相关的数据对传输数据进行解析。其中，若上述传输数据的保护方式为使用加密公钥和 GPK_{enc} 对传输数据进行加密，核心网节点则可从第二预存数据中获取 $SK_{CP_ID_enc}$ 和 GPK_{enc}，并使用 $SK_{BS_ID_enc}$ 和 GPK_{enc} 对保护消息进行解密以得到解密消息。

进一步的，在一些可行的实施方式中，UE 需要向核心网节点发送传输数据时，还可对传输数据进行签名。具体的，UE 可在需要向核心网节点发送传输数据时，从第一预存数据中获取加密公钥、GPK_{enc}、GPK_{sig} 以及 $SK_{UE_ID_Sig}$。进而可根据 GPK_{sig} 和 $SK_{UE_ID_Sig}$ 对传输数据进行签名以得到签名 Sig3，并使用上述加密公钥、GPK_{enc} 对传输数据、UE 的标识信息和上述 Sig3 进行加密以得到保护消息。其中，上述保护消息可携带传输数据的保护方式的指示信息。上述传输数据的保护方式为使用加密公钥、GPK_{enc} 对传输数据以及上述 Sig3 进行加密。

具体实现中，UE 对传输数据进行加密得到保护消息之后，则可将上述保护消息发送给接入点。接入点可将上述保护消息转发给核心网节点。其中，上述保护消息可包含一个指示位，上述指示位用于传输上述指示信息，用于告知接入点上述传输数据的保护方式。

在一些可行的实施方式中，核心网节点接到上述保护消息之后，可首先根据上述保护消息确定传输数据的保护方式，进而可根据保护方式从第二预存数据中获取相关的数据对

传输数据进行解析。其中，上述传输数据的保护方式为使用使用加密公钥、GPK_{enc}对传输数据以及上述 Sig3 进行加密。核心网节点根据加密方式的指示消息确定传输数据的保护方式为使用使用加密公钥、GPK_{enc}对传输数据以及上述 Sig3 进行加密之后，可从第二预存数据中获取 GPK_{enc}和 $SK_{CP_ID_enc}$，并使用 $SK_{CP_ID_enc}$和 GPK_{enc}对保护消息进行解密以获取传输数据。进一步的，核心网节点还可从保护消息解密得到的解密消息中获取 UE 的标识信息（如 UE_ID）和上述 Sig3。具体实现中，UE 向核心网节点发送保护消息时，可在上述保护消息中携带 UE_ID 等标识，以供核心网节点根据 UE_ID 等标识对保护消息中的签名进行验证。

具体实现中，核心网节点根据加密方式的指示消息确定传输数据的保护方式为使用使用加密公钥、GPK_{enc}对传输数据以及上述 Sig3 进行加密之后，可从第二预存数据中获取上述 GPK_{sig}，并使用 UE_ID 和上述 GPK_{sig}对上述保护消息中携带的 Sig3 进行验证。若上述当保护消息中的 Sig3 验证成功，核心网节点则可将传输数据发送到核心网中的相关网元。

进一步的，在一些可行的实施方式中，UE 需要向核心网节点发送传输数据时，还可根据加密公钥、全局公钥以及 UE 对应的数据加密私钥等数据生成对称钥 K3，进而可使用对称钥对传输数据进行保护。具体的，UE 可在需要向核心网节点发送传输数据时，从第一预存数据中获取加密公钥、GPK_{enc}以及 $SK_{UE_ID_enc}$。进一步的，UE 可根据上述加密公钥、GPK_{enc}以及 $SK_{UE_ID_enc}$生成对称钥（设定为 K3），并将上述传输数据和上述 K3 输入系统函数以获取一个完整性校验码（设定为第四完整性校验码 MAC3）。需要说明的是，本发明实施例中所描述的系统函数具体可为哈希函数，也可为其他可实现完整性校验码的生成的系统函数，具体可根据实际应用场景确定，在此不再做限制。

具体实现中，UE 根据加密公钥、GPK_{enc}以及 $SK_{UE_ID_enc}$生成 K3 之后，可使用上述加密公钥和上述 GPK_{enc}对传输数据、UE_ID 等 UE 标识信息以及上述生成的 MAC3 进行加密以得到保护消息。进一步的，UE 可在上述保护消息中携带上述传输数据的保护方式的指示信息，上述指示信息用于指示传输数据的保护方式为使用加密公钥和 GPK_{enc}对传输数据、UE_ID 以及 MAC3 进行加密。

具体实现中，UE 对传输数据进行加密得到保护消息之后，则可将上述保护消息发送给接入点。接入点可将上述保护消息发送给核心网节点。其中，上述保护消息可包含一个指示位，上述指示位用于传输上述指示信息，用于告知接入点上述传输数据的保护方式。

在一些可行的实施方式中，核心网节点接到上述保护消息之后，可首先根据上述保护消息确定传输数据的保护方式，进而可根据保护方式从第二预存数据中获取相关的数据对传输数据进行解析。其中，上述传输数据的保护方式为使用加密公钥和GPK_{enc}对传输数据、UE_ID 以及 MAC3 进行加密。核心网节点可根据上述保护方式的指示消息确定传输数据的保护方式为使用加密公钥和 GPK_{enc}对传输数据、UE_ID 以及 MAC3 进行加密，进而可从上述第二预存数据中获取 GPK_{enc}和 $SK_{CP_ID_enc}$，并使用上述 $SK_{CP_ID_enc}$和 GPK_{enc}对保护消息进行解密以得到解密消息。进一步的，核心网节点还可从上述解密消息中获取保护消息携带的 MAC3、UE_ID 以及传输数据，并使用上述加密公钥、UE_ID、GPK_{enc}和 $SK_{CP_ID_enc}$生成对称钥 K4。核心网节点生成上述 K4 之后，则可使用上述 K4、UE_ID 和解密得到的传输数据计算一个完整性校验码（设定为第五完整性校验码 MAC4）。若上述 MAC4 与保

护消息中携带的上述 MAC3 相匹配，核心网节点则可将上述保护消息中携带的 UE 发送的传输数据发送到核心网中相关网元。

需要说明的是，在本发明实施例中，同一个应用场景中，UE 进行数据加密使用的加密公钥与核心网节点进行数据解密或者验证使用的加密公钥相同，进而可实现加密数据在接收方的正确解密。加密公钥通过 KMS 下发等方式从核心网传递给 UE，传输数据发送方使用传输数据接收方提供的公钥进行数据保护，进而可避免在数据传输中携带数据加密密钥等信息造成信息泄露，增强了网络的安全性。

在本发明实施例中，UE 向核心网节点发送上行数据时，可使用核心网节点的身份等信息作为加密公钥，并使用 IBC 技术的全局公钥和核心网节点对应的私钥对上传传输数据进行加密，可以有效解决 5G 网络中对空口信令及其数据的保护，防止用户隐私、信令内容的泄露。核心网节点对 UE 发送的消息进行解密和签名、完整性校验码等验证，过滤非法信令和数据，保护核心网的安全。

参见图 11，图 11 是本发明实施例提供的保护系统在场景五中的一交互示意图。下面将结合图 11，对本发明实施例提供的传输数据的保护系统中各个数据传输端在场景五中数据交互过程进行描述。其中，上述核心网节点具体可为 CP-AU，则对应的加密公钥则为 CP_AU_ID 或者包含 CP_AU_ID。

在该应用场景中，UE 和 CP-AU 使用基于 IBC 的技术对从 UE 到核心网的信令和数据实施了加密，具体流程如下步骤:

111、CP-AU 获取基于 IBC 的系统参数。

具体实现中，CP-AU 可从 KMS 中获取系统参数。其中，上述系统参数包括 CP_AU_ID，GPK_{enc}，GPK_{sig}，$SK_{CP_AU_ID_enc}$ 以及 $SK_{CP_AU_ID_sig}$ 等。CP-AU 获取得到上述系统参数之后可将上述系统参数存储为其预存数据。

112、UE 与 CP-AU 完成交互认证。

UE 与 CP-AU 认证完成之后，UE 告知 CP-AU 该 UE 支持基于 IBC 的加密能力。

113、UE 从核心网获取核心网处理参数。

其中，上述核心网处理参数包括 CP_AU_ID、 GPK_{sig} 和 GPK_{enc}，或者还包含 UE_ID、$SK_{UE_ID_enc}$ 和 $SK_{UE_ID_sig}$。

114、UE 存储上述步骤 113 获取的核心网处理参数。

进一步的，U E可将上述核心网处理参数存储为其预存数据。

115、UE 根据核心网处理参数对需要发送的传输数据进行保护。

具体实现中，UE 收到应用需要发送的信令或者数据，从第一预存数据中获取 CP_AU_ID, GPK_{sig}，GPK_{enc} 等参数，UE 使用 GPK_{sig} 和 $SK_{UE_ID_sig}$ 对信令或者数据进行签名，UE 还可使用 CP_AU_ID 和 GPK_{enc} 对数据或者信令进行加密以得到保护消息。

116、UE 将加密后的信令或者数据发给基站。

117、基站向 CP-AU 转发加密后的信令或者数据。

118、CP-AU 验证收到的信令或者数据。

CP-AU 使用 GPK_{enc} 和 $SK_{CP_AU_ID_enc}$ 解密数据或者信令，进一步的，CP-AU 还可使用

UE_ID 和 GPK_{sig} 对保护消息中携带的签名进行验证。具体实现中，上述 CP-AU 对保护消息中的加密数据进行解密以及保护消息中的签名进行验证的具体实现方式可参见上述各个应用场景中各个步骤描述的实现方式，在此不再赘述。

119、CP-AU 转发数据。

具体实现中，CP-AU 对保护消息进行解密和验证之后，若判断得接收到的消息是用户面数据包， CP-AU 则可根据解密后的数据包中包含的地址信息，向相对应的核心网数据网关（如 UP_GW）转发数据。若判断得接收到的的消息是信令消息时， CP-AU 则可根据解密后的数据包中包含的信息，自己处理或者向相对应的核心网节点（如 HSS）发送信令。

具体实现中，上述各个步骤的更多详细实现方式可参见上述 S901-S904 中各个步骤的相关描述，在此不再赘述。

参见图 12，图 12 是本发明实施例提供的保护系统在场景五中的另一交互示意图。下面将结合图 12，对本发明实施例提供的传输数据的保护系统中各个数据传输端在场景五中数据交互过程进行描述。其中，上述核心网节点具体可为 HSS，则对应的加密公钥则为 HSS_ID 或者包含 HSS_ID。

在该应用场景中， UE 和 HSS 使用基于 IBC 的技术对从 UE 到核心网的信令和数据实施了加密，具体流程如下步骤:

121、HSS 获取基于 IBC 的系统参数。

具体实现中，HSS 可从 KMS 中获取系统参数，其中，上述系统参数可包括 HSS_ID、GPK_{enc}、GPK_{sig}、$SK_{HSS_ID_enc}$ 和 $SK_{HSS_ID_sig}$ 等。HSS 可将上述系统参数存储为其预存数据。

122、UE 与 CP-AU 完成交互认证。

具体实现中，UE 与 CP-AU 完成交互认证之后，还可告知 CP-AU 该 UE 支持基于 IBC 的加密或者认证等能力。

123、UE 从核心网获取核心网处理参数。

其中，上述核心网处理参数可包括: HSS_ID、GPK_{sig} 和 GPK_{enc} 等。

124、UE 存储上述步骤 123 获取的核心网处理参数。

进一步的，UE 可将获取的核心网处理参数存储为其预存数据。

125、UE 根据核心网处理参数对需要发送的传输数据进行保护。

具体实现中，UE 收到应用需要发送的信令（如 attach 消息）时，可从第一预存数据中获取 HSS_ID、GPK_{sig} 和 GPK_{enc} 等参数，使用 HSS_ID 和 GPK_{enc} 对信令加密以得到保护消息。

126、UE 将加密后的信令发送给基站。

其中，上述加密后的信令中携带 HSS_ID。

127、基站向 CP-AU 转发加密后的信令。

128、CP-AU 向 HSS 转发加密后的信令。

129、HSS 解密信令。

具体实现中，HSS 使用 HSS_ID、 GPK_{enc} 和 $SK_{HSS_ID_enc}$ 等参数解密信令并与 UE 开展后续信令交互。

具体实现中，上述各个步骤的更多详细实现方式可参见上述 S901-S904 中各个步骤的相关描述，在此不再赘述。

参见图 13，图 13 是本发明实施例提供的保护系统在场景五中的另一交互示意图。下面将结合图 13，对本发明实施例提供的传输数据的保护系统中各个数据传输端在场景五中数据交互过程进行描述。其中，上述核心网节点具体可为 CP-AU 和 CP-Function，则对应的加密公钥则为 CP_AU_ID 或者包含 CP_AU_ID。

在该应用场景中，UE 和 CP-AU 使用基于 IBC 的技术对从 UE 到核心网的信令和数据实施了加密，具体流程如下步骤:

131、UE 与 CP-AU 进行交互认证。

具体实现中，UE 与 CP-AU 进行相互认证成功之后，UE 可告知 CP-AU 其支持的基于 IBC 的加密和认证等能力。

132、UE 从核心网获取核心网处理参数。

具体实现中，上述核心网处理参数可包括 CP_AU_ID、GPK_{sig}、GPK_{enc} 和 SK_{UE_ID} 等。

133、UE 存储上述步骤 132 获取的核心网处理参数。

具体实现中，UE 可将获取得到的核心网处理参数存储为其预存数据。

134、UE 对传输数据进行保护。

具体实现中，UE 收到应用需要发送的传输数据之后，可从其预存数据中获取 CP_AU_ID、GPK_{sig} 和 GPK_{enc} 等参数，UE 使用 CP_AU_ID、SK_{UE_ID} 、GPK_{sig} 和 GPK_{enc} 等参数生成对称密钥 K3，使用 K3 对数据进行加密并提供完整性保护 MAC3 以得到保护消息。

135、UE 将上述保护消息发送给基站。

其中，上述保护消息中携带 UE_ID，传输数据和 MAC3 等，其中包含 UE_ID 具体可为全球唯一临时 UE 标识（英文：Globally Unique Temporary UE Identity ， GUTI）。

136、基站向核心网的 CP-Function 转发数据。

其中，上述 CP-Function 是核心网专门处理小数据的节点。

137、CP-Function 获取解密数据。

CP-Function 可使用 GUTI 获取 UE_ID，并使用 UE_ID， $SK_{CP_AU_ID}$、GPK_{enc} 或者 GPK_{sig} 生成对称密钥 K4。进一步的，可根据 K4 和 UE_ID 以及保护消息对消息中包含的 MAC3 进行验证并获取传输数据。

具体实现中，上述各个步骤的更多详细实现方式可参见上述 S901-S904 中各个步骤的相关描述，在此不再赘述。

参见图 14，是本发明实施例提供的数据传输的另一传输架构图。在图 14 所示的传输架构中，可包括 UE、接入点和核心网节点等数据传输端。其中，接入点可包括基站（英文：Base Station，BS），无线保真（英文：Wireless-Fidelity，Wi-Fi）网络中的接入点（英文：Access Point，AP）或者作为网络热点的热点 UE。其中，上述 BS 可为 3G 网络中的基站（英文：Node B，NB），也可为 4G 网络中的演进性基站（英文：Evolved Node B，eNB），或者更前的网络时代中的基站，在此不做限制。本发明实施例将以 BS 为例进行说明。

其中，上述核心网节点可包括：核心网认证节点 CP-AU、HSS 、CP-Function 或者 UP-Function 等。

参见图 15，图 15 是本发明实施例提供的传输数据的保护系统进行下行数据传输的交互示意图。本发明实施例提供的保护系统中各个数据传输端进行数据传输的过程可包括步骤：

S1501，核心网节点接收用户面网关下发的传输数据。

进一步的，核心网节点还可从其第二预存数据中获取 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及核心网节点对应的私钥等数据。

S1502，核心网节点使用 UE 的标识信息、全局公钥和其对应的私钥对传输数据进行保护以得到保护消息，并将保护消息发送给接入点。

S1503，接入点用于将保护消息发送给 UE。

S1504， UE 从其第一预存数据中获取所述核心网节点的标识，全局公钥和 UE 对应的私钥对保护消息进行解析以得到传输数据。

在一些可行的实施方式中，上述全局公钥包括第一全局公钥和第二全局公钥，上述核心网节点对应的私钥包括第五私钥和第六私钥。核心网节点可从网络或者 KMS 中获取核心网系统参数，并将核心网系统参数存储为核心网接入点的第二预存数据。其中，上述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥等。上述第一全局公钥为 GPK_{enc}；上述第五私钥为 IBC 技术的核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$；上述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；上述述第六私钥为 IBC 技术的核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

具体实现中， UE 可从核心网中获取其标识信息和核心网处理参数，并将标识信息和核心网处理参数存储为 UE 的第一预存数据。其中，上述核心网处理参数包括 GPK_{enc}、$SK_{UE_ID_enc}$、GPK_{Sig} 以及 $SK_{UE_ID_Sig}$ 等，其中，上述各个参数的定义可参见上述各个应用场景中各个步骤描述的实现方式，在此不再赘述。

在一些可行的实施方式中，核心网节点可接收用户面网关发送的下行传输数据（以下简称传输数据），进而可在接收到传输数据之后，从第二预存数据中获取 UE 的标识信息（如 UE_ID）、GPK_{enc} 以及 $SK_{CP_ID_enc}$ 等参数，并根据 UE 的标识信息、GPK_{enc} 以及 $SK_{CP_ID_enc}$ 生成对称钥 K5，进而可将传输数据和 K5 输入系统函数以获取第六完整性校验码 MAC5。进一步的，核心网节点还可使用 K5 对传输数据和 MAC5 进行加密得到保护消息。

核心网节点将上述保护消息发送给基站，并通过基站发送给 UE。UE 接收到消息之后，可根据保护消息中携带的信息确认消息是发给自己的，进而可对消息进行解密。

具体实现中，UE 对消息进行解密时，可从其第一预存数据中获取 GPK_{enc} 和 $SK_{UE_ID_enc}$，并使用 GPK_{enc} 和 $SK_{UE_ID_enc}$ 对保护消息进行解密以得到解密消息。进一步的，UE 可使用上述 UE 的标识信息、GPK_{enc} 和 $SK_{UE_ID_enc}$ 生成对称钥 K6，并使用 K6、UE 的标识信息和解密消息生成第七完整性校验码 MAC6，并当所述 MAC6 与解密消息中携带的 MAC5 相匹配时，获取传输数据。

在本发明实施例中，UE 和核心网节点可使用基于 IBC 的技术对下行数据进行加密和验证保护，增强了网络传输数据的安全性。具体实现中，上述 UE 和核心网节点对下行数

据的具体加密和验证保护的方式可参见上述上行数据传输中 UE 和接入点或者核心网节点对上行数据的加密和验证保护的实现方式，在此不再赘述。

参见图 16，图 16 是本发明实施例提供的保护系统在场景六中的交互示意图。下面将结合图 16，对本发明实施例提供的传输数据的保护系统中各个数据传输端在场景六中数据交互过程进行描述。其中，上述核心网节点具体可为 UP-GW、UP-Function 和 CP-Function，则对应的加密公钥则为 CP_ Function _ID（以下简称 CP_ID）或者包含 CP_ Function _ID。

在该应用场景中， UE 和 CP- Function 使用基于 IBC 的技术对从 UE 到核心网的信令和数据实施了加密，具体流程如下步骤：

161、核心网节点 CP_Function 收到 UP-GW 发来的数据。

162、CP_Function 对数据进行保护。

具体实现中，CP_Function 可使用 UE_ID, SK_{CP_ID},GPK_{enc} 生成对称密钥 K5，使用对称密钥 K5 对数据进行加密，并根据传输数据和 K5 生成完整性校验码 MAC5，以对加密后的数据提供完整性保护。

163、CP-Function 发送上述加密后的数据到 RAN。

其中，上述 CP-Function 发送给 RAN 的数据中包括 UE 的 GUTI、加密后的数据和上述 MAC5。

164、RAN 发送数据到 UE。

其中，RAN 向 UE 发送的数据中包括 GUTI、加密后的数据以及 MAC5。

165、UE 解密数据。

具体实现中，UE 可根据 GUTI 确认消息是自己的，并从其预存数据中获取 UE_ID，使用 CP_ID, SK_{UE_ID} 和 GPK_{enc} 生成对称密钥 K6,使用 K6 验证签名并解密数据。

具体实现中，上述各个步骤的更多详细实现方式可参见上述 S1501-S1504 中各个步骤的相关描述，在此不再赘述。

参见图 17，是本发明实施例提供的传输数据的保护方法的一流程示意图。本发明实施例提供的方法，包括步骤：

S1701，UE 接收接入点发送的广播消息，并存储所述广播消息中携带的加密公钥。

S1702，所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息。

S1703，所述 UE 向所述接入点发送所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述 UE 接收所述接入点的广播消息之前，所述方法还包括：

所述 UE 从网络或者 KMS 中获取所述 UE 用于处理传输数据的处理参数，并将所述处理参数存储为所述 UE 的第一预存数据；

其中，所述处理参数包括 UE 所属运营商的身份 operator ID1 以及以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

在一些可行的实施方式中，所述第一预存数据中包括所述 operator ID1 和所述 GPK_{Sig}；

所述 UE 存储所述广播消息中携带的加密公钥之前，所述方法还包括：

所述 UE 根据接收到的所述广播消息中携带的指示信息确定所述接入点具有数据签名功能，并根据所述广播消息对应的接入点的标识信息确定所述接入点所属的运营商的身份 operator ID2；

将所述 operator ID2 与所述 operator ID1 进行匹配，从所述第一预存数据中查找所述接入点对应的第三全局公钥 $GPK_{Sig}1$；

当所述广播消息中携带签名 Sig1 时，使用所述 $GPK_{Sig}1$ 和所述接入点的标识信息对所述广播消息进行验证；

当所述广播消息验证通过时，确定将所述广播消息携带的所述加密公钥添加至所述第一预存数据中。

在一些可行的实施方式中，所述第一预存数据中包括所述 GPK_{enc}；

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥，并使用所述加密公钥和所述全局公钥对所述传输数据进行保护包括：

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc}；

使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密。

在一些可行的实施方式中，所述第一预存数据中包括所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护包括：

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$；

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成第一对称钥 K1，并将所述传输数据和所述 K1 输入系统函数以获取第三完整性校验码 MAC2；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据以及所述 UE 的标识信息、所述 MAC2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息以及所述 MAC2 进行加密。

在一些可行的实施方式中，所述第一预存数据中包括所述所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$;

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$;

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig2，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息和所述 Sig2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述 Sig2 进行加密。

具体实现中，本发明实施例提供的传输数据的保护方法中各个步骤所描述的实现方式可参见上述各个系统中相关描述，在此不再赘述。

参见图 18，是本发明实施例提供的传输数据的保护方法的另一流程示意图。本发明实施例提供的方法，包括步骤:

S1801，接入点发送广播消息。

其中，所述广播消息中携带加密公钥。

S1802，所述接入点接收用户设备 UE 发送的根据所述加密公钥对传输数据进行保护得到的保护消息。

其中，所述保护消息中携带所述 UE 发送的传输数据的保护方式的指示消息。

S1803，所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据。

S1804，所述接入点将解析得到的所述 UE 发送的传输数据发送到核心网中。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述接入点对应的私钥包括第一私钥和第二私钥;

所述接入点发送广播消息之前，所述方法还包括:

所述接入点从网络或者密钥管理系统 KMS 中获取系统参数，并将所述系统参数存储为所述接入点的第二预存数据;

其中，所述系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第一私钥，或者第二全局公钥和第二私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第一私钥为 IBC 技术的所述接入点对应的数据加密私钥 $SK_{BS_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第二私钥为 IBC 技术的所述接入点对应的数据签名私钥 $SK_{BS_ID_Sig}$。

在一些可行的实施方式中，所述加密公钥为基站 BS 的身份 BS_ID，或者所述加密公钥包含 BS_ID；或者

所述加密公钥包括无线保真 Wi-Fi 切入点 AP 的介质控制子层 MAC 地址，或者 Wi-Fi AP 的服务集标识 SSID；或者

所述加密公钥包括热点 UE 的身份 UE_ID，或者热点 UE 的移动用户身份 IMSI。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$；

所述接入点发送广播消息之前，所述方法还包括：

所述接入点使用所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$ 对所述广播消息进行签名以得到所述广播消息的签名 Sig1，并在所述广播消息中携带所述接入点具有数据签名功能的指示信息或者所述广播消息的签名 Sig1。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$、所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$；

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析包括：

所述接入点根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息。

在一些可行的实施方式中，所述第二预存数据中包括加密公钥、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$；

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析包括：

所述接入点根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息；

所述接入点将解析得到的所述 UE 发送的传输数据发送到核心网中包括：

所述接入点从所述解密消息中获取所述保护消息携带的第三完整性保护码 MAC2、UE 的标识信息以及所述传输数据；

使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$ 生成对称钥 K2；

使用所述对称钥 K2、所述 UE 的标识信息和解密得到的传输数据计算第四完整性校验码 MAC3，并当所述 MAC3 与所述 MAC2 相匹配时，将所述 UE 发送的传输数据发送到核心网。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$ 和所述 GPK_{Sig}；

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析包括：

根据所述加密方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消

息进行解密以获取所述传输数据;

所述接入点将解析得到的所述 UE 发送的传输数据发送到核心网中包括:

从所述保护消息解密得到的解密消息中获取所述 UE 的标识信息和所述签名 Sig2;

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{sig};

使用所述 UE 的标识信息以及所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，将所述 UE 发送的传输数据发送到核心网。

具体实现中，本发明实施例提供的传输数据的保护方法中各个步骤所描述的实现方式可参见上述各个系统中相关描述，在此不再赘述。

参见图 19，是本发明实施例提供的传输数据的保护方法的另一流程示意图。本发明实施例提供的方法，包括步骤:

S1901，用户设备 UE 在需要发送传输数据时，从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息。

S1902，所述 UE 向接入点发送所述保护消息，以通过所述接入点将所述保护消息发送给核心网节点。

其中，所述保护消息中携带所述传输数据的保护方式的指示消息。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥;

所述 UE 发送传输数据之前，所述方法还包括:

所述 UE 从核心网中获取加密公钥、所述 UE 用于处理传输数据的核心网处理参数，并将所述加密公钥和所述核心网处理参数存储为所述 UE 的第一预存数据;

其中，所述核心网处理参数包括以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

在一些可行的实施方式中，所述第一预存数据中包括所述加密公钥和所述 GPK_{enc};

所述 UE 从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥，并使用所述加密公钥，以及所述全局公钥对所述传输数据进行保护包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc};

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密。

在一些可行的实施方式中，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和所

述 $SK_{UE_ID_enc}$;

所述 UE 从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$;

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成对称钥 K3，并将所述传输数据和所述 K3 输入系统函数以获取第四完整性校验码 MAC3;

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密。

在一些可行的实施方式中，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$;

所述 UE 从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$;

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig3，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据和所述签名 Sig2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述签名进行加密。

具体实现中，本发明实施例提供的传输数据的保护方法中各个步骤所描述的实现方式可参见上述各个系统中相关描述，在此不再赘述。

参见图 20，是本发明实施例提供的传输数据的保护方法的另一流程示意图。本发明实施例提供的方法，包括步骤:

S2001，核心网节点接收接入点发送的保护消息。

其中，所述保护消息中携带用户设备 UE 发送的所述传输数据的保护方式的指示消息。

S2002，所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥;

所述核心网节点接收接入点发送的保护消息之前，所述方法还包括:

所述核心网节点从密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据;

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公

钥和第五私钥，或者第二全局公钥和第六私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

在一些可行的实施方式中，所述加密公钥为核心网认证节点的身份，或者所述加密公钥包含所述核心网节点的身份。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析包括:

所述核心网节点根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到所述 UE 的传输数据。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析包括:

所述核心网节点根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$，对所述保护消息进行解密以得到解密消息;

获取所述解密消息中携带的第四完整性校验码 MAC3，并使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$ 生成对称钥 K4;

使用所述 K4、所述 UE 的标识信息和所述解密消息生成第五完整性校验码 MAC4，并当所述 MAC4 与所述 MAC3 相匹配时，获取所述传输数据。

在一些可行的实施方式中，所述第二预存数据中包括所述加密公钥、所述 GPK_{enc}、所述 $SK_{CP_ID_enc}$ 和所述 GPK_{Sig};

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析包括:

所述核心网节点根据所述加密方式的指示消息确定所述传输数据的保护方式，并使用从所述第二预存数据中获取的所述 GPK_{enc}、所述加密公钥和所述 $SK_{CP_ID_enc}$ 对所述保护消息进行解密;

从所述保护消息解密得到的解密消息中获取所述签名 Sig3，并使用所述 UE 的标识信息和所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，获取所述传输数据。

具体实现中，本发明实施例提供的传输数据的保护方法中各个步骤所描述的实现方式可参见上述各个系统中相关描述，在此不再赘述。

参见图 21，是本发明实施例提供的传输数据的保护方法的另一流程示意图。本发明实施例提供的方法，包括步骤:

S2101，核心网节点接收用户面网关下发的传输数据，并从其第二预存数据中获取用户设备 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥。

S2102，所述核心网节点使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述传输数据进行保护以得到保护消息，并将所述保护消息发送给接入点。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥;

所述核心网节点接收用户面网关下发的传输数据之前，所述方法还包括:

所述核心网节点从网络或者密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据;

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述核心网节点从其第二预存数据中获取用户设备 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥包括:

所述核心网节点从所述第二预存数据中获取所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$;

所述核心网节点使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述传输数据进行保护以得到保护消息包括:

所述核心网节点根据所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$ 生成对称钥 K5，并将所述传输数据和所述 K5 输入系统函数以获取第六完整性校验码 MAC5;

使用所述 K5 对所述传输数据加密得到保护消息。

具体实现中，本发明实施例提供的传输数据的保护方法中各个步骤所描述的实现方式可参见上述各个系统中相关描述，在此不再赘述。

参见图 22，是本发明实施例提供的传输数据的保护方法的另一流程示意图。本发明实施例提供的方法，包括步骤:

S2201，用户设备 UE 接收接入点发送的保护消息。

S2202，所述 UE 从其第一预存数据中获取核心网节点的标识，基于身份的密码 IBC 技术的全局公钥和所述 UE 对应的私钥对所述保护消息进行解析以得到所述传输数据。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE

对应的私钥包括第三私钥和第四私钥;

所述 UE 接收接入点发送的保护消息之前，所述方法还包括:

所述 UE 从核心网中获取其标识信息、所述 UE 用于处理传输数据的核心网处理参数，并将所述标识信息和所述核心网处理参数存储为所述 UE 的第一预存数据;

其中，所述核心网处理参数包括以下两组数据中至少一组: 第一全局公钥和第三私钥，或者第二全局公钥和第四私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

在一些可行的实施方式中，所述第一预存数据中包括所述 UE 的标识信息、所述核心网节点的标识、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$;

所述 UE 从其第一预存数据中获取核心网节点的标识，基于身份的密码 IBC 技术的全局公钥和所述 UE 对应的私钥对所述保护消息进行解析以得到所述传输数据包括:

所述 UE 从所述第一预存数据中获取所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$，并使用所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 对所述保护消息进行解密以得到解密消息;

使用所述核心网节点的标识信息、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 生成对称钥 K6;

使用所述 K6 对所述保护消息进行解密以得到解密消息;

使用所述 K6 和所述解密消息生成第七完整性校验码 MAC6，并当所述 MAC6 与所述解密消息中携带的第六完整性校验码 MAC5 相匹配时，获取所述传输数据。

具体实现中，本发明实施例提供的传输数据的保护方法中各个步骤所描述的实现方式可参见上述各个系统中相关描述，在此不再赘述。

参见图 23，是本发明实施例提供的传输数据的保护装置的一结构示意图。本发明实施例提供的保护装置，包括:

接收单元 231，用于接收接入点发送的广播消息，并存储所述广播消息中携带的加密公钥。

处理单元 232，用于在需要向所述接入点发送传输数据时，从用户设备 UE 的第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述接收单元接收的所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息。

发送单元 233，用于向所述接入点发送所述处理单元处理的所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥;

所述处理单元 232 还用于:

从网络或者 KMS 中获取所述 UE 用于处理传输数据的处理参数，并将所述处理参数存储为所述 UE 的第一预存数据;

其中，所述处理参数包括 UE 所属运营商的身份 operator ID1 以及以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

在一些可行的实施方式中，所述第一预存数据中包括所述 operator ID1 和所述 GPK_{Sig}；

所述接收单元 231 具体用于：

根据接收到的所述广播消息中携带的指示信息确定所述接入点具有数据签名功能，并根据所述广播消息对应的接入点的标识信息确定所述接入点所属的运营商的身份 operator ID2；

将所述 operator ID2 与所述 operator ID1 进行匹配，从所述第一预存数据中查找所述接入点对应的第三全局公钥 $GPK_{Sig}1$；

当所述广播消息中携带签名 Sig1 时，使用所述 $GPK_{Sig}1$ 和所述接入点的标识信息对所述广播消息进行验证；

当所述广播消息验证通过时，确定将所述广播消息携带的所述加密公钥添加至所述第一预存数据中。

在一些可行的实施方式中，所述第一预存数据中包括所述 GPK_{enc}；

所述处理单元 232 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc}；

使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密。

在一些可行的实施方式中，所述第一预存数据中包括所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述处理单元 232 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$；

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成第一对称钥 K1，并将所述传输数据和所述 K1 输入系统函数以获取第三完整性校验码 MAC2；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据以及所述 UE 的标识信息、所述 MAC2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息以及所述 MAC2 进行加密。

在一些可行的实施方式中，所述第一预存数据中包括所述所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$；

所述处理单元 232 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$；

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig2，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息和所述 Sig2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述 Sig2 进行加密。

具体实现中，本发明实施例提供的传输数据的保护装置中各个单元所执行的实现方式可参见上述各个系统中相关数据传输中对应的实现方式，在此不再赘述。

参见图 24，是本发明实施例提供的传输数据的保护装置的另一结构示意图。本发明实施例提供的保护装置，包括：

发送单元 241，用于发送广播消息，所述广播消息中携带加密公钥。

接收单元 242，用于接收用户设备 UE 发送的根据所述发送单元发送的所述加密公钥对传输数据进行保护得到的保护消息，所述保护消息中携带所述 UE 发送的传输数据的保护方式的指示消息。

解析单元 243，用于根据所述接收单元接收的所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据。

所述发送单元 241，还用于将所述解析单元解析得到的所述 UE 发送的传输数据发送到核心网中。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述接入点对应的私钥包括第一私钥和第二私钥；

所述解析单元 243 还用于：

从网络或者密钥管理系统 KMS 中获取系统参数，并将所述系统参数存储为所述接入点的第二预存数据；

其中，所述系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第一私钥，或者第二全局公钥和第二私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第一私钥为 IBC 技术的所述接入点对应的数据加密私钥 $SK_{BS_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第二私钥为 IBC 技术的所述接入点对应的数据签名私钥 $SK_{BS_ID_Sig}$。

在一些可行的实施方式中，所述加密公钥为基站 BS 的身份 BS_ID，或者所述加密公钥包含 BS_ID；或者

所述加密公钥包括无线保真 Wi-Fi 切入点 AP 的介质控制子层 MAC 地址，或者 Wi-Fi AP 的服务集标识 SSID；或者

所述加密公钥包括热点 UE 的身份 UE_ID，或者热点 UE 的移动用户身份 IMSI。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$；

所述发送单元 241 具体用于：

使用所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$ 对所述广播消息进行签名以得到所述广播消息的签

名 Sig1，并在所述广播消息中携带所述接入点具有数据签名功能的指示信息或者所述广播消息的签名 Sig1。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$、所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$；

所述解析单元 243 具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息。

在一些可行的实施方式中，所述第二预存数据中包括加密公钥、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$；

所述解析单元 243 具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息；

所述发送单元 241 具体用于：

从所述解析单元解析得到的所述解密消息中获取所述保护消息携带的第三完整性保护码 MAC2、UE 的标识信息以及所述传输数据；

使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$ 生成对称钥 K2；

使用所述对称钥 K2、所述 UE 的标识信息和解密得到的传输数据计算第四完整性校验码 MAC3，并当所述 MAC3 与所述 MAC2 相匹配时，将所述 UE 发送的传输数据发送到核心网。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$ 和所述 GPK_{Sig}；

所述解析单元 243 具体用于：

根据所述加密方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以获取所述传输数据；

所述发送单元 241 具体用于：

从所述保护消息解密得到的解密消息中获取所述 UE 的标识信息和所述签名 Sig2；

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{sig}；

使用所述 UE 的标识信息以及所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，将所述 UE 发送的传输数据发送到核心网。

具体实现中，本发明实施例提供的传输数据的保护装置中各个单元所执行的实现方式可参见上述各个系统中相关数据传输中对应的实现方式，在此不再赘述。

参见图 25，是本发明实施例提供的传输数据的保护装置的另一结构示意图。本发明实施例提供的保护装置，包括：

保护单元 251，用于在需要发送传输数据时，从用户设备的第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息。

发送单元 252，用于向接入点发送所述保护单元处理得到的所述保护消息，以通过所述接入点将所述保护消息发送给核心网节点，所述保护消息中携带所述传输数据的保护方式的指示消息。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述保护单元 251 还用于：

从核心网中获取加密公钥、所述 UE 用于处理传输数据的核心网处理参数，并将所述加密公钥和所述核心网处理参数存储为所述 UE 的第一预存数据；

其中，所述核心网处理参数包括以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

在一些可行的实施方式中，所述第一预存数据中包括所述加密公钥和所述 GPK_{enc}；

所述保护单元 251 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc}；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密。

在一些可行的实施方式中，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述保护单元 251 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$；

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成对称钥 K3，并将所述传输数据和所述 K3 输入系统函数以获取第四完整性校验码 MAC3；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密。

在一些可行的实施方式中，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$；

所述保护单元 251 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所

述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$;

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig3，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据和所述签名 Sig2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述签名进行加密。

具体实现中，本发明实施例提供的传输数据的保护装置中各个单元所执行的实现方式可参见上述各个系统中相关数据传输中对应的实现方式，在此不再赘述。

参见图 26，是本发明实施例提供的传输数据的保护装置的另一结构示意图。本发明实施例提供的保护装置，包括:

接收单元 261，用于接收接入点发送的保护消息，所述保护消息中携带用户设备 UE 发送的所述传输数据的保护方式的指示消息。

解析单元 262，用于根据所述接收单元接收的所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥;

所述解析单元 262 还用于:

从密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据;

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

在一些可行的实施方式中，所述加密公钥为核心网认证节点的身份，或者所述加密公钥包含所述核心网节点的身份。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述解析单元 262 具体用于:

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到所述 UE 的传输数据。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述解析单元 262 具体用于:

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$，对所述保护消息进行解密以得到解密消息;

获取所述解密消息中携带的第四完整性校验码 MAC3，并使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$ 生成对称钥 K4;

使用所述 K4、所述 UE 的标识信息和所述解密消息生成第五完整性校验码 MAC4，并当所述 MAC4 与所述 MAC3 相匹配时，获取所述传输数据。

在一些可行的实施方式中，所述第二预存数据中包括所述加密公钥、所述 GPK_{enc}、所述 $SK_{CP_ID_enc}$ 和所述 GPK_{Sig};

所述解析单元 262 具体用于:

根据所述加密方式的指示消息确定所述传输数据的保护方式，并使用从所述第二预存数据中获取的所述 GPK_{enc}、所述加密公钥和所述 $SK_{CP_ID_enc}$ 对所述保护消息进行解密;

从所述保护消息解密得到的解密消息中获取所述签名 Sig3，并使用所述 UE 的标识信息和所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，获取所述传输数据。

具体实现中，本发明实施例提供的传输数据的保护装置中各个单元所执行的实现方式可参见上述各个系统中相关数据传输中对应的实现方式，在此不再赘述。

参见图 27，是本发明实施例提供的传输数据的保护装置的另一结构示意图。本发明实施例提供的保护装置，包括:

接收单元 271，用于接收用户面网关下发的传输数据。

处理单元 272，用于从核心网节点的第二预存数据中获取用户设备 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥，并使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述接收单元接收的所述传输数据进行保护以得到保护消息。

发送单元 273，用于将所述处理单元处理得到的所述保护消息发送给接入点。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥;

所述处理单元 272 还用于:

从网络或者密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据;

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

在一些可行的实施方式中，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述处理单元 272 具体用于:

从所述第二预存数据中获取所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$;

根据所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$ 生成对称钥 K5，并将所述

传输数据和所述 K5 输入系统函数以获取第六完整性校验码 MAC5;

使用所述 K5 对所述传输数据加密得到保护消息。

具体实现中，本发明实施例提供的传输数据的保护装置中各个单元所执行的实现方式可参见上述各个系统中相关数据传输中对应的实现方式，在此不再赘述。

参见图 28，是本发明实施例提供的传输数据的保护装置的另一结构示意图。本发明实施例提供的保护装置，包括:

接收单元 281，用于接收接入点发送的保护消息。

解析单元 282，用于从用户设备的第一预存数据中获取核心网节点的标识，基于身份的密码 IBC 技术的全局公钥和所述 UE 对应的私钥对所述保护消息进行解析以得到所述传输数据。

在一些可行的实施方式中，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥;

所述解析单元 282 还用于:

从核心网中获取其标识信息、所述 UE 用于处理传输数据的核心网处理参数，并将所述标识信息和所述核心网处理参数存储为所述 UE 的第一预存数据;

其中，所述核心网处理参数包括以下两组数据中至少一组: 第一全局公钥和第三私钥，或者第二全局公钥和第四私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

在一些可行的实施方式中，所述第一预存数据中包括所述 UE 的标识信息、所述核心网节点的标识、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$;

所述解析单元 282 具体用于:

从所述第一预存数据中获取所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$，并使用所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 对所述保护消息进行解密以得到解密消息;

使用所述核心网节点的标识信息、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 生成对称钥 K6;

使用所述 K6 对所述保护消息进行解密以得到解密消息;

使用所述 K6 和所述解密消息生成第七完整性校验码 MAC6，并当所述 MAC6 与所述解密消息中携带的 MAC5 相匹配时，获取所述传输数据。

具体实现中，本发明实施例提供的传输数据的保护装置中各个单元所执行的实现方式可参见上述各个系统中相关数据传输中对应的实现方式，在此不再赘述。

本发明的说明书、权利要求书以及附图中的术语“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，意图在于覆盖不排他的包含。例如包含了一系列步骤或者单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或者单元，

或可选地还包括对于这些过程、方法、系统、产品或设备固有的其他步骤或单元。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。

以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

权 利 要 求

1、一种传输数据的保护系统，其特征在于，包括：用户设备 UE 和接入点；

所述接入点用于发送广播消息，所述广播消息中携带加密公钥；

所述 UE 用于接收所述接入点的所述广播消息，并存储所述加密公钥；

所述 UE 还用于在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息；

所述 UE 还用于向所述接入点发送所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息；

所述接入点还用于在接收到所述保护消息之后，根据所述保护方式的指示消息从其第二预存数据中获取所述全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据；

所述接入点还用于将解析得到的所述 UE 发送的传输数据发送到核心网中。

2、如权利要求 1 所述的保护系统，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述接入点对应的私钥包括第一私钥和第二私钥；

所述接入点还用于在发送广播消息之前，从网络或者密钥管理系统 KMS 中获取系统参数，并将所述系统参数存储为所述接入点的第二预存数据；

其中，所述系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第一私钥，或者第二全局公钥和第二私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第一私钥为 IBC 技术的所述接入点对应的数据加密私钥 $SK_{BS_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第二私钥为 IBC 技术的所述接入点对应的数据签名私钥 $SK_{BS_ID_Sig}$。

3、如权利要求 2 所述的保护系统，其特征在于，所述加密公钥为基站 BS 的身份 BS_ID，或者所述加密公钥包含 BS_ID；或者

所述加密公钥包括无线保真 Wi-Fi 切入点 AP 的介质控制子层 MAC 地址，或者 Wi-Fi AP 的服务集标识 SSID；或者

所述加密公钥包括热点 UE 的身份 UE_ID，或者热点 UE 的移动用户身份 IMSI。

4、如权利要求 1 所述的保护系统，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述 UE 还用于在接收所述接入点的广播消息之前，从网络或者 KMS 中获取所述 UE 用于处理传输数据的处理参数，并将所述处理参数存储为所述 UE 的第一预存数据；

其中，所述处理参数包括 UE 所属运营商的身份 operator ID1 以及以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

5、如权利要求 3 或 4 所述的保护系统，其特征在于，所述第二预存数据中包括所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$;

所述接入点还用于使用所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$ 对所述广播消息进行签名以得到所述广播消息的签名 Sig1，并在所述广播消息中携带所述接入点具有数据签名功能的指示信息或者所述广播消息的签名 Sig1。

6、如权利要求 5 所述的保护系统，其特征在于，所述第一预存数据中包括所述 operator ID1 和所述 GPK_{Sig};

所述 UE 具体用于:

根据接收到的所述广播消息中携带的指示信息确定所述接入点具有数据签名功能，并根据所述广播消息对应的接入点的标识信息确定所述接入点所属的运营商的身份 operator ID2;

将所述 operator ID2 与所述 operator ID1 进行匹配，从所述第一预存数据中查找所述接入点对应的第三全局公钥 $GPK_{Sig}1$;

当所述广播消息中携带签名 Sig1 时，使用所述 $GPK_{Sig}1$ 和所述接入点的标识信息对所述广播消息进行验证;

当所述广播消息验证通过时，确定将所述广播消息携带的所述加密公钥添加至所述第一预存数据中。

7、如权利要求 6 所述的保护系统，其特征在于，所述第一预存数据中包括所述 GPK_{enc};

所述 UE 具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc};

使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密。

8、如权利要求 7 所述的保护系统，其特征在于，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$、所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$;

所述接入点具体用于:

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息;

执行将所述解密消息中携带的所述 UE 发送的传输数据发送到核心网的步骤。

9、如权利要求 6 所述的保护系统，其特征在于，所述第一预存数据中包括所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述 UE 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$；

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成第一对称钥 K1，并将所述传输数据和所述 K1 输入系统函数以获取第三完整性校验码 MAC2；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据以及所述 UE 的标识信息、所述 MAC2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息以及所述 MAC2 进行加密。

10、如权利要求 9 所述的保护系统，其特征在于，所述第二预存数据中包括加密公钥、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$；

所述接入点具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息；

所述接入点还用于：

从所述解密消息中获取所述保护消息携带的所述 MAC2、UE 的标识信息以及所述传输数据；

使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$ 生成对称钥 K2；

使用所述对称钥 K2、所述 UE 的标识信息和解密得到的传输数据计算第四完整性校验码 MAC3，并当所述 MAC3 与所述 MAC2 相匹配时，执行将所述 UE 发送的传输数据发送到核心网的步骤。

11、如权利要求 6 所述的保护系统，其特征在于，所述第一预存数据中包括所述所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$；

所述 UE 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$；

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig2，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息和所述 Sig2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述 Sig2 进行加密。

12、如权利要求 11 所述的保护系统，其特征在于，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$ 和所述 GPK_{Sig}；

所述接入点具体用于：

根据所述加密方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以获取所述传输数据；

所述接入点还用于：

从所述保护消息解密得到的解密消息中获取所述 UE 的标识信息和所述签名 Sig2；

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{sig}；

使用所述 UE 的标识信息以及所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，执行将所述 UE 发送的传输数据发送到核心网的步骤。

13、一种传输数据的保护系统，其特征在于，包括：用户设备 UE、接入点和核心网节点；

所述 UE 用于在需要发送传输数据时，从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息；

所述 UE 还用于向所述接入点发送所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息；

所述接入点用于向所述核心网节点发送所述保护消息；

所述核心网节点用于在接收到所述保护消息之后，根据所述保护方式的指示消息从其第二预存数据中获取所述全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据。

14、如权利要求 13 所述的保护系统，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥；

所述核心网节点还用于从密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据；

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

15、如权利要求 14 所述的保护系统，其特征在于，所述加密公钥为核心网认证节点的

身份，或者所述加密公钥包含所述核心网节点的身份。

16、如权利要求 13 所述的保护系统，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述 UE 还用于从核心网中获取加密公钥、所述 UE 用于处理传输数据的核心网处理参数，并将所述加密公钥和所述核心网处理参数存储为所述 UE 的第一预存数据；

其中，所述核心网处理参数包括以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

17、如权利要求 15 或 16 所述的保护系统，其特征在于，所述第一预存数据中包括所述加密公钥和所述 GPK_{enc}；

所述 UE 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc}；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密。

18、如权利要求 17 所述的保护系统，其特征在于，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述核心网节点具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到所述 UE 的传输数据。

19、如权利要求 15 或 16 所述的保护系统，其特征在于，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述 UE 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$；

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成对称钥 K3，并将所述传输数据和所述 K3 输入系统函数以获取第四完整性校验码 MAC3；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和

所述 MAC3 进行加密。

20、如权利要求 19 所述的保护系统，其特征在于，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述核心网节点具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$，对所述保护消息进行解密以得到解密消息；

使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$ 生成对称钥 K4；

使用所述 K4、所述 UE 的标识信息和所述解密消息生成第五完整性校验码 MAC4，并当所述 MAC4 与所述 MAC3 相匹配时，获取所述传输数据。

21、如权利要求 15 或 16 所述的保护系统，其特征在于，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$；

所述 UE 具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$；

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig3，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据和所述签名 Sig2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述签名进行加密。

22、如权利要求 21 所述的保护系统，其特征在于，所述第二预存数据中包括所述加密公钥、所述 GPK_{enc}、所述 $SK_{CP_ID_enc}$ 和所述 GPK_{Sig}；

所述核心网节点具体用于：

根据所述加密方式的指示消息确定所述传输数据的保护方式，并使用从所述第二预存数据中获取的所述 GPK_{enc}、所述加密公钥和所述 $SK_{CP_ID_enc}$ 对所述保护消息进行解密；

从所述保护消息解密得到的解密消息中获取所述签名 Sig3，并使用所述 UE 的标识信息和所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，获取所述传输数据。

23、一种传输数据的保护系统，其特征在于，包括：用户设备 UE、接入点和核心网节点；

所述核心网节点用于接收用户面网关下发的传输数据，并从其第二预存数据中获取所述 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥；

所述核心网节点还用于使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述传输数据进行保护以得到保护消息，并将所述保护消息发送给所述接入点；

所述接入点用于将所述保护消息发送给所述 UE；

所述 UE 从其第一预存数据中获取所述所述核心网节点的标识，所述全局公钥和所述

UE 对应的私钥对所述保护消息进行解析以得到所述传输数据。

24、如权利要求 23 所述的保护系统，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥；

所述核心网节点还用于从网络或者密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据；

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

25、如权利要求 23 所述的保护系统，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述 UE 还用于从核心网中获取其标识信息、所述 UE 用于处理传输数据的核心网处理参数，并将所述标识信息和所述核心网处理参数存储为所述 UE 的第一预存数据；

其中，所述核心网处理参数包括以下两组数据中至少一组：第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

26、如权利要求 24 或 25 所述的保护系统，其特征在于，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述核心网节点具体用于：

在接收到所述传输数据之后，从所述第二预存数据中获取所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$；

根据所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$ 生成对称钥 K5，并将所述传输数据和所述 K5 输入系统函数以获取第六完整性校验码 MAC5；

使用所述 K5 对所述传输数据加密得到保护消息。

27、如权利要求 26 所述的保护系统，其特征在于，所述第一预存数据中包括所述 UE 的标识信息、所述核心网节点的标识、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述 UE 具体用于：

从所述第一预存数据中获取所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$，并使用所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 对所述保护消息进行解密以得到解密消息；

使用所述核心网节点的标识信息、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 生成对称钥 K6;

使用所述 K6 对所述保护消息进行解密以得到解密消息;

使用所述 K6 和所述解密消息生成第七完整性校验码 MAC6，并当所述 MAC6 与所述解密消息中携带的 MAC5 相匹配时，获取所述传输数据。

28、一种传输数据的保护方法，其特征在于，包括:

用户设备 UE 接收接入点发送的广播消息，并存储所述广播消息中携带的加密公钥;

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息;

所述 UE 向所述接入点发送所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息。

29、如权利要求 28 所述的保护方法，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥;

所述 UE 接收所述接入点的广播消息之前，所述方法还包括:

所述 UE 从网络或者 KMS 中获取所述 UE 用于处理传输数据的处理参数，并将所述处理参数存储为所述 UE 的第一预存数据;

其中，所述处理参数包括 UE 所属运营商的身份 operator ID1 以及以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

30、如权利要求 29 所述的保护方法，其特征在于，所述第一预存数据中包括所述 operator ID1 和所述 GPK_{Sig};

所述 UE 存储所述广播消息中携带的加密公钥之前，所述方法还包括:

所述 UE 根据接收到的所述广播消息中携带的指示信息确定所述接入点具有数据签名功能，并根据所述广播消息对应的接入点的标识信息确定所述接入点所属的运营商的身份 operator ID2;

将所述 operator ID2 与所述 operator ID1 进行匹配，从所述第一预存数据中查找所述接入点对应的第三全局公钥 $GPK_{Sig}1$;

当所述广播消息中携带签名 Sig1 时，使用所述 $GPK_{Sig}1$ 和所述接入点的标识信息对所述广播消息进行验证;

当所述广播消息验证通过时，确定将所述广播消息携带的所述加密公钥添加至所述第一预存数据中。

31、如权利要求 30 所述的保护方法，其特征在于，所述第一预存数据中包括所述 GPK_{enc}；

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥，并使用所述加密公钥和所述全局公钥对所述传输数据进行保护包括：

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc}；

使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密。

32、如权利要求 30 所述的保护方法，其特征在于，所述第一预存数据中包括所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护包括：

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$；

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成第一对称钥 K1，并将所述传输数据和所述 K1 输入系统函数以获取第三完整性校验码 MAC2；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据以及所述 UE 的标识信息、所述 MAC2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息以及所述 MAC2 进行加密。

33、如权利要求 30 所述的保护方法，其特征在于，所述第一预存数据中包括所述所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$；

所述 UE 在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息包括：

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$；

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig2，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息和所述 Sig2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述 Sig2 进行加密。

34、一种传输数据的保护方法，其特征在于，包括：

接入点发送广播消息，所述广播消息中携带加密公钥；

所述接入点接收用户设备 UE 发送的根据所述加密公钥对传输数据进行保护得到的保护消息，所述保护消息中携带所述 UE 发送的传输数据的保护方式的指示消息；

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据；

所述接入点将解析得到的所述 UE 发送的传输数据发送到核心网中。

35、如权利要求 34 所述的保护方法，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述接入点对应的私钥包括第一私钥和第二私钥；

所述接入点发送广播消息之前，所述方法还包括：

所述接入点从网络或者密钥管理系统 KMS 中获取系统参数，并将所述系统参数存储为所述接入点的第二预存数据；

其中，所述系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第一私钥，或者第二全局公钥和第二私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第一私钥为 IBC 技术的所述接入点对应的数据加密私钥 $SK_{BS_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第二私钥为 IBC 技术的所述接入点对应的数据签名私钥 $SK_{BS_ID_Sig}$。

36、如权利要求 35 所述的保护方法，其特征在于，所述加密公钥为基站 BS 的身份 BS_ID，或者所述加密公钥包含 BS_ID；或者

所述加密公钥包括无线保真 Wi-Fi 切入点 AP 的介质控制子层 MAC 地址，或者 Wi-Fi AP 的服务集标识 SSID；或者

所述加密公钥包括热点 UE 的身份 UE_ID，或者热点 UE 的移动用户身份 IMSI。

37、如权利要求 36 所述的保护方法，其特征在于，所述第二预存数据中包括所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$；

所述接入点发送广播消息之前，所述方法还包括：

所述接入点使用所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$ 对所述广播消息进行签名以得到所述广播消息的签名 Sig1，并在所述广播消息中携带所述接入点具有数据签名功能的指示信息或者所述广播消息的签名 Sig1。

38、如权利要求 36 所述的保护方法，其特征在于，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$、所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$；

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析包括：

所述接入点根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息。

39、如权利要求 36 所述的保护方法，其特征在于，所述第二预存数据中包括加密公钥、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$；

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析包括：

所述接入点根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息；

所述接入点将解析得到的所述 UE 发送的传输数据发送到核心网中包括：

所述接入点从所述解密消息中获取所述保护消息携带的第三完整性保护码 MAC2、UE 的标识信息以及所述传输数据；

使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$ 生成对称钥 K2；

使用所述对称钥 K2、所述 UE 的标识信息和解密得到的传输数据计算第四完整性校验码 MAC3，并当所述 MAC3 与所述 MAC2 相匹配时，将所述 UE 发送的传输数据发送到核心网。

40、如权利要求 36 所述的保护方法，其特征在于，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$ 和所述 GPK_{Sig}；

所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析包括：

根据所述加密方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以获取所述传输数据；

所述接入点将解析得到的所述 UE 发送的传输数据发送到核心网中包括：

从所述保护消息解密得到的解密消息中获取所述 UE 的标识信息和所述签名 Sig2；

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{sig}；

使用所述 UE 的标识信息以及所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，将所述 UE 发送的传输数据发送到核心网。

41、一种传输数据的保护方法，其特征在于，包括：

用户设备 UE 在需要发送传输数据时，从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全

局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息;

所述 UE 向接入点发送所述保护消息，以通过所述接入点将所述保护消息发送给核心网节点，所述保护消息中携带所述传输数据的保护方式的指示消息。

42、如权利要求 41 所述的保护方法，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥;

所述 UE 发送传输数据之前，所述方法还包括:

所述 UE 从核心网中获取加密公钥、所述 UE 用于处理传输数据的核心网处理参数，并将所述加密公钥和所述核心网处理参数存储为所述 UE 的第一预存数据;

其中，所述核心网处理参数包括以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

43、如权利要求 42 所述的保护方法，其特征在于，所述第一预存数据中包括所述加密公钥和所述 GPK_{enc};

所述 UE 从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥，并使用所述加密公钥，以及所述全局公钥对所述传输数据进行保护包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc};

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密。

44、如权利要求 42 所述的保护方法，其特征在于，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$;

所述 UE 从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护包括:

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$;

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成对称钥 K3，并将所述传输数据和所述 K3 输入系统函数以获取第四完整性校验码 MAC3;

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密。

45、如权利要求 42 所述的保护方法，其特征在于，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$；

所述 UE 从其第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护包括：

所述 UE 在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$；

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig3，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据和所述签名 Sig2 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述签名进行加密。

46、一种传输数据的保护方法，其特征在于，包括：

核心网节点接收接入点发送的保护消息，所述保护消息中携带用户设备 UE 发送的所述传输数据的保护方式的指示消息；

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据。

47、如权利要求 46 所述的保护方法，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥；

所述核心网节点接收接入点发送的保护消息之前，所述方法还包括：

所述核心网节点从密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据；

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

48、如权利要求 47 所述的保护方法，其特征在于，所述加密公钥为核心网认证节点的身份，或者所述加密公钥包含所述核心网节点的身份。

49、如权利要求 48 所述的保护方法，其特征在于，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密

码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析包括:

所述核心网节点根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到所述 UE 的传输数据。

50、如权利要求 48 所述的保护方法，其特征在于，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析包括:

所述核心网节点根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$，对所述保护消息进行解密以得到解密消息;

获取所述解密消息中携带的第四完整性校验码 MAC3，并使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$ 生成对称钥 K4;

使用所述 K4、所述 UE 的标识信息和所述解密消息生成第五完整性校验码 MAC4，并当所述 MAC4 与所述 MAC3 相匹配时，获取所述传输数据。

51、如权利要求 48 所述的保护方法，其特征在于，所述第二预存数据中包括所述加密公钥、所述 GPK_{enc}、所述 $SK_{CP_ID_enc}$ 和所述 GPK_{Sig};

所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析包括:

所述核心网节点根据所述加密方式的指示消息确定所述传输数据的保护方式，并使用从所述第二预存数据中获取的所述 GPK_{enc}、所述加密公钥和所述 $SK_{CP_ID_enc}$ 对所述保护消息进行解密;

从所述保护消息解密得到的解密消息中获取所述签名 Sig3，并使用所述 UE 的标识信息和所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，获取所述传输数据。

52、一种传输数据的保护方法，其特征在于，包括:

核心网节点接收用户面网关下发的传输数据，并从其第二预存数据中获取用户设备 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥;

所述核心网节点使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述传输数据进行保护以得到保护消息，并将所述保护消息发送给接入点。

53、如权利要求 52 所述的保护方法，其特征在于，所述全局公钥包括第一全局公钥和

第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥；

所述核心网节点接收用户面网关下发的传输数据之前，所述方法还包括：

所述核心网节点从网络或者密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据；

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

54、如权利要求 53 所述的保护方法，其特征在于，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述核心网节点从其第二预存数据中获取用户设备 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥包括：

所述核心网节点从所述第二预存数据中获取所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$；

所述核心网节点使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述传输数据进行保护以得到保护消息包括：

所述核心网节点根据所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$ 生成对称钥 K5，并将所述传输数据和所述 K5 输入系统函数以获取第六完整性校验码 MAC5；

使用所述 K5 对所述传输数据加密得到保护消息。

55、一种传输数据的保护方法，其特征在于，包括：

用户设备 UE 接收接入点发送的保护消息；

所述 UE 从其第一预存数据中获取核心网节点的标识，基于身份的密码 IBC 技术的全局公钥和所述 UE 对应的私钥对所述保护消息进行解析以得到所述传输数据。

56、如权利要求 55 所述的保护方法，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述 UE 接收接入点发送的保护消息之前，所述方法还包括：

所述 UE 从核心网中获取其标识信息、所述 UE 用于处理传输数据的核心网处理参数，并将所述标识信息和所述核心网处理参数存储为所述 UE 的第一预存数据；

其中，所述核心网处理参数包括以下两组数据中至少一组：第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

57、如权利要求 56 所述的保护方法，其特征在于，所述第一预存数据中包括所述 UE 的标识信息、所述核心网节点的标识、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述 UE 从其第一预存数据中获取核心网节点的标识，基于身份的密码 IBC 技术的全局公钥和所述 UE 对应的私钥对所述保护消息进行解析以得到所述传输数据包括：

所述 UE 从所述第一预存数据中获取所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$，并使用所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 对所述保护消息进行解密以得到解密消息；

使用所述核心网节点的标识信息、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 生成对称钥 K6；

使用所述 K6 对所述保护消息进行解密以得到解密消息；

使用所述 K6 和所述解密消息生成第七完整性校验码 MAC6，并当所述 MAC6 与所述解密消息中携带的第六完整性校验码 MAC5 相匹配时，获取所述传输数据。

58、一种传输数据的保护装置，其特征在于，包括：

接收单元，用于接收接入点发送的广播消息，并存储所述广播消息中携带的加密公钥；

处理单元，用于在需要向所述接入点发送传输数据时，从用户设备 UE 的第一预存数据中获取基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述接收单元接收的所述加密公钥和所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息；

发送单元，用于向所述接入点发送所述处理单元处理的所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息。

59、如权利要求 58 所述的保护装置，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述处理单元还用于：

从网络或者 KMS 中获取所述 UE 用于处理传输数据的处理参数，并将所述处理参数存储为所述 UE 的第一预存数据；

其中，所述处理参数包括 UE 所属运营商的身份 operator ID1 以及以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

60、如权利要求 59 所述的保护装置，其特征在于，所述第一预存数据中包括所述 operator ID1 和所述 GPK_{Sig}；

所述接收单元具体用于：

根据接收到的所述广播消息中携带的指示信息确定所述接入点具有数据签名功能，并

根据所述广播消息对应的接入点的标识信息确定所述接入点所属的运营商的身份 operator ID2;

将所述 operator ID2 与所述 operator ID1 进行匹配，从所述第一预存数据中查找所述接入点对应的第三全局公钥 $GPK_{Sig}1$;

当所述广播消息中携带签名 Sig1 时，使用所述 $GPK_{Sig}1$ 和所述接入点的标识信息对所述广播消息进行验证;

当所述广播消息验证通过时，确定将所述广播消息携带的所述加密公钥添加至所述第一预存数据中。

61、如权利要求 60 所述的保护装置，其特征在于，所述第一预存数据中包括所述 GPK_{enc};

所述处理单元具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc};

使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据进行加密。

62、如权利要求 60 所述的保护装置，其特征在于，所述第一预存数据中包括所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$;

所述处理单元具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$;

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成第一对称钥 K1，并将所述传输数据和所述 K1 输入系统函数以获取第三完整性校验码 MAC2;

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据以及所述 UE 的标识信息、所述 MAC2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息以及所述 MAC2 进行加密。

63、如权利要求 60 所述的保护装置，其特征在于，所述第一预存数据中包括所述所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$;

所述处理单元具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$;

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig2，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据、所述 UE 的标识信息和所述 Sig2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以

及所述 Sig2 进行加密。

64、一种传输数据的保护装置，其特征在于，包括:

发送单元，用于发送广播消息，所述广播消息中携带加密公钥;

接收单元，用于接收用户设备 UE 发送的根据所述发送单元发送的所述加密公钥对传输数据进行保护得到的保护消息，所述保护消息中携带所述 UE 发送的传输数据的保护方式的指示消息;

解析单元，用于根据所述接收单元接收的所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据;

所述发送单元，还用于将所述解析单元解析得到的所述 UE 发送的传输数据发送到核心网中。

65、如权利要求 64 所述的保护装置，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述接入点对应的私钥包括第一私钥和第二私钥;

所述解析单元还用于:

从网络或者密钥管理系统 KMS 中获取系统参数，并将所述系统参数存储为所述接入点的第二预存数据;

其中，所述系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第一私钥，或者第二全局公钥和第二私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第一私钥为 IBC 技术的所述接入点对应的数据加密私钥 $SK_{BS_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第二私钥为 IBC 技术的所述接入点对应的数据签名私钥 $SK_{BS_ID_Sig}$。

66、如权利要求 65 所述的保护装置，其特征在于，所述加密公钥为基站 BS 的身份 BS_ID，或者所述加密公钥包含 BS_ID; 或者

所述加密公钥包括无线保真 Wi-Fi 切入点 AP 的介质控制子层 MAC 地址，或者 Wi-Fi AP 的服务集标识 SSID; 或者

所述加密公钥包括热点 UE 的身份 UE_ID，或者热点 UE 的移动用户身份 IMSI。

67、如权利要求 66 所述的保护装置，其特征在于，所述第二预存数据中包括所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$;

所述发送单元具体用于:

使用所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$ 对所述广播消息进行签名以得到所述广播消息的签名 Sig1，并在所述广播消息中携带所述接入点具有数据签名功能的指示信息或者所述广播消息的签名 Sig1。

68、如权利要求 66 所述的保护装置，其特征在于，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$、所述 GPK_{Sig} 和所述 $SK_{BS_ID_Sig}$；

所述解析单元具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息。

69、如权利要求 66 所述的保护装置，其特征在于，所述第二预存数据中包括加密公钥、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$；

所述解析单元具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到解密消息；

所述发送单元具体用于：

从所述解析单元解析得到的所述解密消息中获取所述保护消息携带的第三完整性保护码 MAC2、UE 的标识信息以及所述传输数据；

使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$ 生成对称钥 K2；

使用所述对称钥 K2、所述 UE 的标识信息和解密得到的传输数据计算第四完整性校验码 MAC3，并当所述 MAC3 与所述 MAC2 相匹配时，将所述 UE 发送的传输数据发送到核心网。

70、如权利要求 66 所述的保护装置，其特征在于，所述第二预存数据中包括所述 GPK_{enc}、所述 $SK_{BS_ID_enc}$ 和所述 GPK_{Sig}；

所述解析单元具体用于：

根据所述加密方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{BS_ID_enc}$，并使用所述 $SK_{BS_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以获取所述传输数据；

所述发送单元具体用于：

从所述保护消息解密得到的解密消息中获取所述 UE 的标识信息和所述签名 Sig2；

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 GPK_{sig}；

使用所述 UE 的标识信息以及所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，将所述 UE 发送的传输数据发送到核心网。

71、一种传输数据的保护装置，其特征在于，包括：

保护单元，用于在需要发送传输数据时，从用户设备的第一预存数据中获取加密公钥、基于身份的密码 IBC 技术的全局公钥或者所述 UE 对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述 UE 对应的私钥对所述传输数据进行保护以得到保护消息；

发送单元，用于向接入点发送所述保护单元处理得到的所述保护消息，以通过所述接入点将所述保护消息发送给核心网节点，所述保护消息中携带所述传输数据的保护方式的指示消息。

72、如权利要求 71 所述的保护装置，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述保护单元还用于：

从核心网中获取加密公钥、所述 UE 用于处理传输数据的核心网处理参数，并将所述加密公钥和所述核心网处理参数存储为所述 UE 的第一预存数据；

其中，所述核心网处理参数包括以下三组数据中至少一组：第一全局公钥，或者第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

73、如权利要求 72 所述的保护装置，其特征在于，所述第一预存数据中包括所述加密公钥和所述 GPK_{enc}；

所述保护单元具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥和所述 GPK_{enc}；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据进行加密。

74、如权利要求 72 所述的保护装置，其特征在于，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述保护单元具体用于：

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$；

根据所述加密公钥、所述 GPK_{enc} 以及所述 $SK_{UE_ID_enc}$ 生成对称钥 K3，并将所述传输数据和所述 K3 输入系统函数以获取第四完整性校验码 MAC3；

使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密得到保护消息；

其中，所述传输数据的保护方式为使用所述加密公钥和所述 GPK_{enc} 对所述传输数据和所述 MAC3 进行加密。

75、如权利要求 72 所述的保护装置，其特征在于，所述第一预存数据中包括所述加密公钥、所述 GPK_{enc} 和 $SK_{UE_ID_Sig}$；

所述保护单元具体用于:

在需要向所述接入点发送传输数据时，从所述第一预存数据中获取所述加密公钥、所述 GPK_{enc}、所述 GPK_{sig} 以及所述 $SK_{UE_ID_Sig}$;

根据所述 GPK_{sig} 和所述 $SK_{UE_ID_Sig}$ 对所述传输数据进行签名以得到签名 Sig3，并使用所述加密公钥、所述 GPK_{enc} 对所述传输数据和所述签名 Sig2 进行加密得到保护消息;

其中，所述传输数据的保护方式为使用所述加密公钥、所述 GPK_{enc} 对所述传输数据以及所述签名进行加密。

76、一种传输数据的保护装置，其特征在于，包括:

接收单元，用于接收接入点发送的保护消息，所述保护消息中携带用户设备 UE 发送的所述传输数据的保护方式的指示消息;

解析单元，用于根据所述接收单元接收的所述保护方式的指示消息从其第二预存数据中获取基于身份的密码 IBC 技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析以得到所述 UE 发送的传输数据。

77、如权利要求 76 所述的保护装置，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥;

所述解析单元还用于:

从密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据;

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥;

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc};

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$;

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig};

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

78、如权利要求 77 所述的保护装置，其特征在于，所述加密公钥为核心网认证节点的身份，或者所述加密公钥包含所述核心网节点的身份。

79、如权利要求 78 所述的保护装置，其特征在于，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$;

所述解析单元具体用于:

根据所述保护方式的指示消息确定所述传输数据的保护方式，并从所述第二预存数据中获取所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc}，并使用所述 $SK_{CP_ID_enc}$ 和所述 GPK_{enc} 对所述保护消息进行解密以得到所述 UE 的传输数据。

80、如权利要求 78 所述的保护装置，其特征在于，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述解析单元具体用于：

根据所述保护方式的指示消息确定所述传输数据的保护方式，从所述第二预存数据中获取所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$，对所述保护消息进行解密以得到解密消息；

获取所述解密消息中携带的第四完整性校验码 MAC3，并使用所述 UE 的标识信息、所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$ 生成对称钥 K4；

使用所述 K4、所述 UE 的标识信息和所述解密消息生成第五完整性校验码 MAC4，并当所述 MAC4 与所述 MAC3 相匹配时，获取所述传输数据。

81、如权利要求 78 所述的保护装置，其特征在于，所述第二预存数据中包括所述加密公钥、所述 GPK_{enc}、所述 $SK_{CP_ID_enc}$ 和所述 GPK_{Sig}；

所述解析单元具体用于：

根据所述加密方式的指示消息确定所述传输数据的保护方式，并使用从所述第二预存数据中获取的所述 GPK_{enc}、所述加密公钥和所述 $SK_{CP_ID_enc}$ 对所述保护消息进行解密；

从所述保护消息解密得到的解密消息中获取所述签名 Sig3，并使用所述 UE 的标识信息和所述 GPK_{sig} 对所述保护消息进行验证，当所述保护消息验证成功时，获取所述传输数据。

82、一种传输数据的保护装置，其特征在于，包括：

接收单元，用于接收用户面网关下发的传输数据；

处理单元，用于从核心网节点的第二预存数据中获取用户设备 UE 的标识信息、基于身份的密码 IBC 技术的全局公钥以及所述核心网节点对应的私钥，并使用所述 UE 的标识信息、所述全局公钥和所述私钥对所述接收单元接收的所述传输数据进行保护以得到保护消息；

发送单元，用于将所述处理单元处理得到的所述保护消息发送给接入点。

83、如权利要求 82 所述的保护装置，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述核心网节点对应的私钥包括第五私钥和第六私钥；

所述处理单元还用于：

从网络或者密钥管理系统 KMS 中获取核心网系统参数，并将所述核心网系统参数存储为所述核心网接入点的第二预存数据；

其中，所述核心网系统参数包括加密公钥以及以下两组数据中至少一组：第一全局公钥和第五私钥，或者第二全局公钥和第六私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第五私钥为 IBC 技术的所述核心网节点对应的数据加密私钥 $SK_{CP_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第六私钥为 IBC 技术的所述核心网节点对应的数据签名私钥 $SK_{CP_ID_Sig}$。

84、如权利要求 83 所述的保护装置，其特征在于，所述第二预存数据中包括所述 GPK_{enc} 和所述 $SK_{CP_ID_enc}$；

所述处理单元具体用于：

从所述第二预存数据中获取所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$；

根据所述 UE 的标识信息、所述 GPK_{enc} 以及所述 $SK_{CP_ID_enc}$ 生成对称钥 K5，并将所述传输数据和所述 K5 输入系统函数以获取第六完整性校验码 MAC5；

使用所述 K5 对所述传输数据加密得到保护消息。

85、一种传输数据的保护装置，其特征在于，包括：

接收单元，用于接收接入点发送的保护消息；

解析单元，用于从用户设备的第一预存数据中获取核心网节点的标识，基于身份的密码 IBC 技术的全局公钥和所述 UE 对应的私钥对所述保护消息进行解析以得到所述传输数据。

86、如权利要求 85 所述的保护装置，其特征在于，所述全局公钥包括第一全局公钥和第二全局公钥，所述 UE 对应的私钥包括第三私钥和第四私钥；

所述解析单元还用于：

从核心网中获取其标识信息、所述 UE 用于处理传输数据的核心网处理参数，并将所述标识信息和所述核心网处理参数存储为所述 UE 的第一预存数据；

其中，所述核心网处理参数包括以下两组数据中至少一组：第一全局公钥和第三私钥，或者第二全局公钥和第四私钥；

所述第一全局公钥为 IBC 技术的数据加密全局公钥 GPK_{enc}；

所述第三私钥为 IBC 技术的所述 UE_ID 对应的数据加密私钥 $SK_{UE_ID_enc}$；

所述第二全局公钥为 IBC 技术的数据签名全局公钥 GPK_{Sig}；

所述第四私钥为 IBC 技术的所述 UE_ID 对应的数据签名私钥 $SK_{UE_ID_Sig}$。

87、如权利要求 86 所述的保护装置，其特征在于，所述第一预存数据中包括所述 UE 的标识信息、所述核心网节点的标识、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$；

所述解析单元具体用于：

从所述第一预存数据中获取所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$，并使用所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 对所述保护消息进行解密以得到解密消息；

使用所述核心网节点的标识信息、所述 GPK_{enc} 和所述 $SK_{UE_ID_enc}$ 生成对称钥 K6；

使用所述 K6 对所述保护消息进行解密以得到解密消息；

使用所述 K6 和所述解密消息生成第七完整性校验码 MAC6，并当所述 MAC6 与所述解密消息中携带的 MAC5 相匹配时，获取所述传输数据。

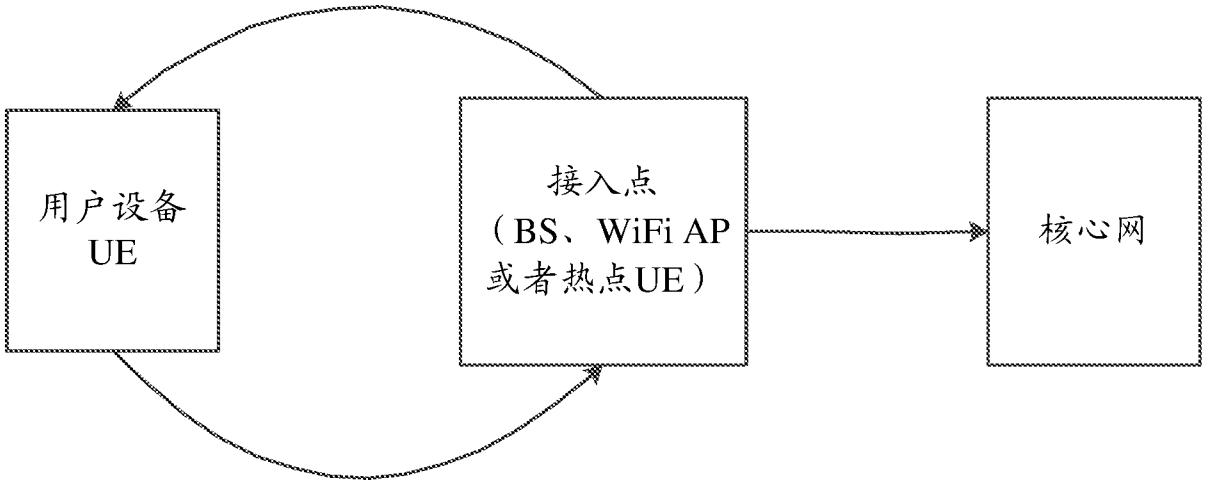


图 1

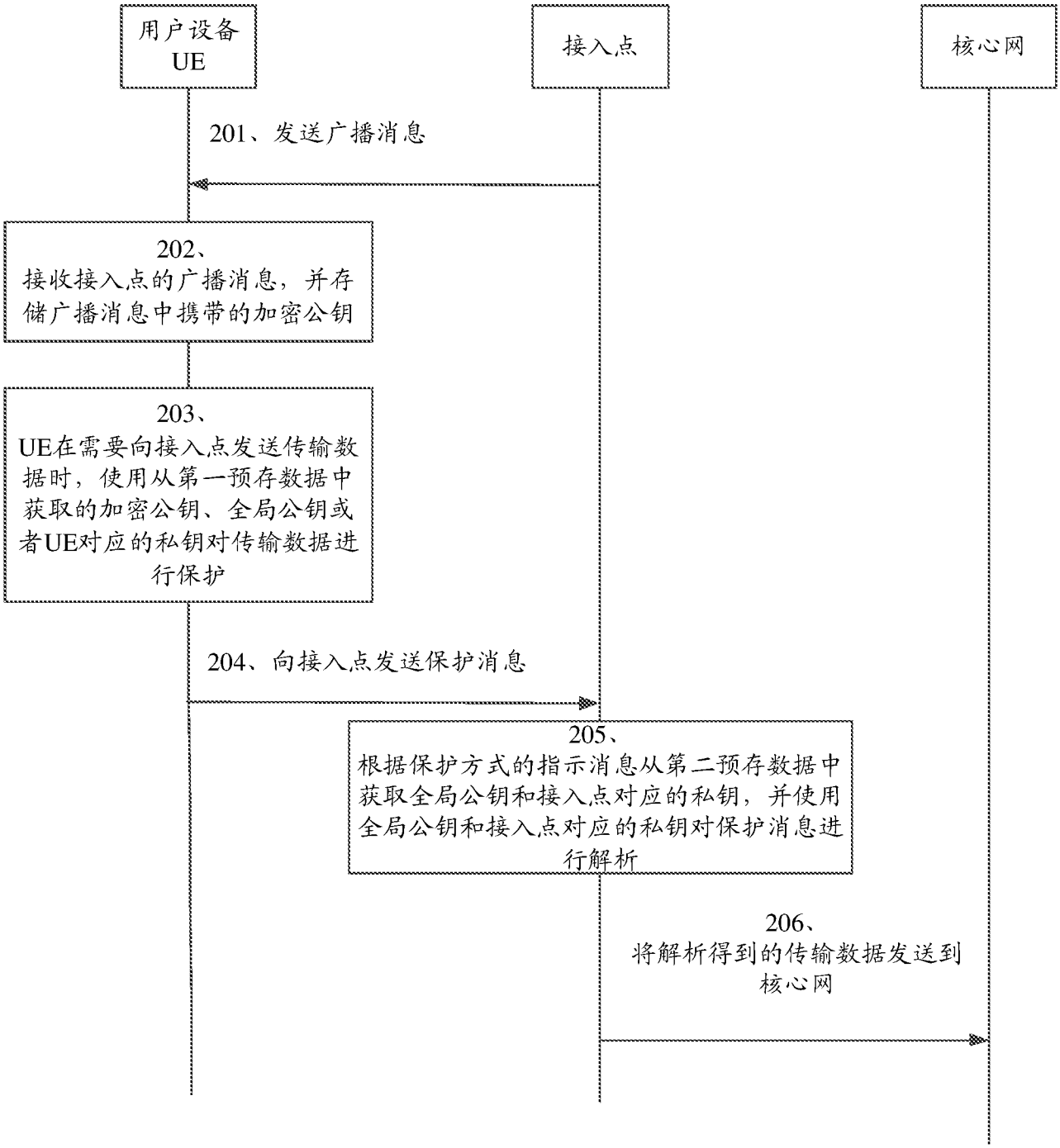

用户设备
UE
接入点
核心网
201、发送广播消息
202、
接收接入点的广播消息，并存储广播消息中携带的加密公钥
203、
UE在需要向接入点发送传输数据时，使用从第一预存数据中获取的加密公钥、全局公钥或者UE对应的私钥对传输数据进行保护
204、向接入点发送保护消息
205、
根据保护方式的指示消息从第二预存数据中获取全局公钥和接入点对应的私钥，并使用全局公钥和接入点对应的私钥对保护消息进行解析
206、
将解析得到的传输数据发送到核心网

图 2

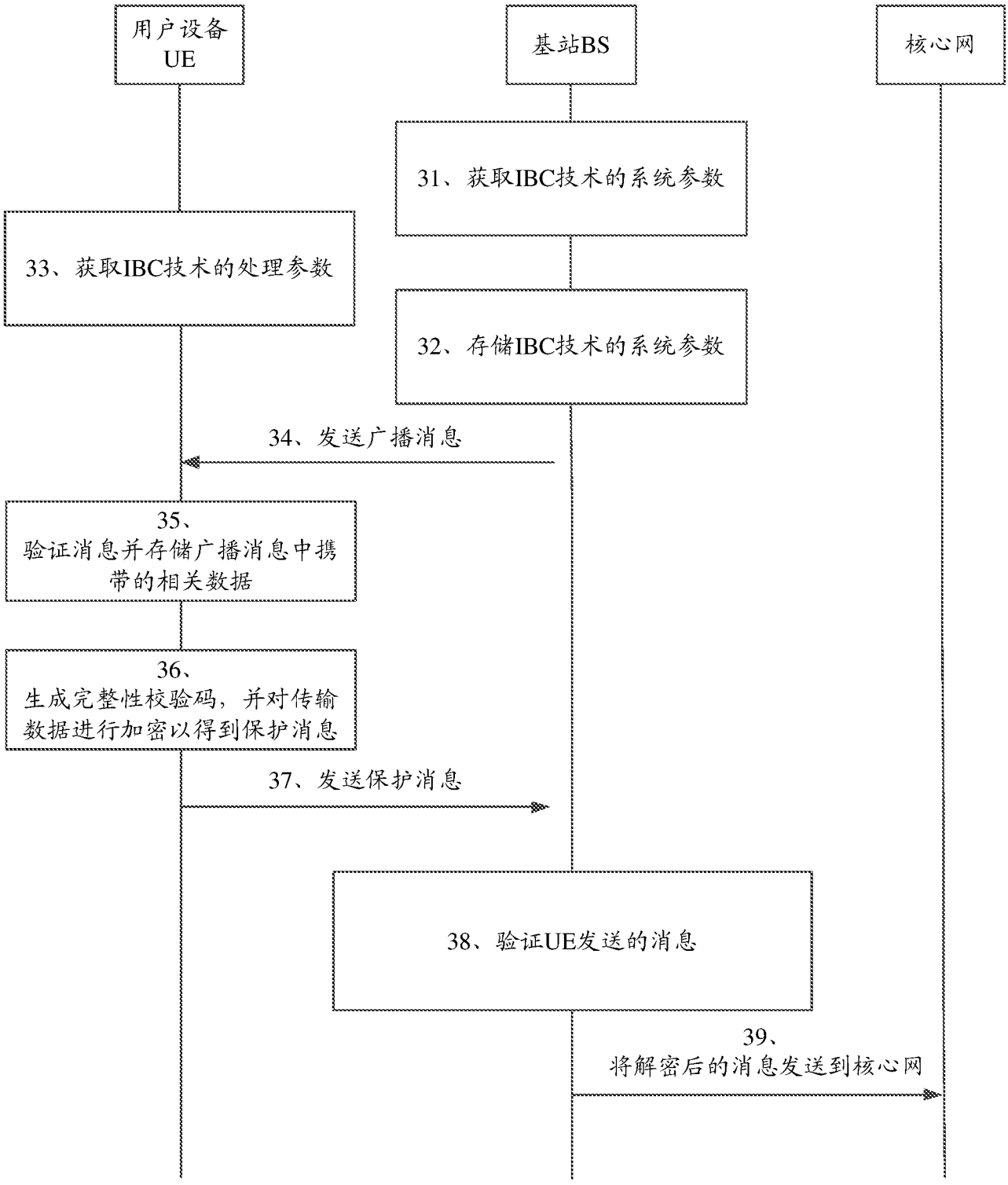

用户设备
UE
基站BS
核心网
31、获取IBC技术的系统参数
33、获取IBC技术的处理参数
32、存储IBC技术的系统参数
34、发送广播消息
35、
验证消息并存储广播消息中携带的相关数据
36、
生成完整性校验码，并对传输数据进行加密以得到保护消息
37、发送保护消息
38、验证UE发送的消息
39、
将解密后的消息发送到核心网

图 3

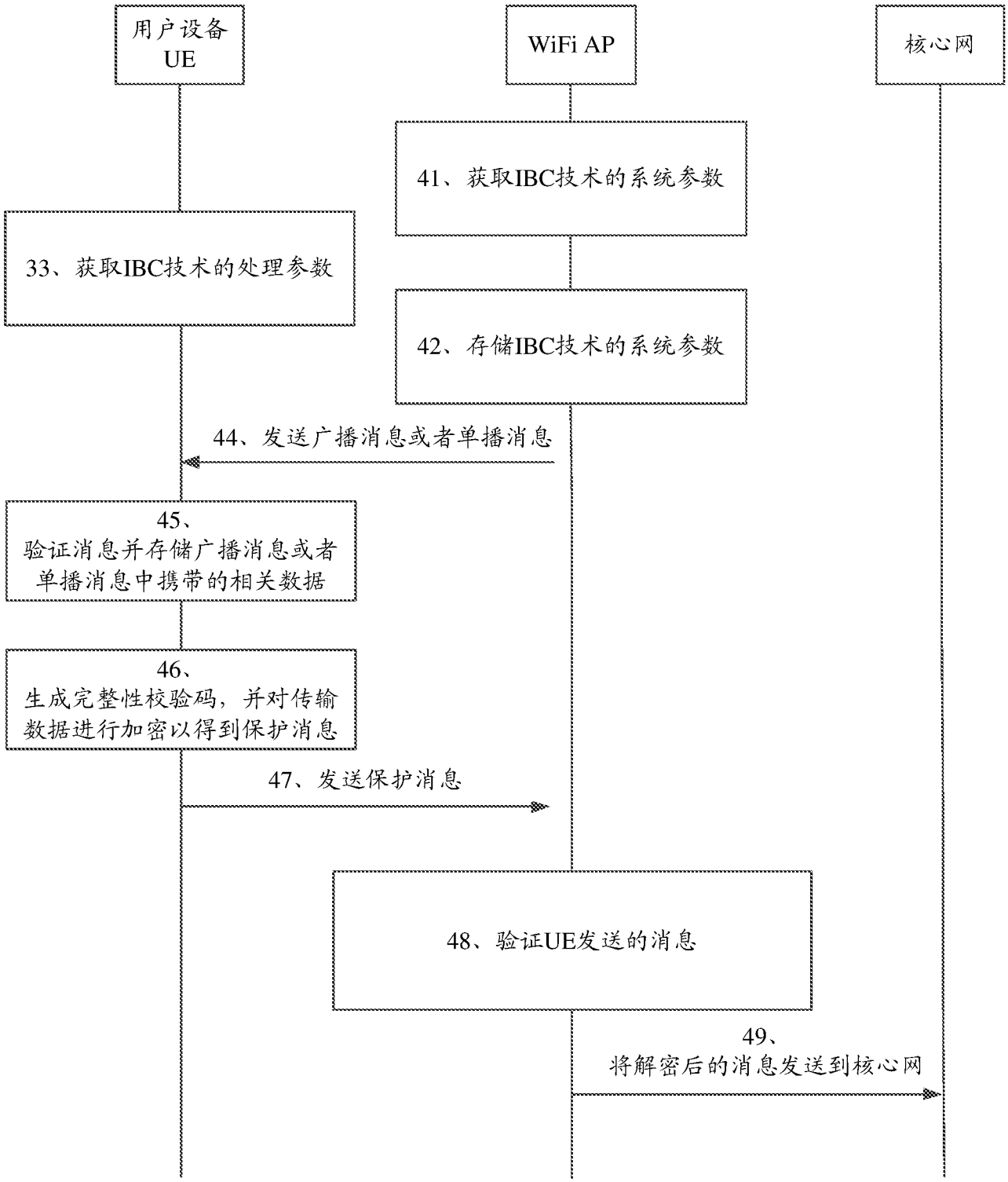

用户设备
UE
WiFi AP
核心网
41、获取IBC技术的系统参数
33、获取IBC技术的处理参数
42、存储IBC技术的系统参数
44、发送广播消息或者单播消息
45、
验证消息并存储广播消息或者
单播消息中携带的相关数据
46、
生成完整性校验码，并对传输
数据进行加密以得到保护消息
47、发送保护消息
48、验证UE发送的消息
49、
将解密后的消息发送到核心网

图 4

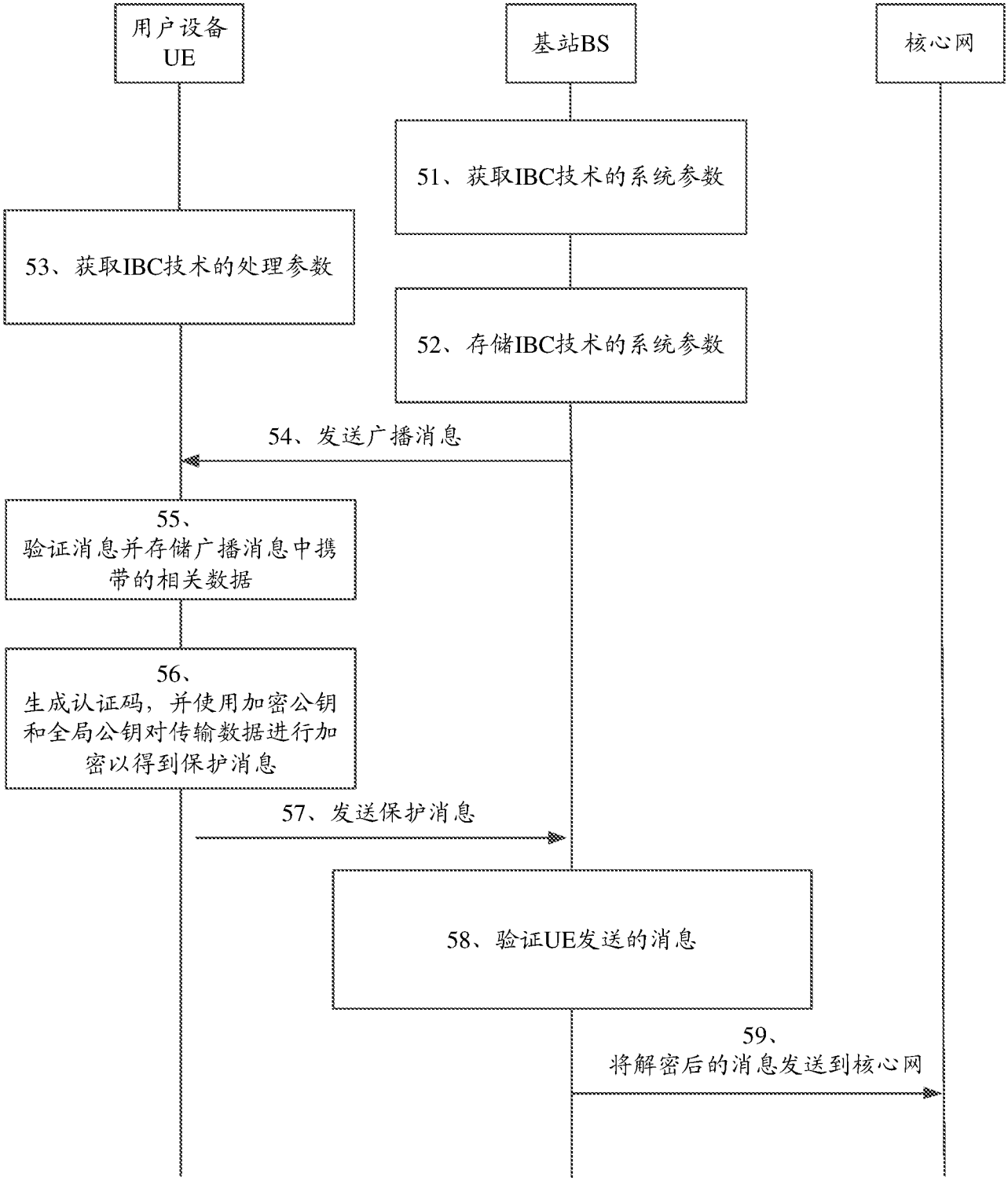

用户设备
UE
基站BS
核心网
51、获取IBC技术的系统参数
53、获取IBC技术的处理参数
52、存储IBC技术的系统参数
54、发送广播消息
55、
验证消息并存储广播消息中携带的相关数据
56、
生成认证码，并使用加密公钥和全局公钥对传输数据进行加密以得到保护消息
57、发送保护消息
58、验证UE发送的消息
59、
将解密后的消息发送到核心网

图 5

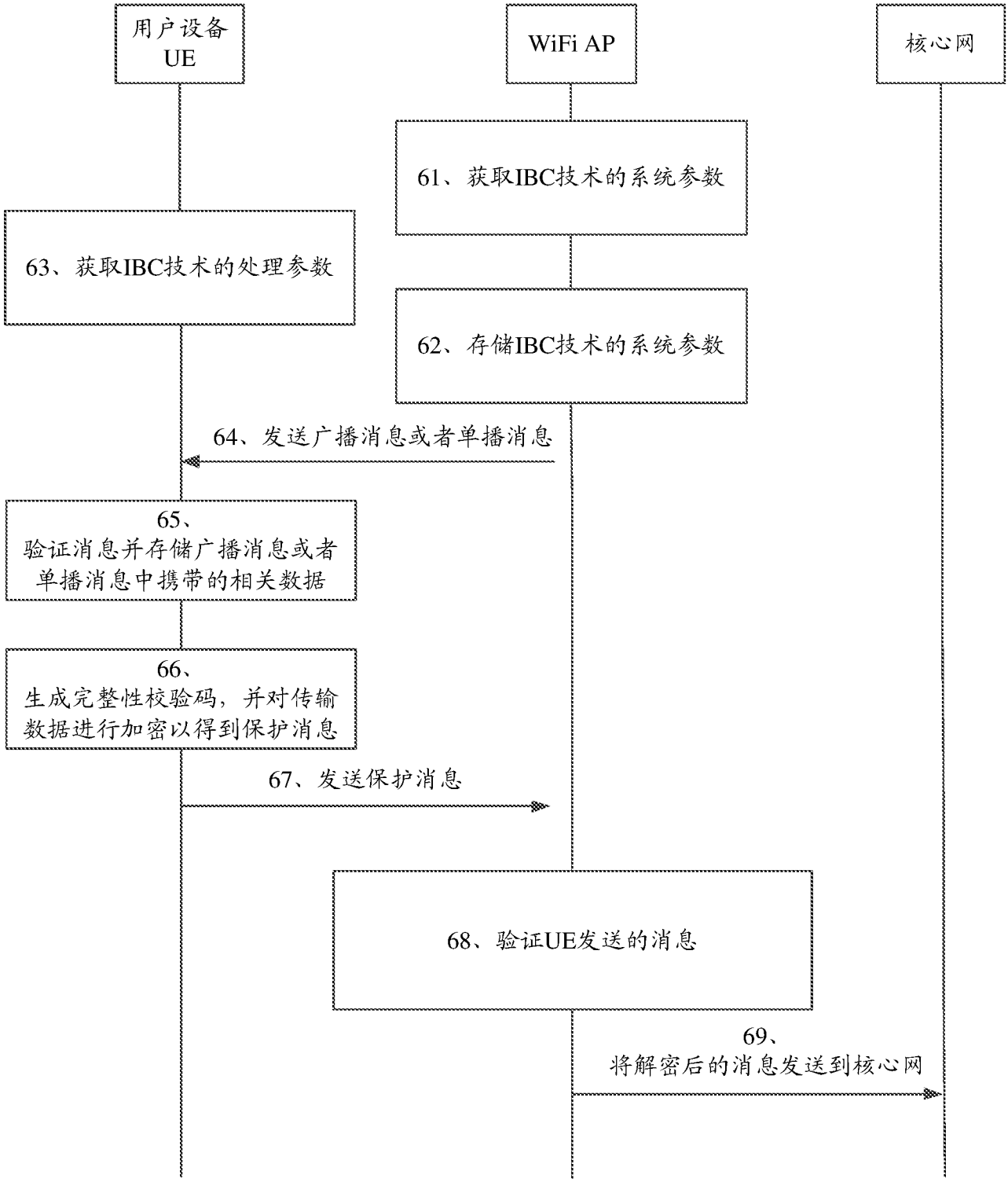

用户设备
UE
WiFi AP
核心网
61、获取IBC技术的系统参数
63、获取IBC技术的处理参数
62、存储IBC技术的系统参数
64、发送广播消息或者单播消息
65、
验证消息并存储广播消息或者
单播消息中携带的相关数据
66、
生成完整性校验码，并对传输
数据进行加密以得到保护消息
67、发送保护消息
68、验证UE发送的消息
69、
将解密后的消息发送到核心网

图 6

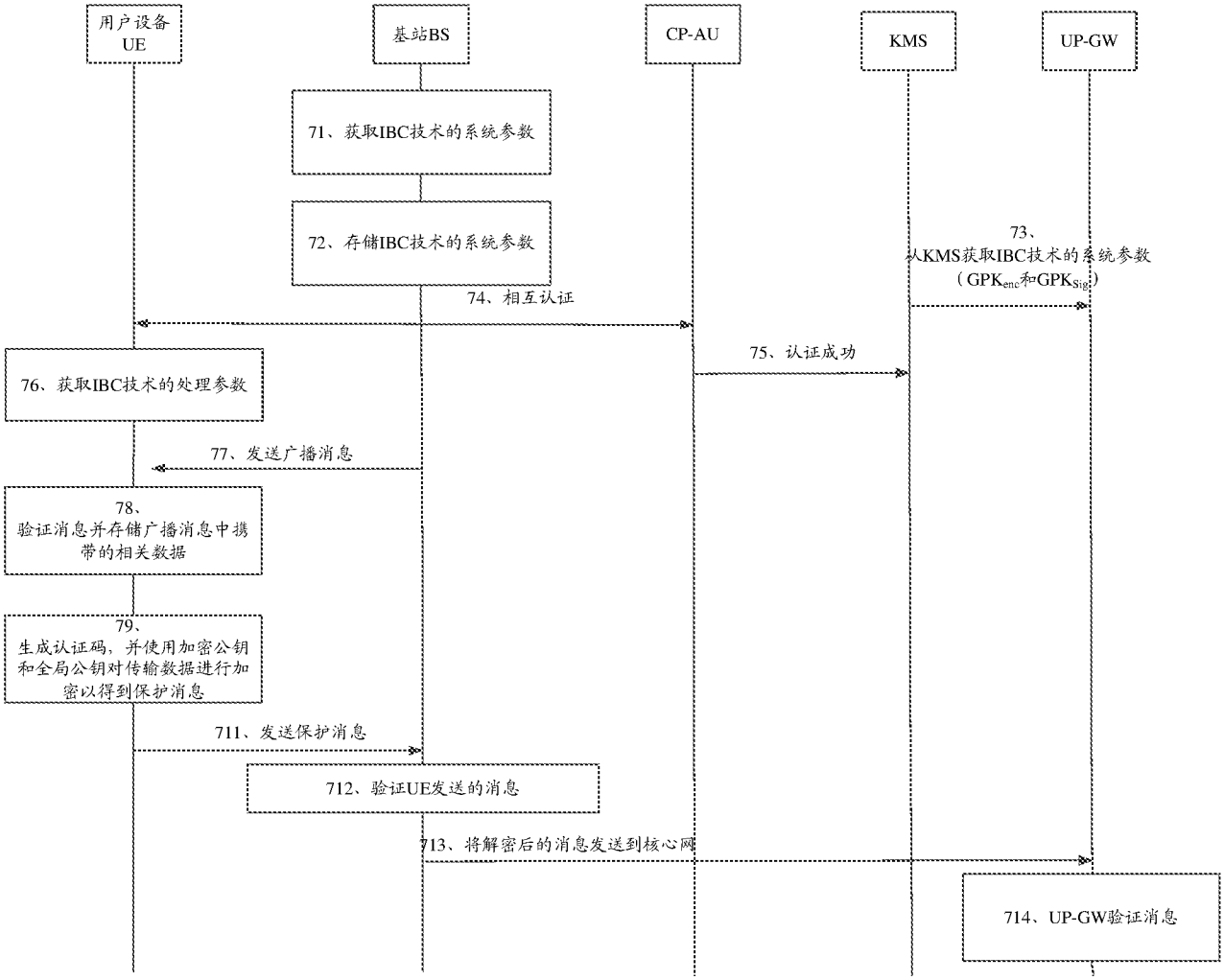

用户设备
UE
基站BS
CP-AU
KMS
UP-GW
71、获取IBC技术的系统参数
72、存储IBC技术的系统参数
73、
从KMS获取IBC技术的系统参数
（GPK_{enc}和GPK_{Sig}）
74、相互认证
75、认证成功
76、获取IBC技术的处理参数
77、发送广播消息
78、
验证消息并存储广播消息中携带的相关数据
79、
生成认证码，并使用加密公钥和全局公钥对传输数据进行加密以得到保护消息
711、发送保护消息
712、验证UE发送的消息
713、将解密后的消息发送到核心网
714、UP-GW验证消息

图 7

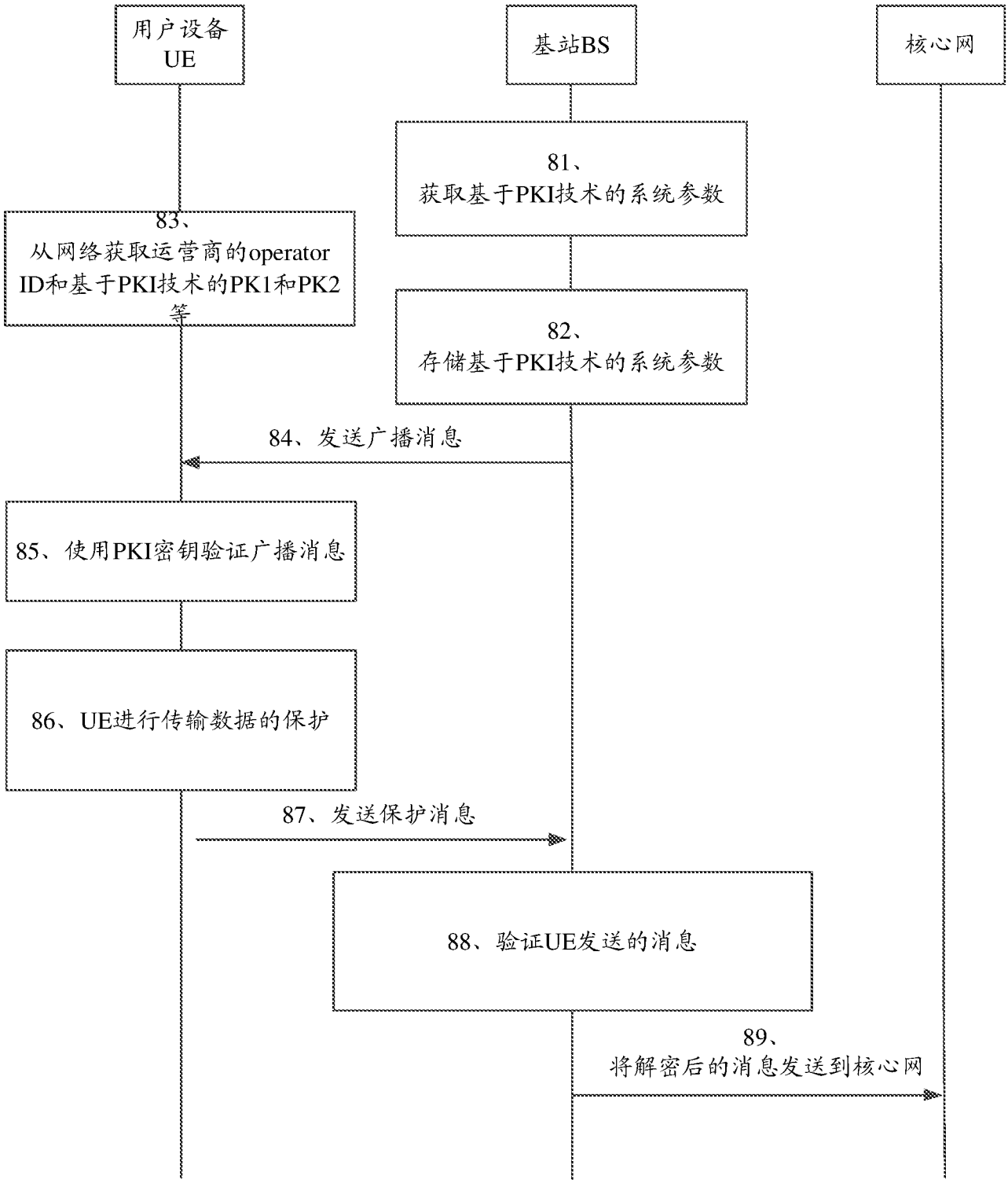

用户设备
UE
基站BS
核心网
81、
获取基于PKI技术的系统参数
83、
从网络获取运营商的operator ID和基于PKI技术的PK1和PK2等
82、
存储基于PKI技术的系统参数
84、发送广播消息
85、使用PKI密钥验证广播消息
86、UE进行传输数据的保护
87、发送保护消息
88、验证UE发送的消息
89、
将解密后的消息发送到核心网

图 8

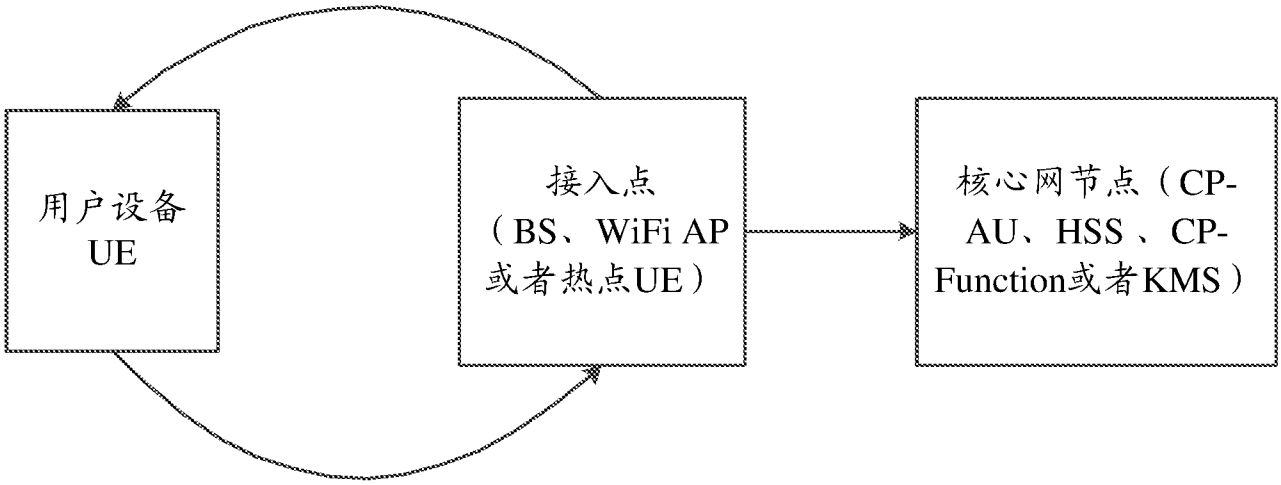

用户设备
UE
接入点
（BS、WiFi AP
或者热点UE）
核心网节点（CP-
AU、HSS 、CP-
Function或者KMS）

图 9

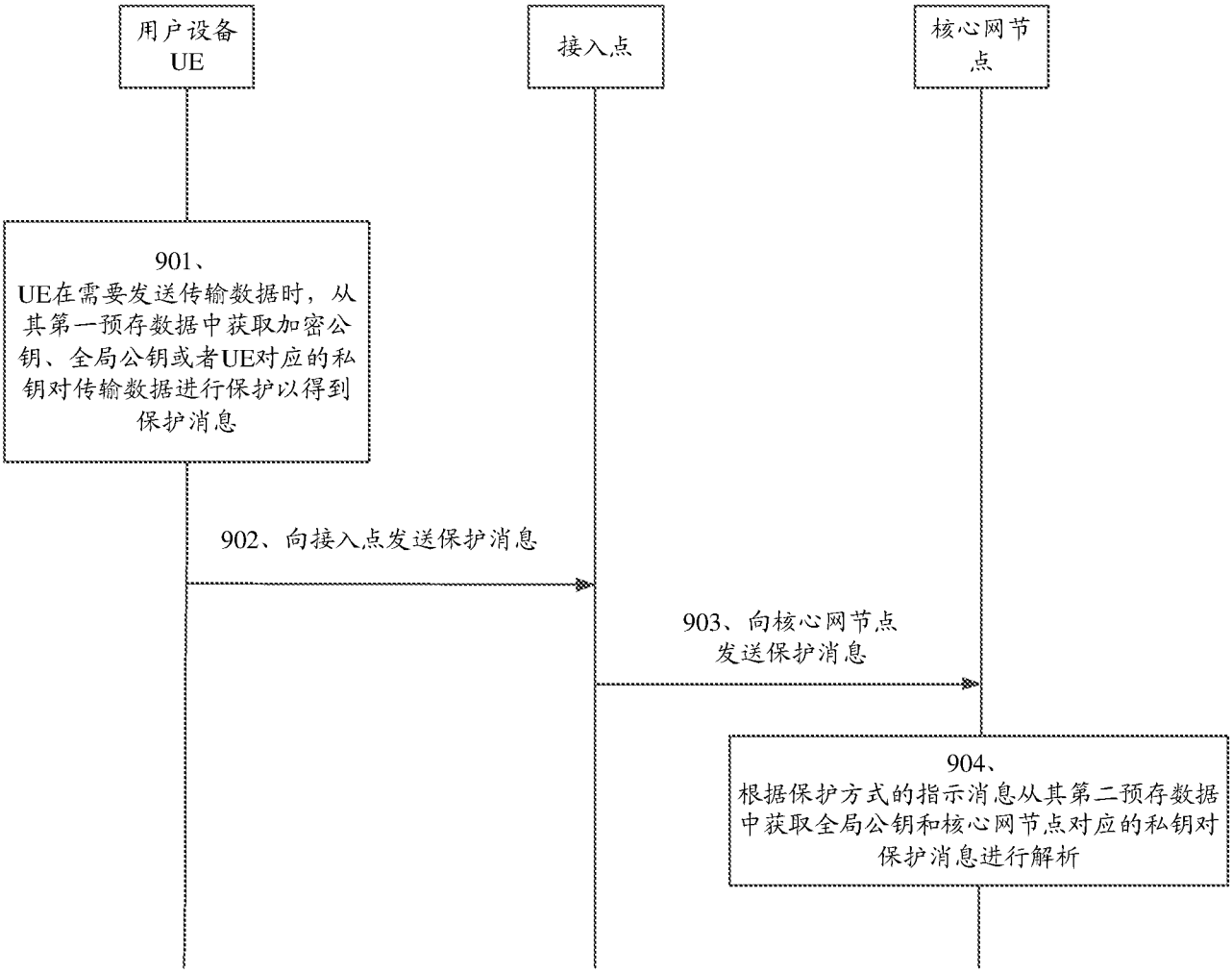

用户设备
UE
接入点
核心网节
点
901、
UE在需要发送传输数据时，从
其第一预存数据中获取加密公
钥、全局公钥或者UE对应的私
钥对传输数据进行保护以得到
保护消息
902、向接入点发送保护消息
903、向核心网节点
发送保护消息
904、
根据保护方式的指示消息从其第二预存数据
中获取全局公钥和核心网节点对应的私钥对
保护消息进行解析

图 10

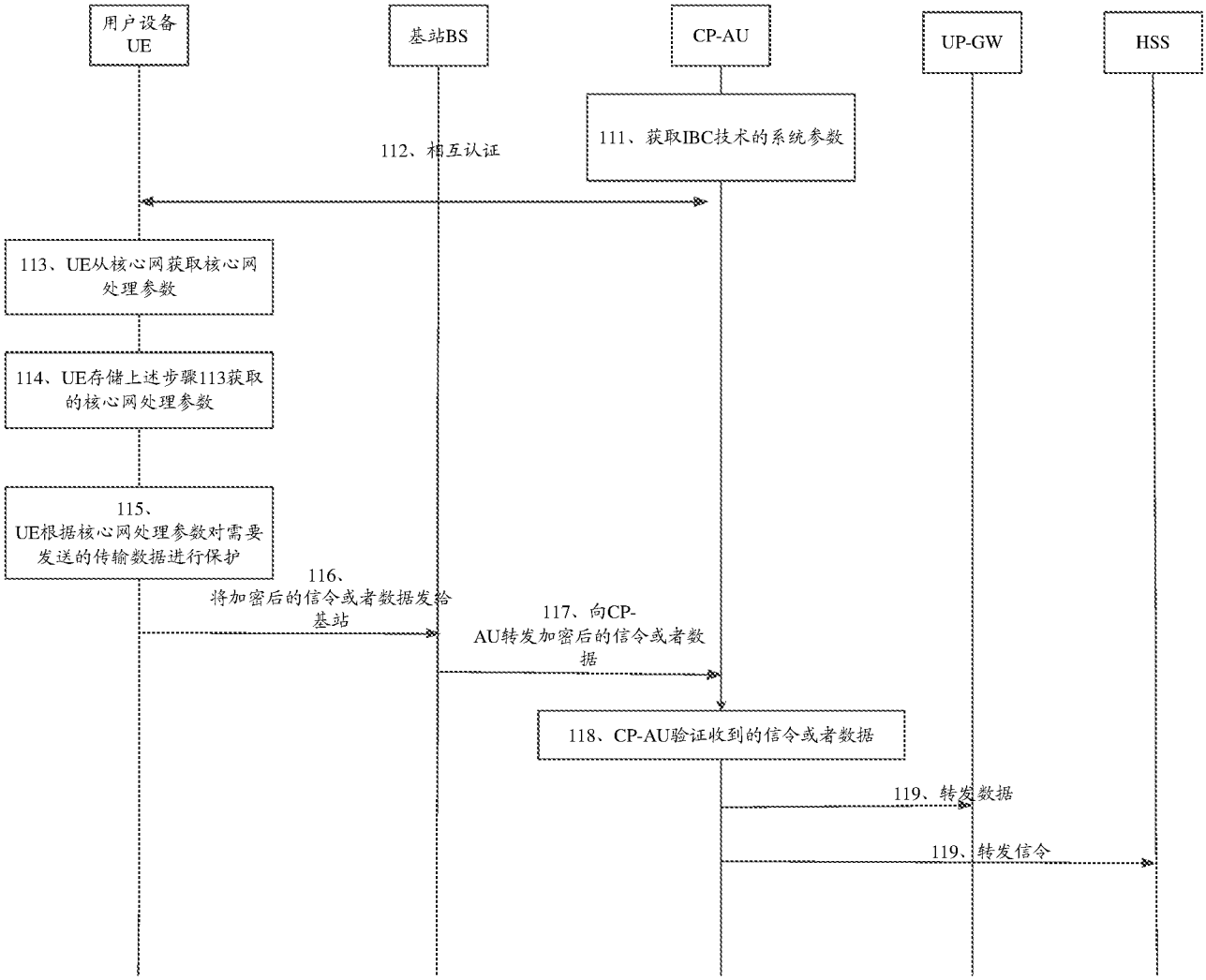

用户设备
UE
基站BS
CP-AU
UP-GW
HSS
111、获取IBC技术的系统参数
112、相互认证
113、UE从核心网获取核心网处理参数
114、UE存储上述步骤113获取的核心网处理参数
115、
UE根据核心网处理参数对需要发送的传输数据进行保护
116、
将加密后的信令或者数据发给基站
117、向CP-AU转发加密后的信令或者数据
118、CP-AU验证收到的信令或者数据
119、转发数据
119、转发信令

图 11

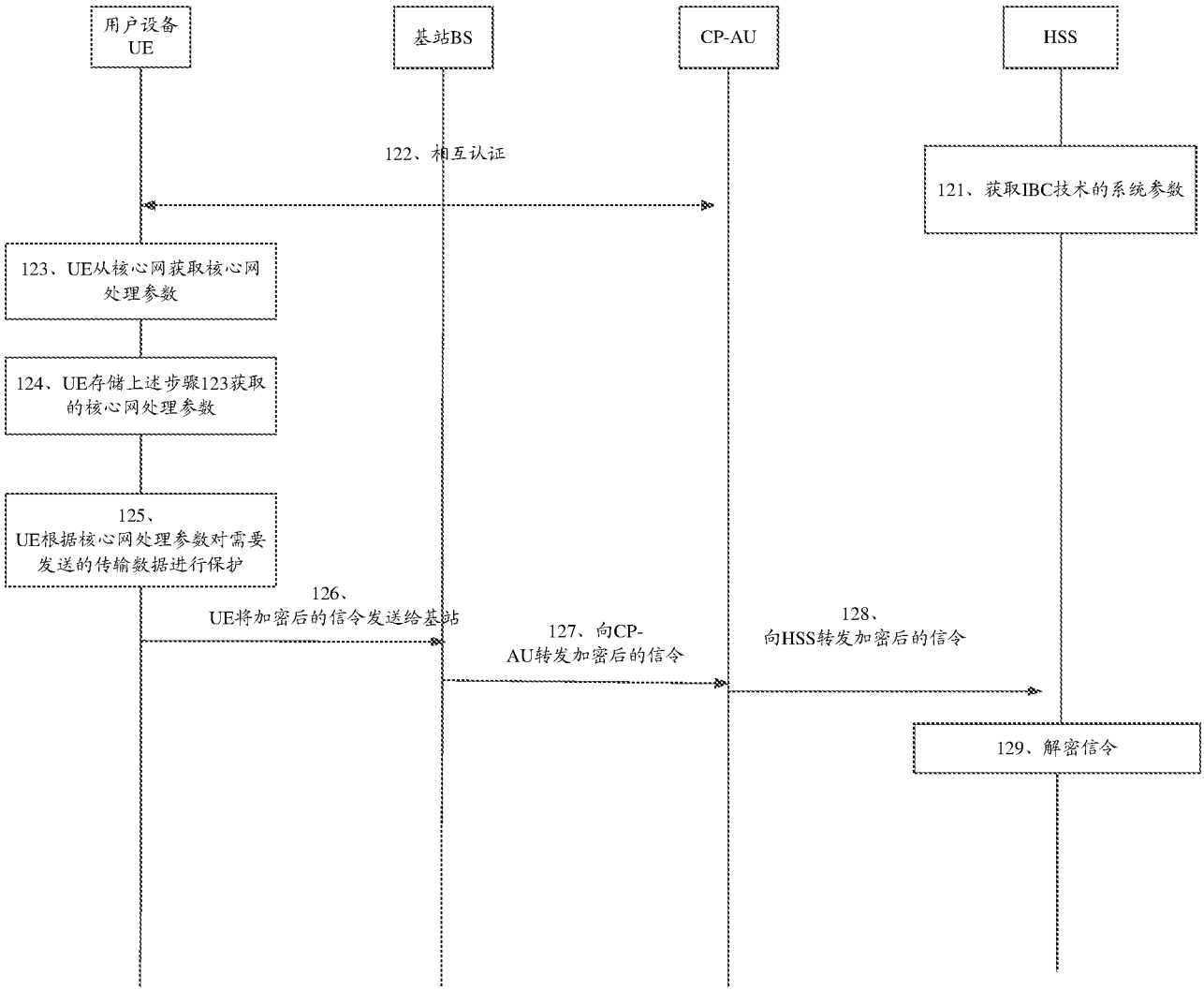

用户设备
UE
基站BS
CP-AU
HSS
122、相互认证
121、获取IBC技术的系统参数
123、UE从核心网获取核心网处理参数
124、UE存储上述步骤123获取的核心网处理参数
125、
UE根据核心网处理参数对需要发送的传输数据进行保护
126、
UE将加密后的信令发送给基站
127、向CP-
AU转发加密后的信令
128、
向HSS转发加密后的信令
129、解密信令

图 12

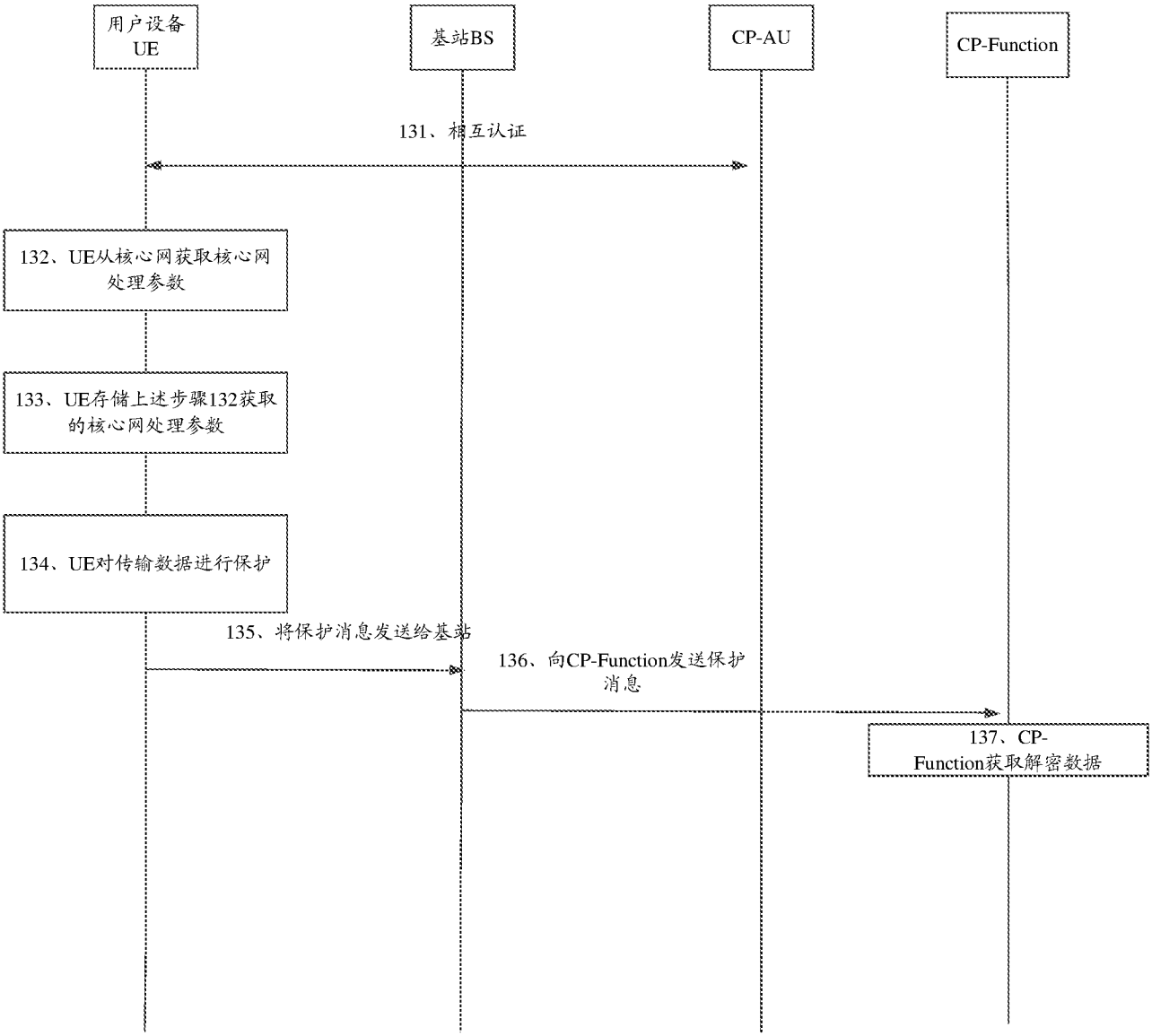

用户设备
UE
基站BS
CP-AU
CP-Function
131、相互认证
132、UE从核心网获取核心网处理参数
133、UE存储上述步骤132获取的核心网处理参数
134、UE对传输数据进行保护
135、将保护消息发送给基站
136、向CP-Function发送保护消息
137、CP-Function获取解密数据

图 13

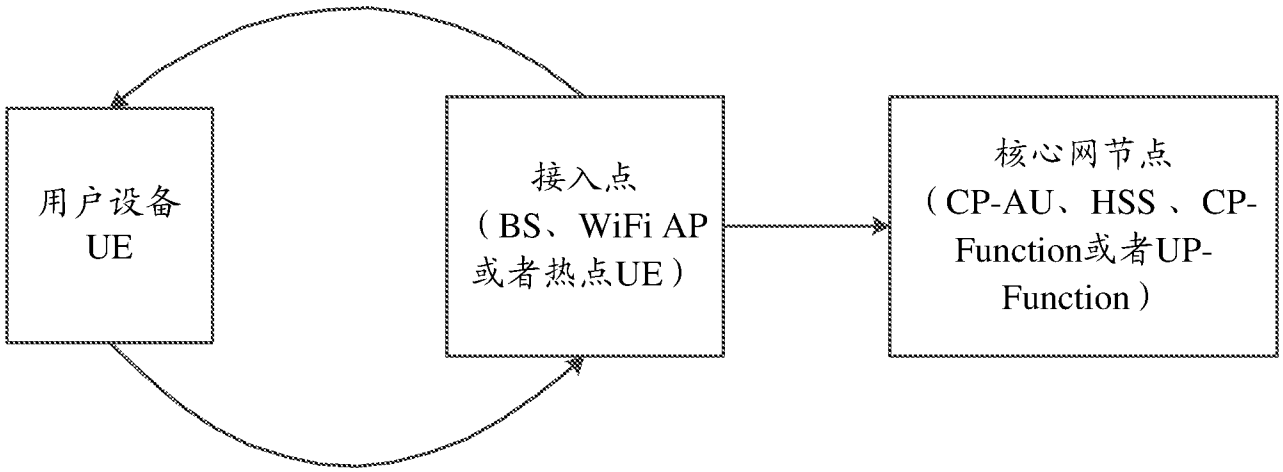

用户设备
UE
接入点
（BS、WiFi AP
或者热点UE）
核心网节点
（CP-AU、HSS 、CP-Function或者UP-Function）

图 14

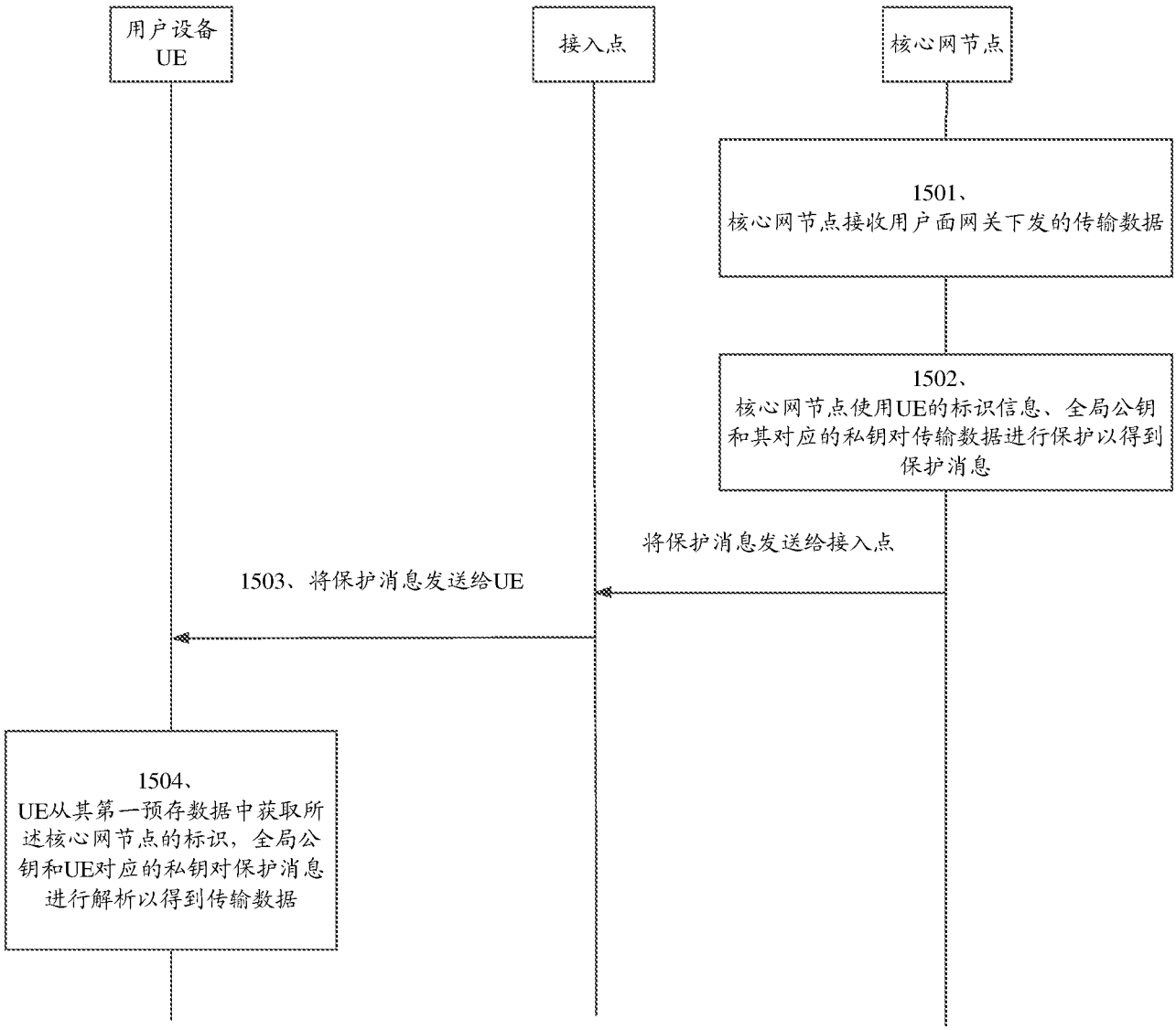

用户设备
UE
接入点
核心网节点
1501、
核心网节点接收用户面网关下发的传输数据
1502、
核心网节点使用UE的标识信息、全局公钥和其对应的私钥对传输数据进行保护以得到保护消息
将保护消息发送给接入点
1503、将保护消息发送给UE
1504、
UE从其第一预存数据中获取所述核心网节点的标识，全局公钥和UE对应的私钥对保护消息进行解析以得到传输数据

图 15

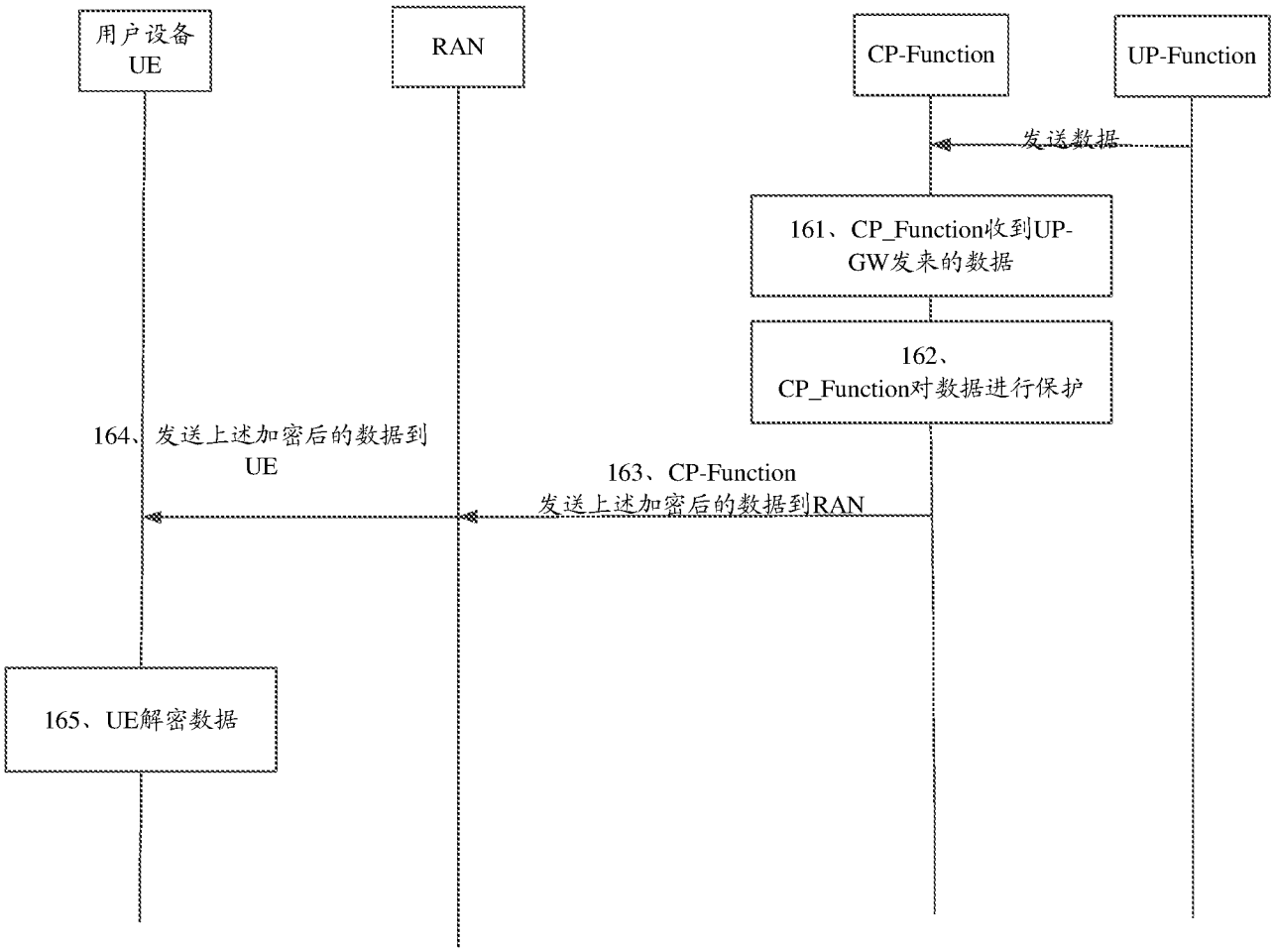

用户设备
UE
RAN
CP-Function
UP-Function
发送数据
161、CP_Function收到UP-GW发来的数据
162、CP_Function对数据进行保护
164、发送上述加密后的数据到UE
163、CP-Function发送上述加密后的数据到RAN
165、UE解密数据

图 16

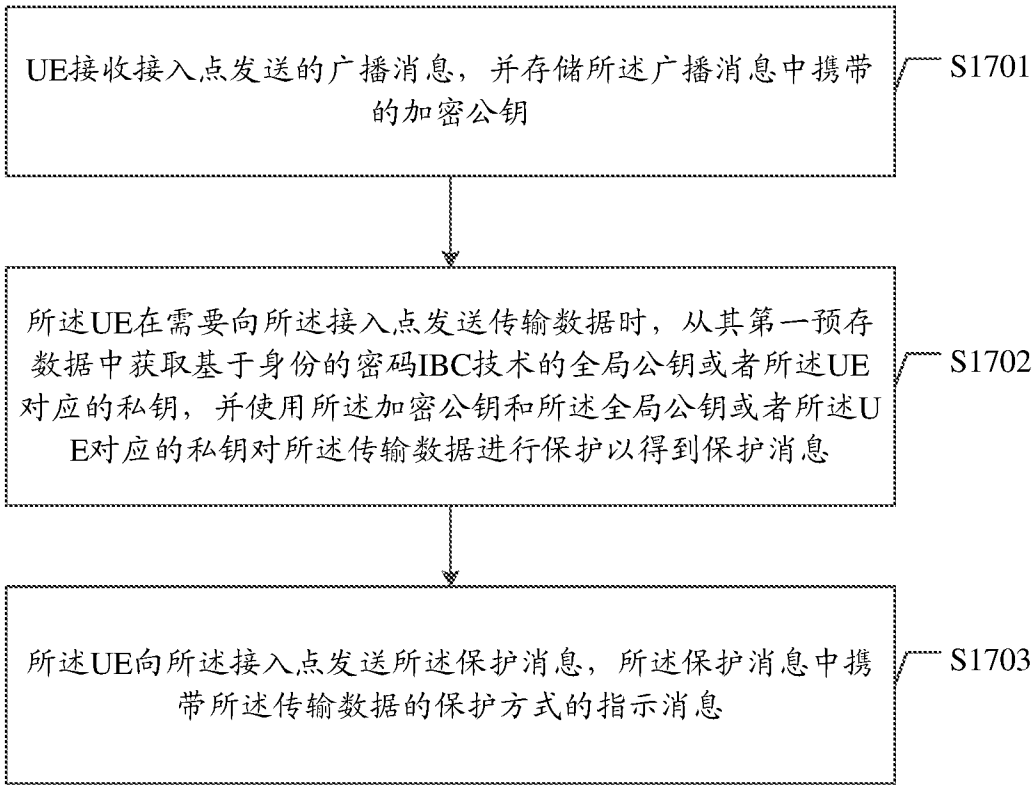

UE接收接入点发送的广播消息，并存储所述广播消息中携带的加密公钥
S1701
所述UE在需要向所述接入点发送传输数据时，从其第一预存数据中获取基于身份的密码IBC技术的全局公钥或者所述UE对应的私钥，并使用所述加密公钥和所述全局公钥或者所述UE对应的私钥对所述传输数据进行保护以得到保护消息
S1702
所述UE向所述接入点发送所述保护消息，所述保护消息中携带所述传输数据的保护方式的指示消息
S1703

图 17

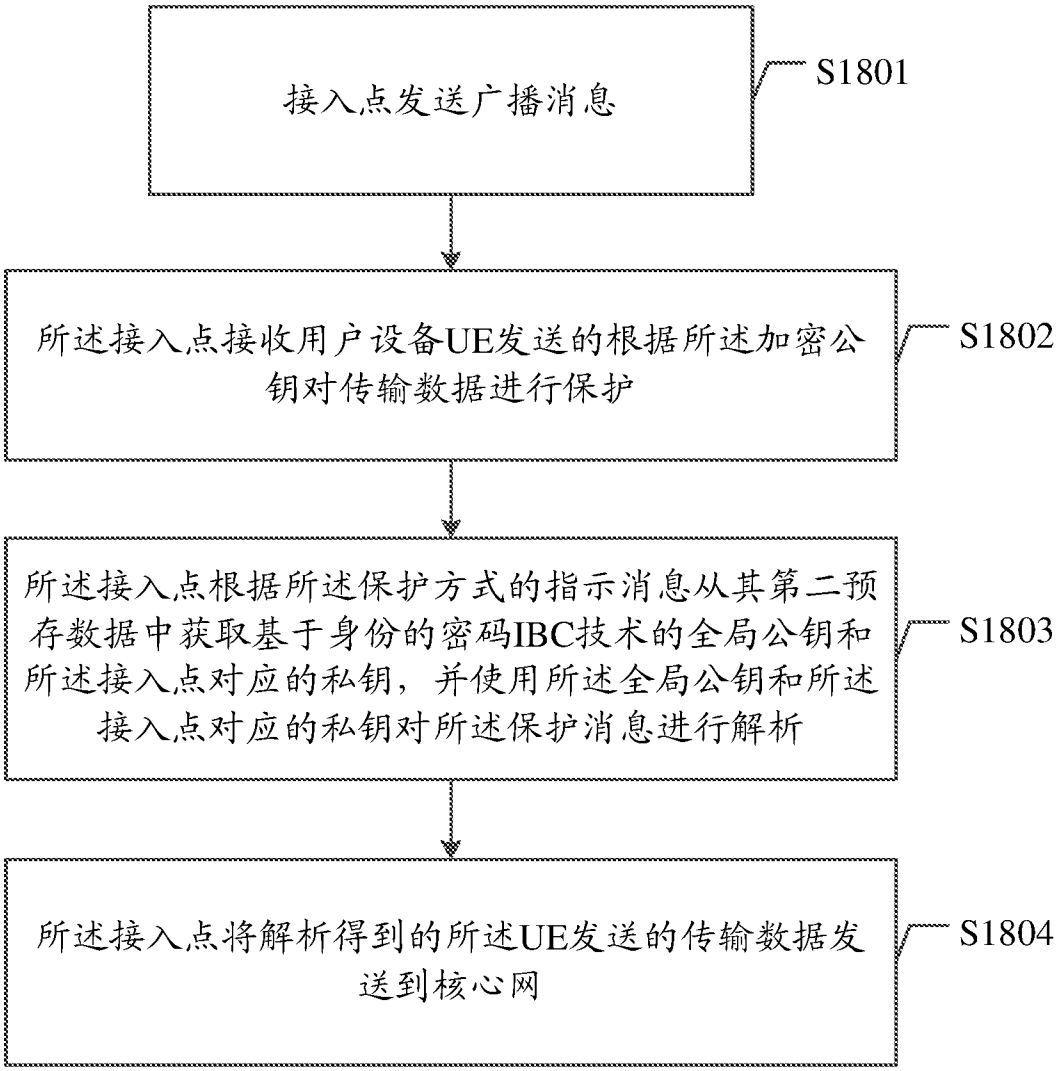

接入点发送广播消息
S1801
所述接入点接收用户设备UE发送的根据所述加密公钥对传输数据进行保护
S1802
所述接入点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码IBC技术的全局公钥和所述接入点对应的私钥，并使用所述全局公钥和所述接入点对应的私钥对所述保护消息进行解析
S1803
所述接入点将解析得到的所述UE发送的传输数据发送到核心网
S1804

图 18

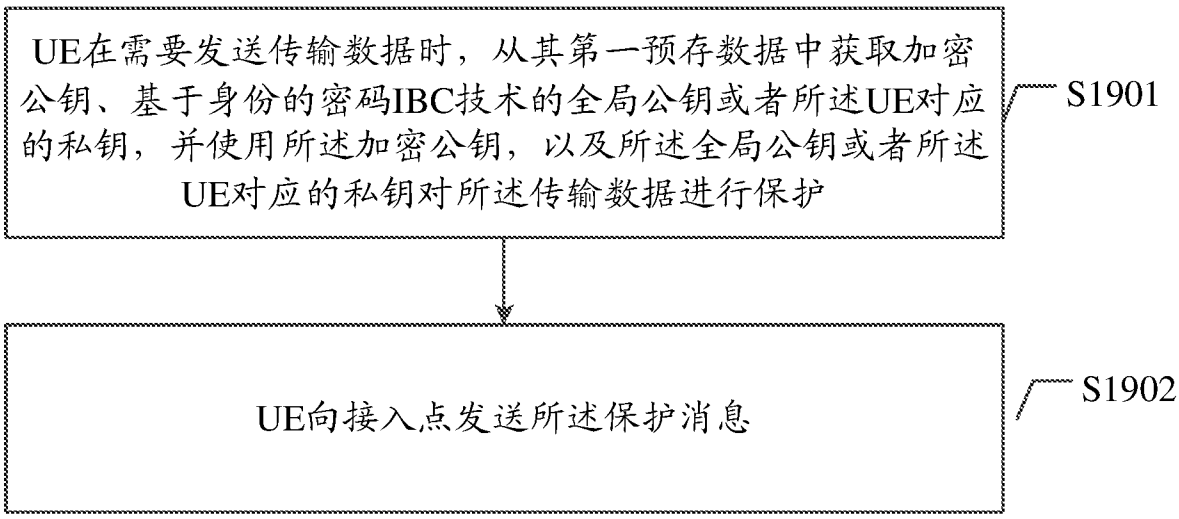

UE在需要发送传输数据时，从其第一预存数据中获取加密公钥、基于身份的密码IBC技术的全局公钥或者所述UE对应的私钥，并使用所述加密公钥，以及所述全局公钥或者所述UE对应的私钥对所述传输数据进行保护
S1901
UE向接入点发送所述保护消息
S1902

图 19

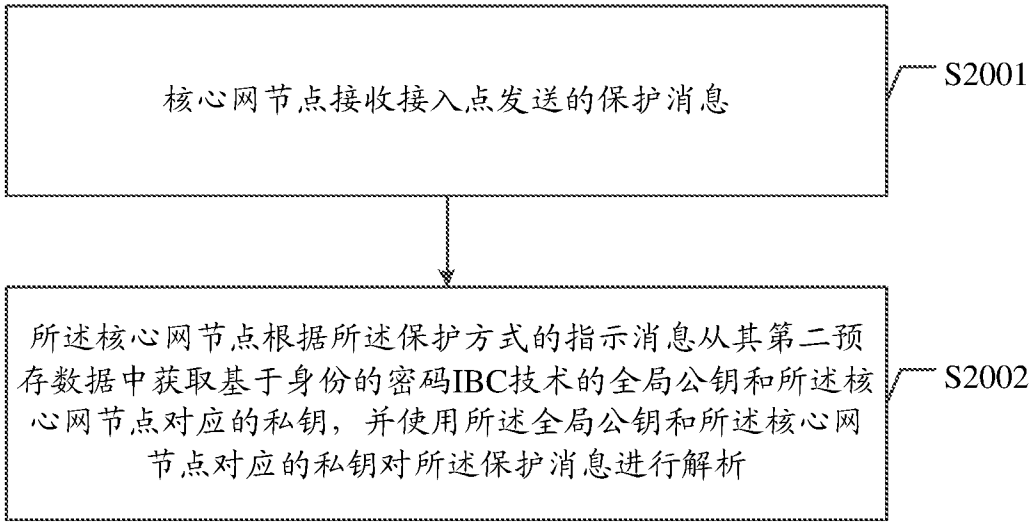

核心网节点接收接入点发送的保护消息
S2001
所述核心网节点根据所述保护方式的指示消息从其第二预存数据中获取基于身份的密码IBC技术的全局公钥和所述核心网节点对应的私钥，并使用所述全局公钥和所述核心网节点对应的私钥对所述保护消息进行解析
S2002

图 20

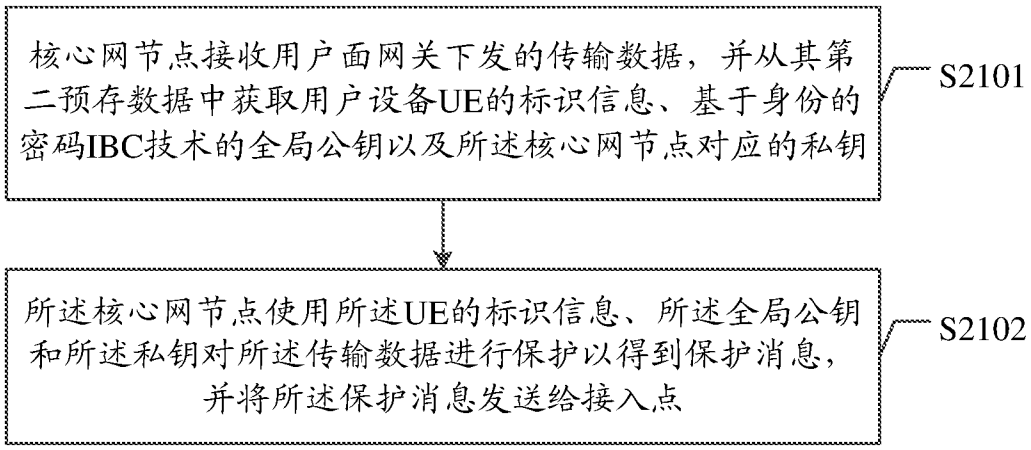

核心网节点接收用户面网关下发的传输数据，并从其第二预存数据中获取用户设备UE的标识信息、基于身份的密码IBC技术的全局公钥以及所述核心网节点对应的私钥
S2101
所述核心网节点使用所述UE的标识信息、所述全局公钥和所述私钥对所述传输数据进行保护以得到保护消息，并将所述保护消息发送给接入点
S2102

图 21

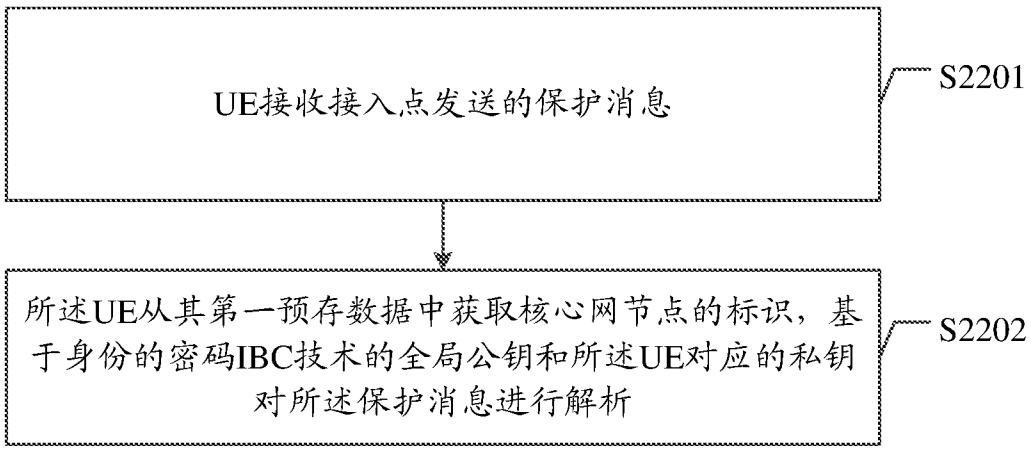

UE接收接入点发送的保护消息
S2201
所述UE从其第一预存数据中获取核心网节点的标识，基于身份的密码IBC技术的全局公钥和所述UE对应的私钥对所述保护消息进行解析
S2202

图 22

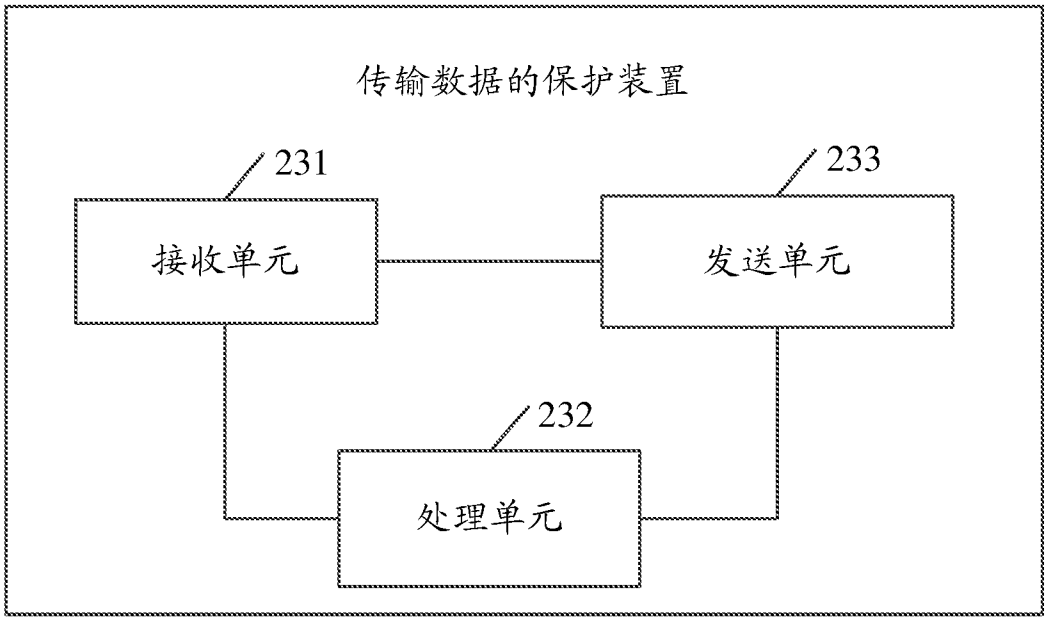

传输数据的保护装置
231
接收单元
233
发送单元
232
处理单元

图 23

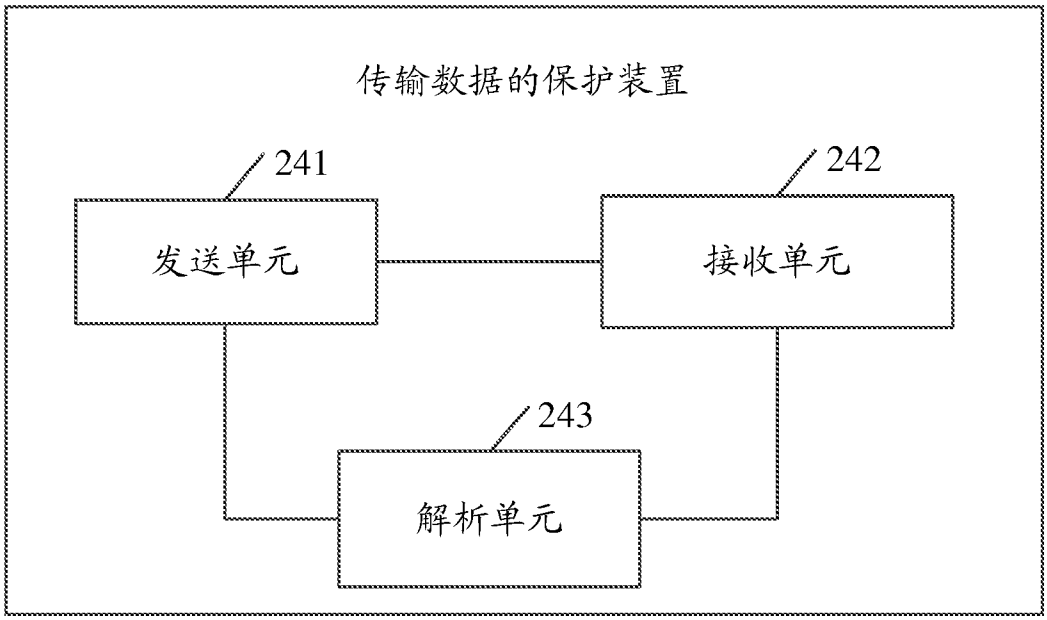

传输数据的保护装置
241
发送单元
242
接收单元
243
解析单元

图 24

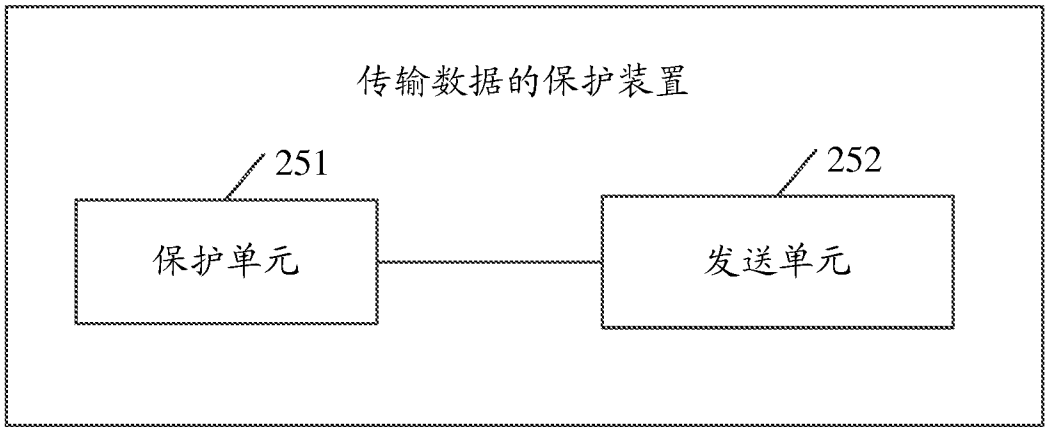

传输数据的保护装置
251
保护单元
252
发送单元

图 25

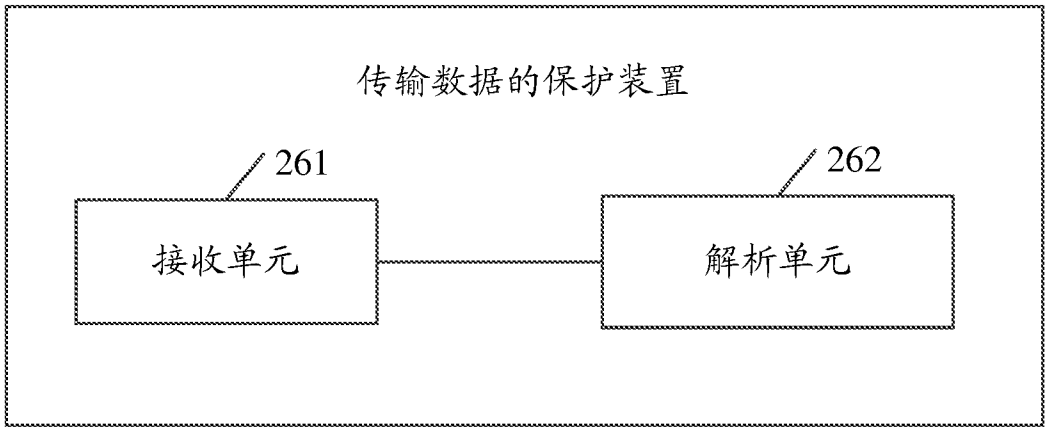

传输数据的保护装置
261
接收单元
262
解析单元

图 26

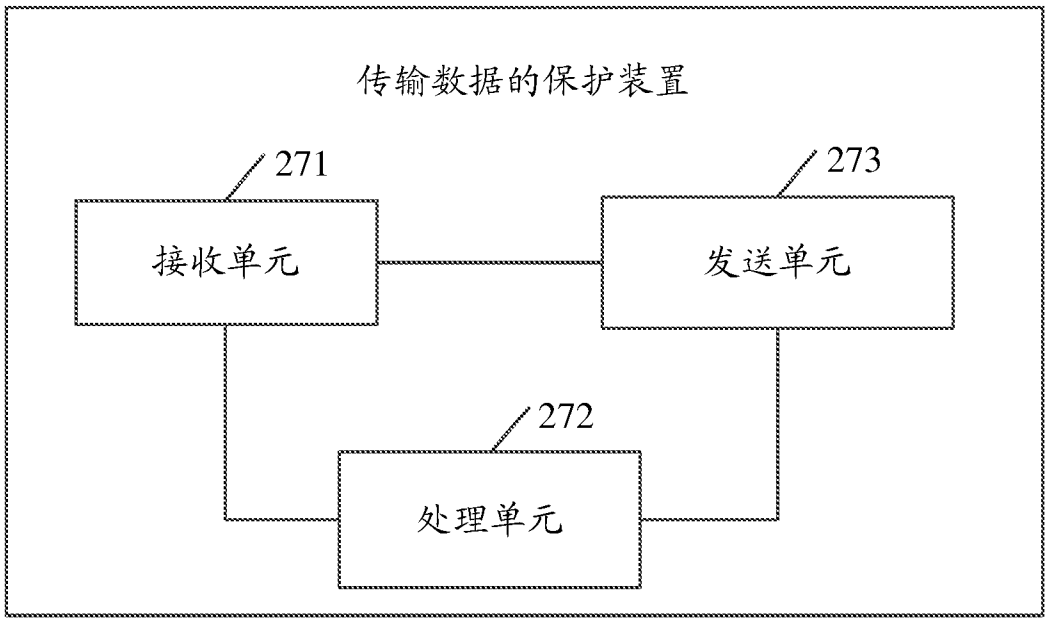

传输数据的保护装置
271
接收单元
273
发送单元
272
处理单元

图 27

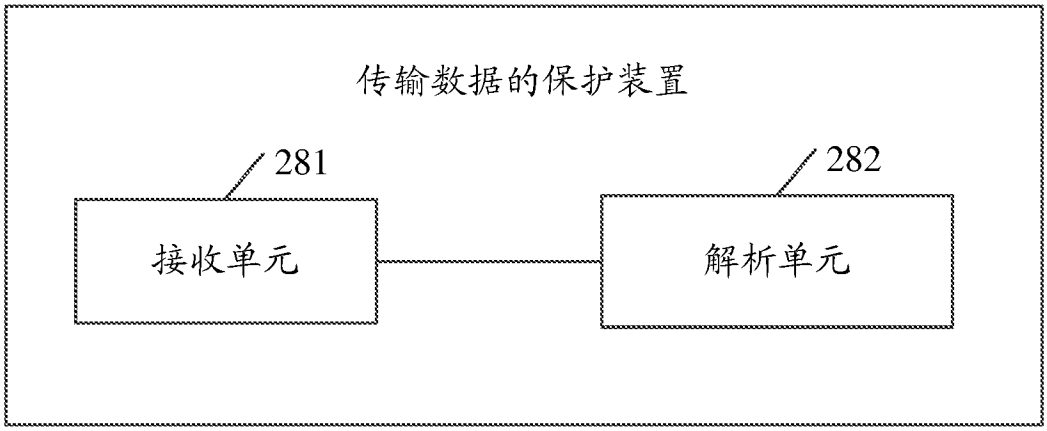


图 28

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/077952

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 9/30 (2006.01) i; H04L 9/08 (2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W

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

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

WPI, EPODOC, CNPAT, CNKI, 3GPP: identity, identification, code, IBC, UE, base station, AN, AP, eNB, core network, identi+ based crypto+, user equipment, access node, access point, enodeb, global, public key, private key, encrypt+, signatur+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2008047195 A1 (NOKIA CORPORATION), 24 April 2008 (24.04.2008), description, page 7, line 9 to page 9, line 15, and figures 1-3	1-87
A	CN 103002417 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 27 March 2013 (27.03.2013), the whole document	1-87
A	CN 103812650 A (HUAWEI TECHNOLOGIES CO., LTD.), 21 May 2014 (21.05.2014), the whole document	1-87
A	CN 104902471 A (SOUTHEAST UNIVERSITY), 09 September 2015 (09.09.2015), the whole document	1-87
A	MOTOROLA SOLUTIONS et al., "pCR to Add IBC Managed Content Encryption Key (CEK) for S/MIME", 3GPP TSG SA WG3 (SECURITY) MEETING #81 S3-152231, 13 November 2015 (13.11.2015), pages 1-5	1-87

☐ 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
11 May 2017 (11.05.2017)	**15 June 2017 (15.06.2017)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **LI, Wenjuan** Telephone No.: (86-10) **62413337**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/077952

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2008047195 A1	24 April 2008	US 2008130898 A1	05 June 2008
		US 2013080779 A1	28 March 2013
CN 103002417 A	27 March 2013	None	
CN 103812650 A	21 May 2014	WO 2014071719 A1	15 May 2014
CN 104902471 A	09 September 2015	None	

国际检索报告

国际申请号
PCT/CN2017/077952

A. 主题的分类

H04L 29/06(2006.01)i; H04L 9/30(2006.01)i; H04L 9/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI, EPODOC, CNPAT, CNKI, 3GPP: 身份，标识，密码，IBC，用户设备，UE，接入点，基站，AN，AP，eNB，核心网，全局，公钥，私钥，签名，加密，identi+ based crypto+，user equipment，access node，access point，enodeb，global，public key，private key，encrypt+，signatur+

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
A	WO 2008047195 A1 (NOKIA CORPORATION) 2008年 4月 24日 (2008-04-24) 说明书第7页第9行-第9页第15行，图1-3	1-87
A	CN 103002417 A (中国联合网络通信集团有限公司) 2013年 3月 27日 (2013-03-27) 全文	1-87
A	CN 103812650 A (华为技术有限公司) 2014年 5月 21日 (2014-05-21) 全文	1-87
A	CN 104902471 A (东南大学) 2015年 9月 9日 (2015-09-09) 全文	1-87
A	MOTOROLA SOLUTIONS等. "pCR to add IBC managed Content Encryption Key (CEK) for S/MIME" 3GPP TSG SA WG3 (Security) Meeting #81 S3-152231, 2015年 11月 13日 (2015-11-13), 第1-5页	1-87

☐ 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
2017年 5月 11日	2017年 6月 15日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 李文娟 电话号码 (86-10)62413337

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/077952

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)
WO	2008047195	A1	2008年 4月 24日	US	2008130898	A1	2008年 6月 5日
				US	2013080779	A1	2013年 3月 28日
CN	103002417	A	2013年 3月 27日		无		
CN	103812650	A	2014年 5月 21日	WO	2014071719	A1	2014年 5月 15日
CN	104902471	A	2015年 9月 9日		无		