



US 20250260566A1

(19) **United States**

(12) **Patent Application Publication**
WANG et al.

(10) **Pub. No.: US 2025/0260566 A1**

(43) **Pub. Date: Aug. 14, 2025**

(54) **COMMUNICATION METHOD AND APPARATUS**

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.**, Shenzhen (CN)

(72) Inventors: **Wenhui WANG**, Shanghai (CN);
Jianjun WU, Shenzhen (CN)

(21) Appl. No.: **19/192,456**

(22) Filed: **Apr. 29, 2025**

Related U.S. Application Data

(63) Continuation of application No. PCT/CN2022/128562, filed on Oct. 31, 2022.

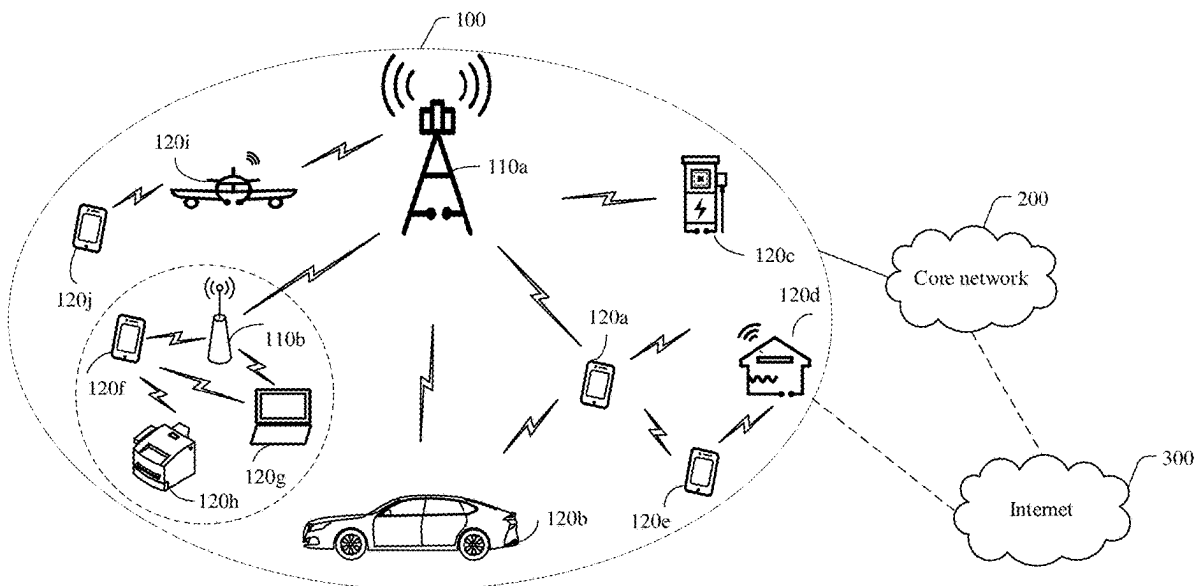
Publication Classification

(51) **Int. Cl.**
H04L 9/08 (2006.01)

(52) **U.S. Cl.**
CPC **H04L 9/0869** (2013.01)

(57) **ABSTRACT**

The technology of this application relates to a terminal device generating, by using a random number generator, at least one random number based on a user-specific parameter of a physical channel from a network device and a specified historical message exchanged between the terminal device and the network device. The at least one random number includes a first random number. The terminal device generates a physical channel encryption key based on the first random number by using a key generator. The terminal device encrypts or decrypts the physical channel based on the physical channel encryption key.



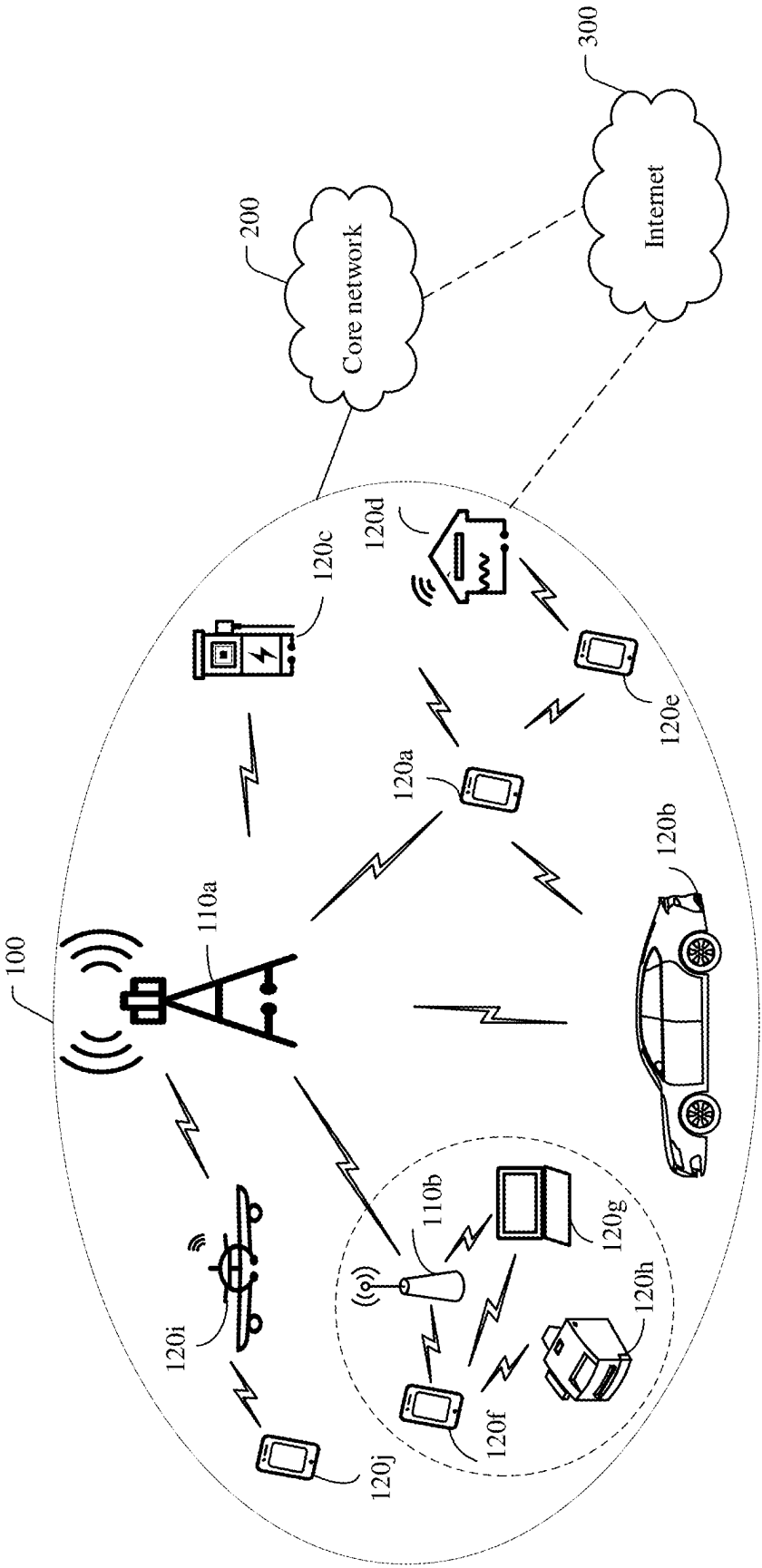


FIG. 1

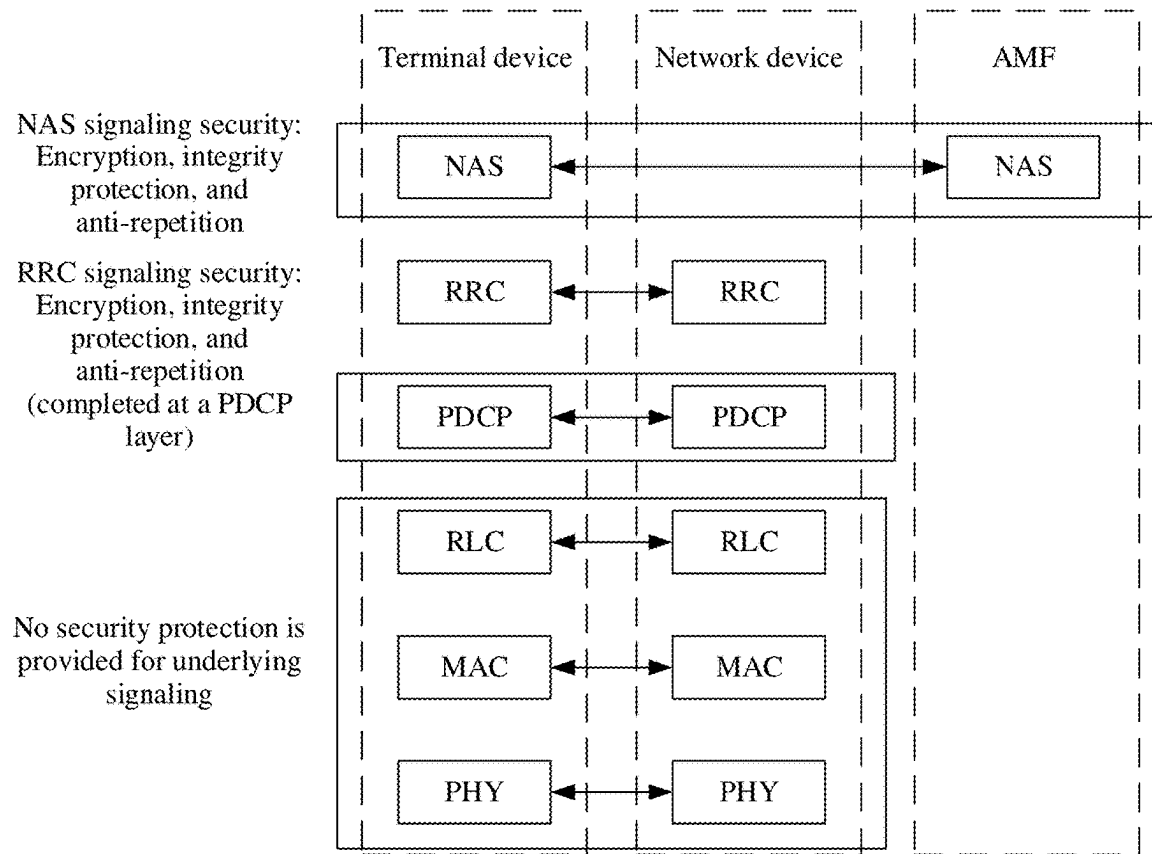


FIG. 2

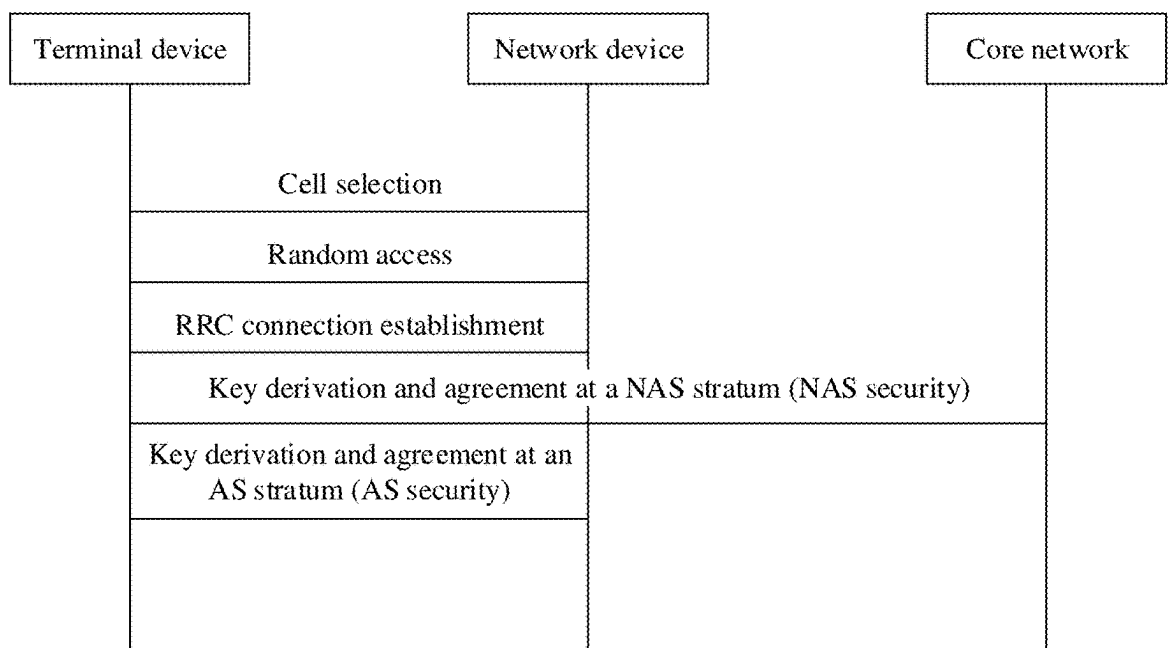


FIG. 3

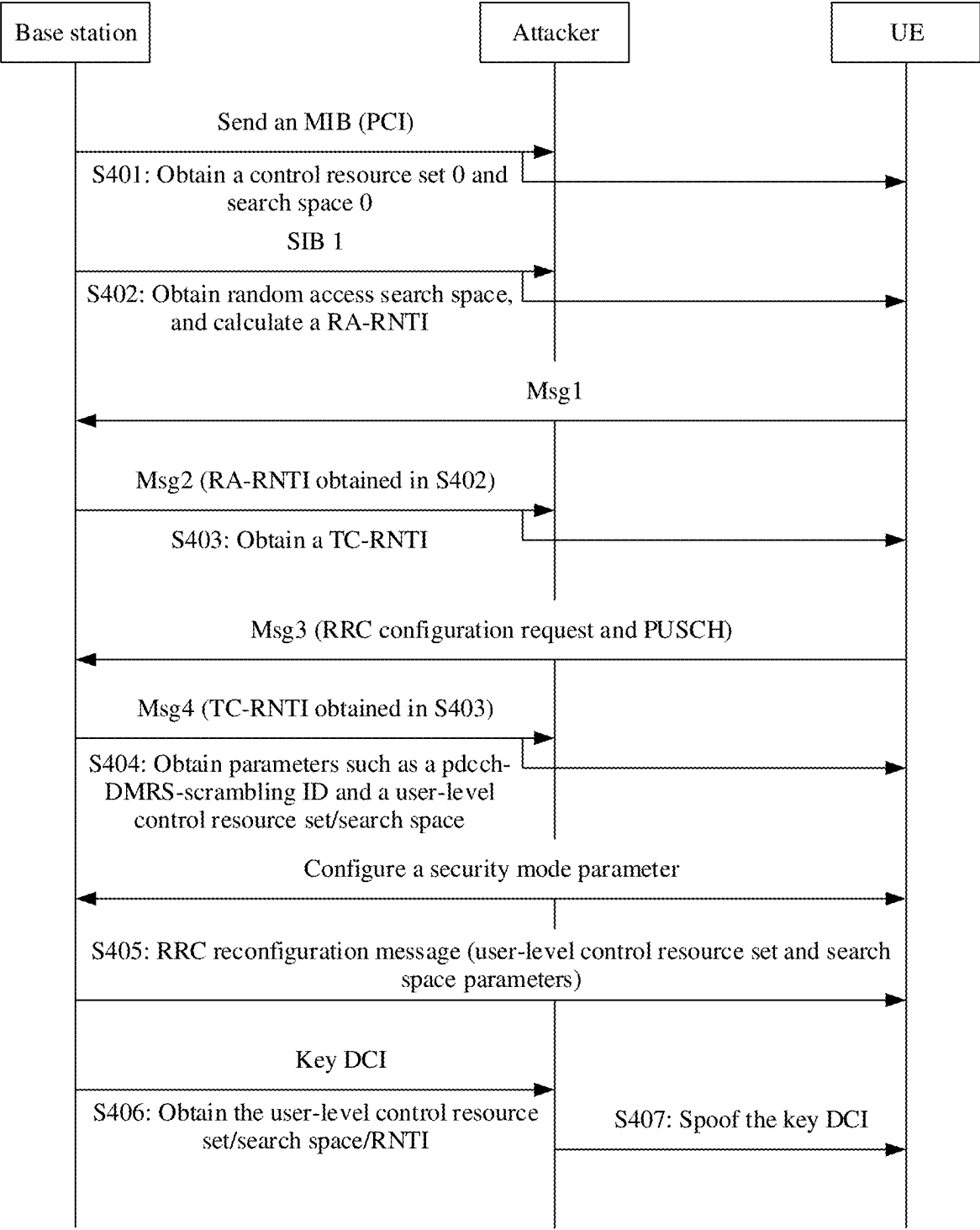


FIG. 4

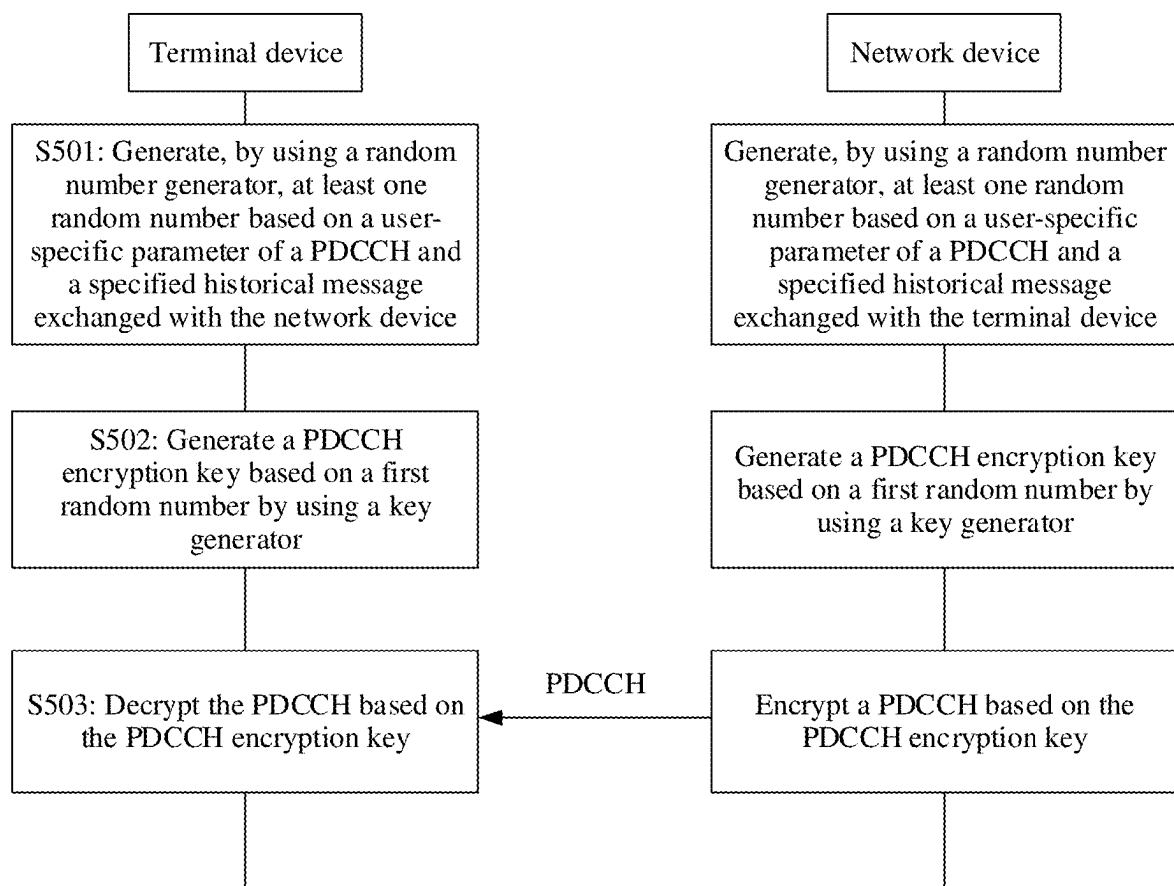


FIG. 5

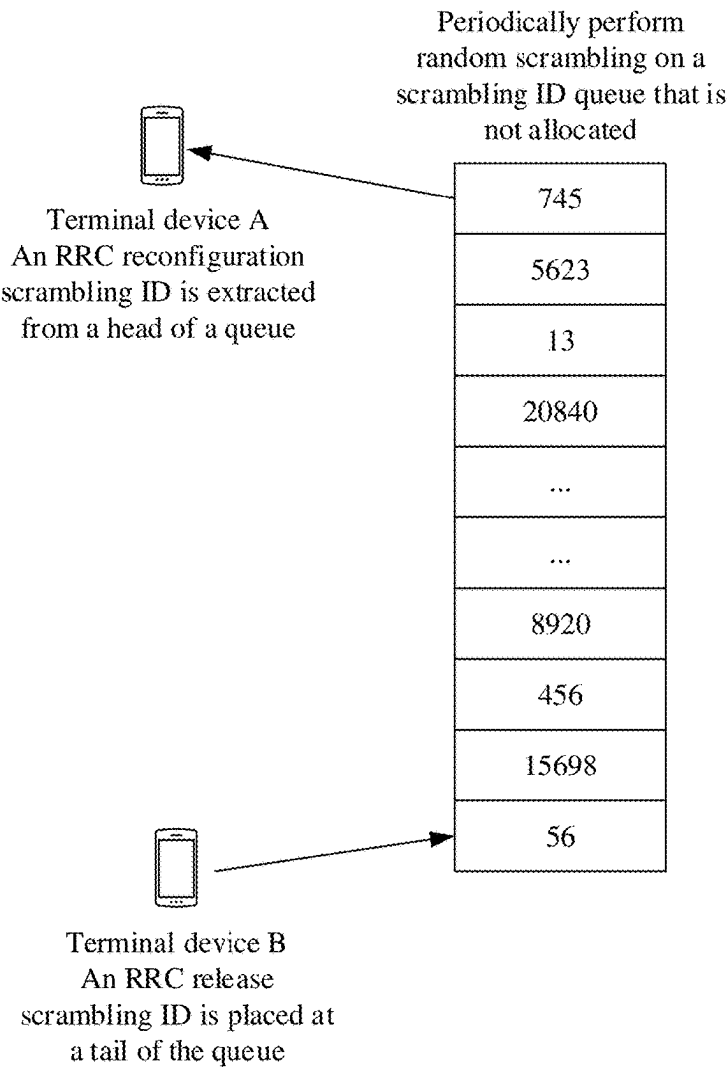


FIG. 6

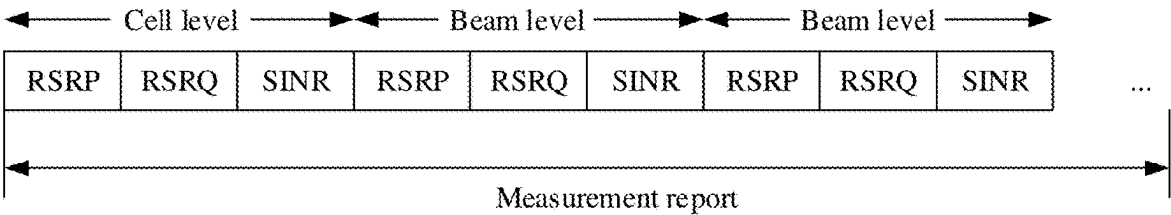


FIG. 7

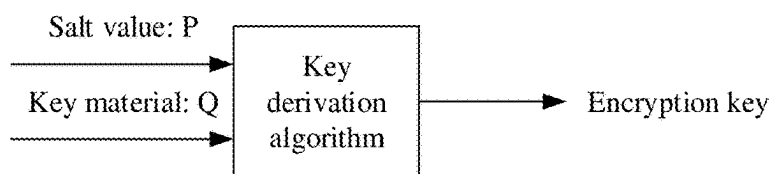


FIG. 8

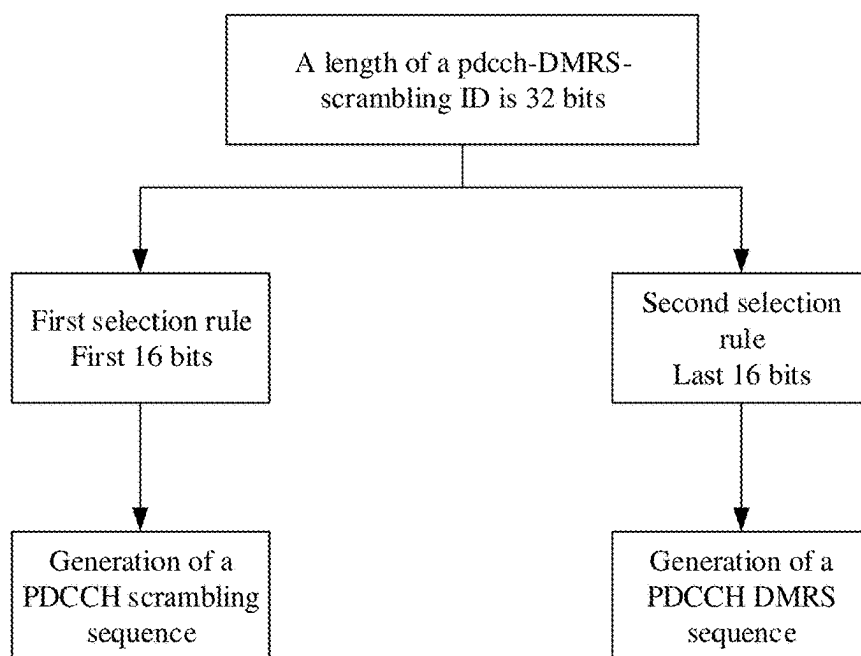


FIG. 9

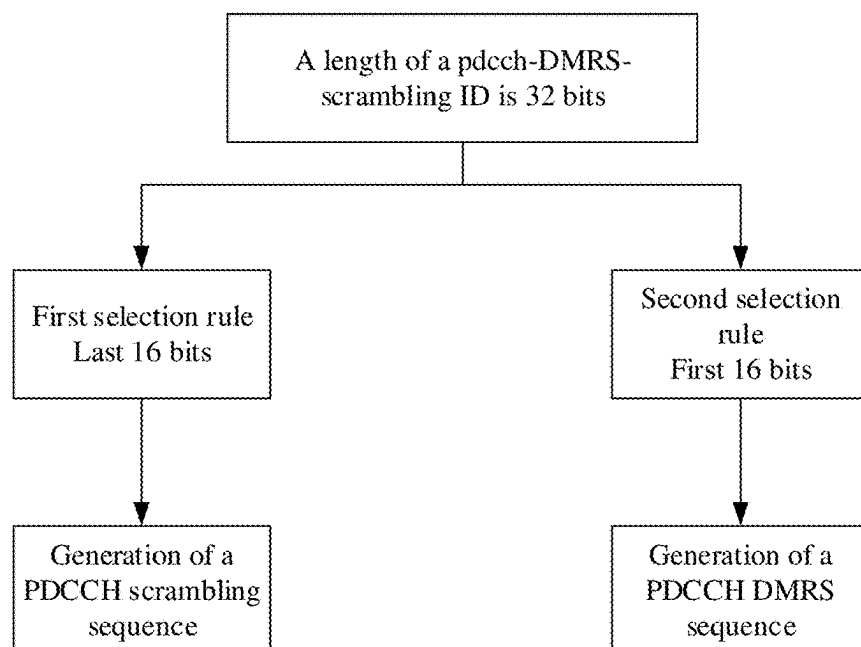


FIG. 10

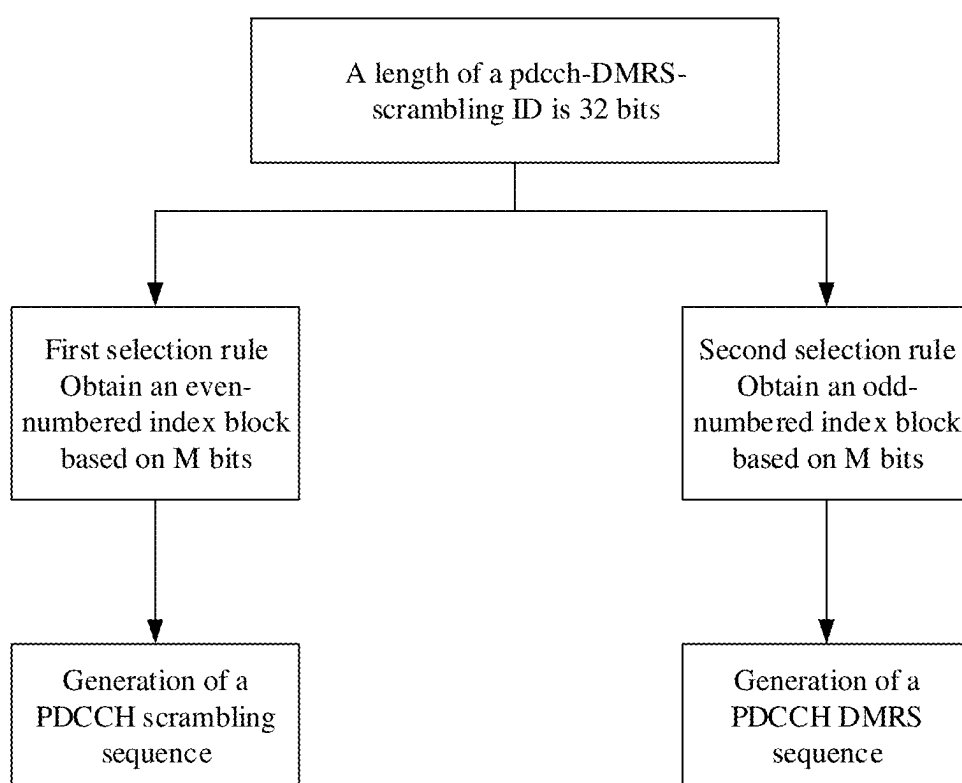


FIG. 11

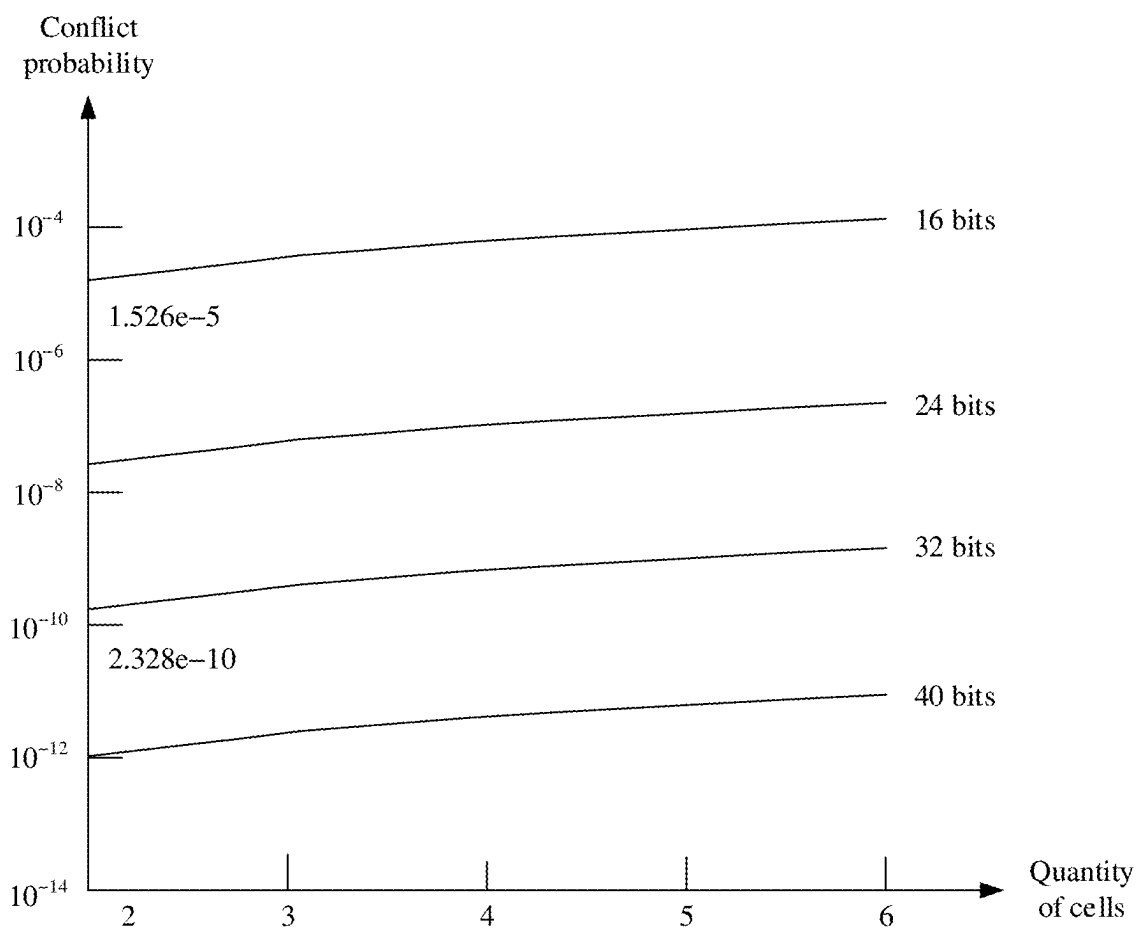


FIG. 12

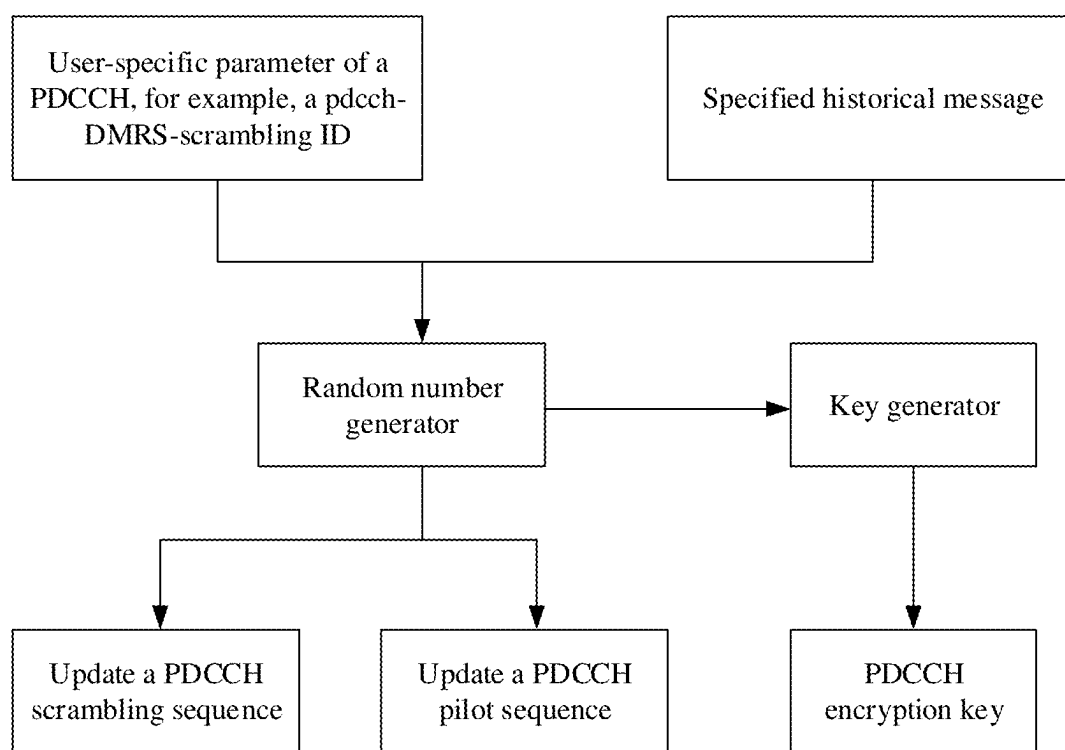


FIG. 13

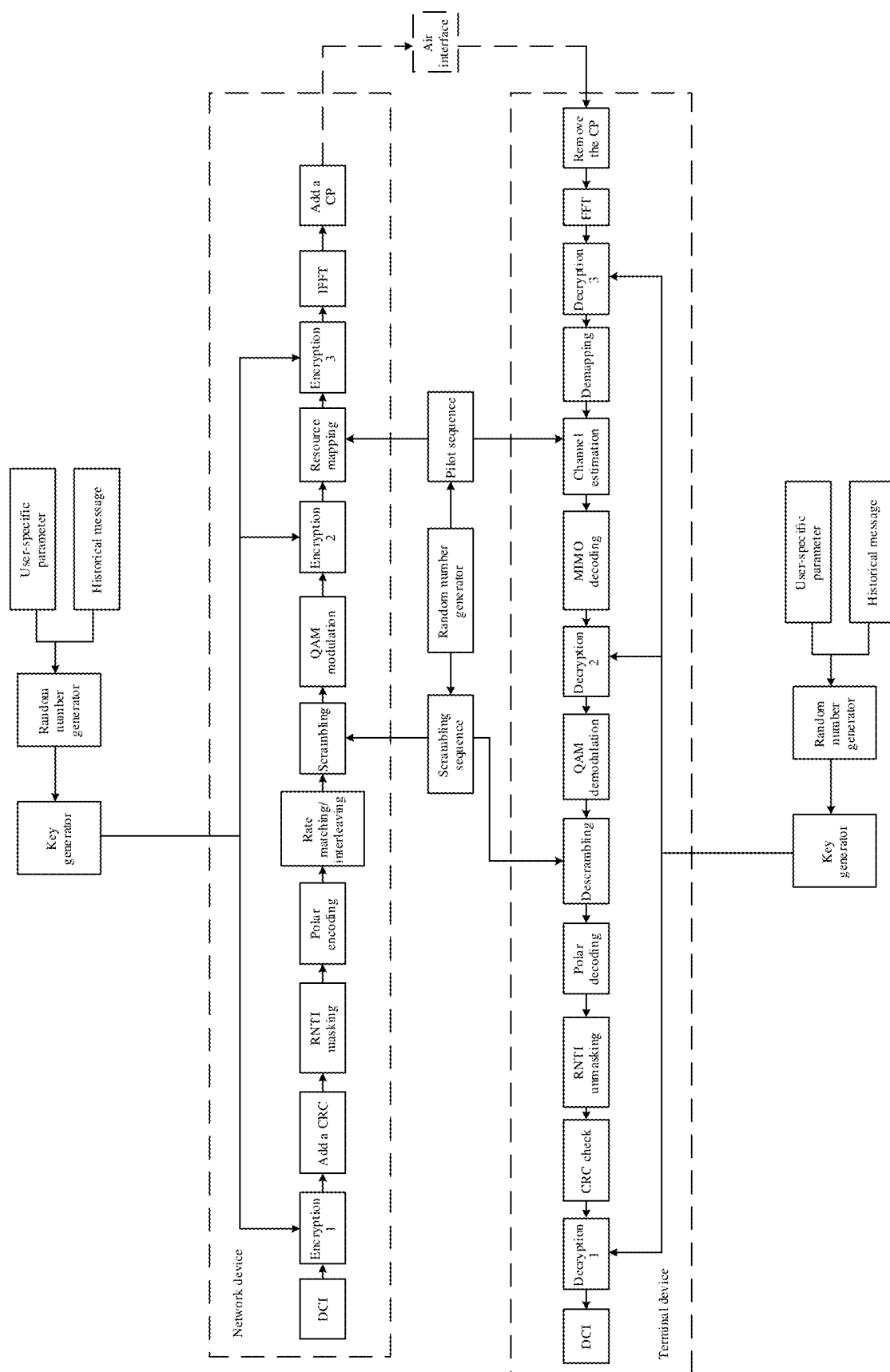


FIG. 14

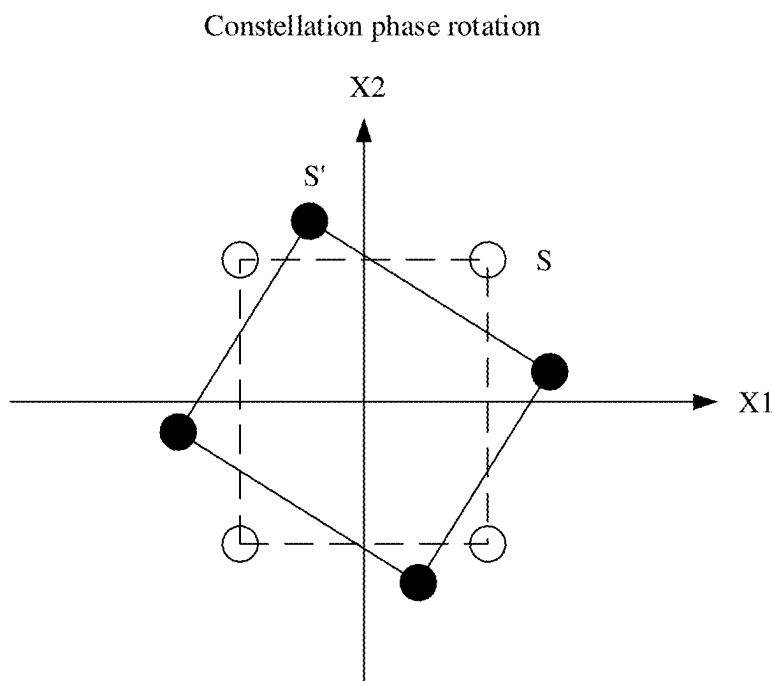


FIG. 15

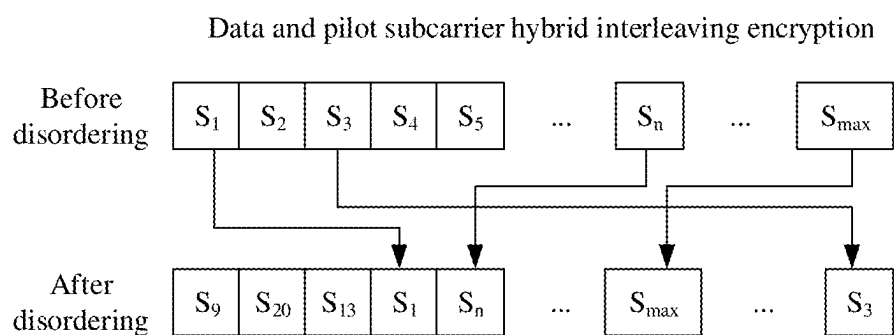


FIG. 16

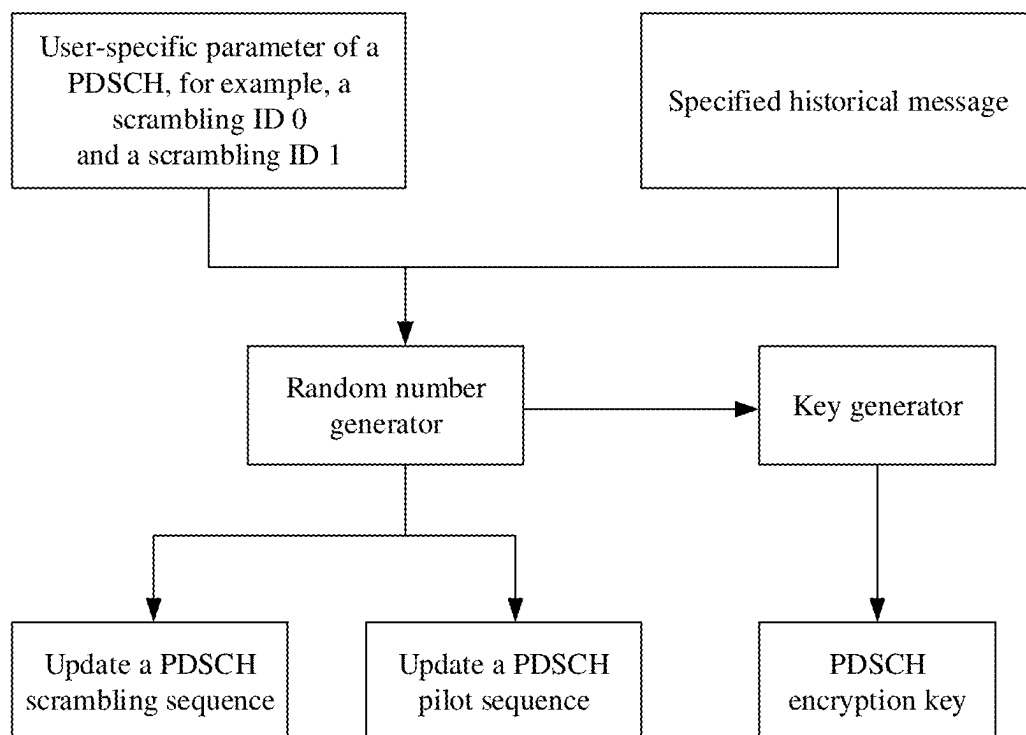


FIG. 17

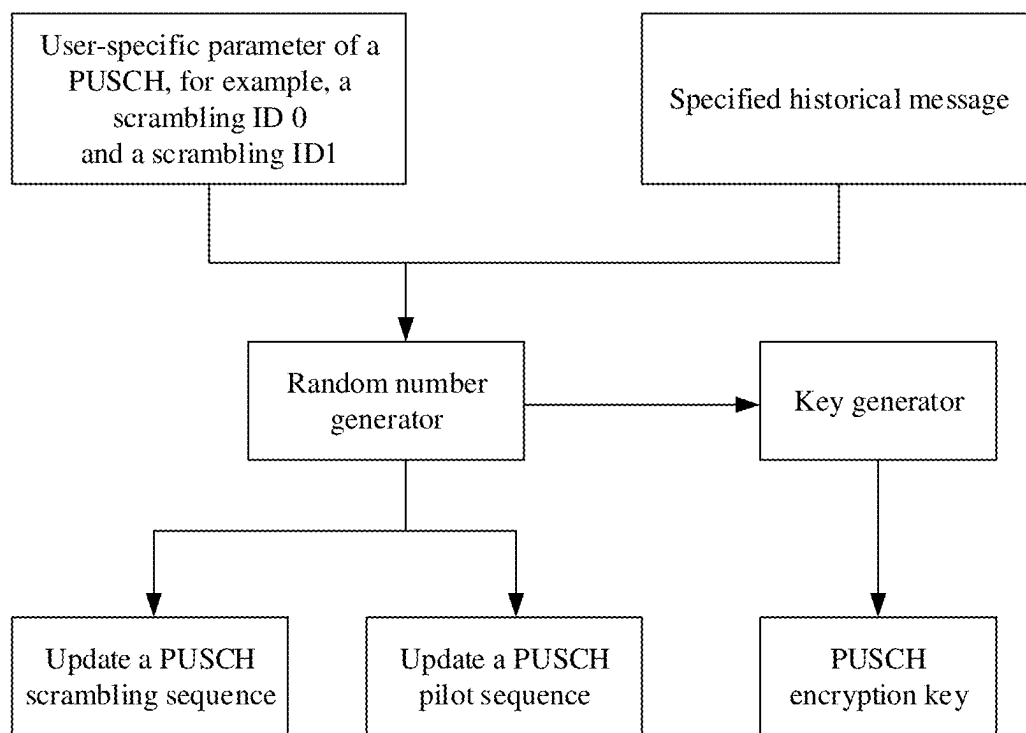


FIG. 18

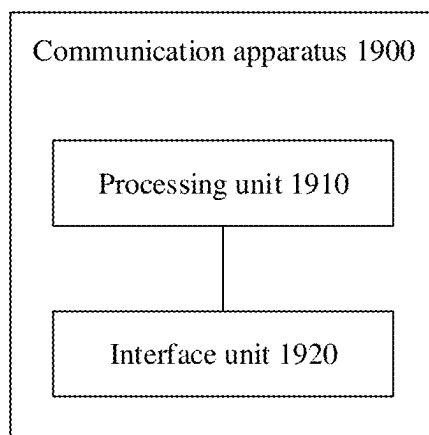


FIG. 19

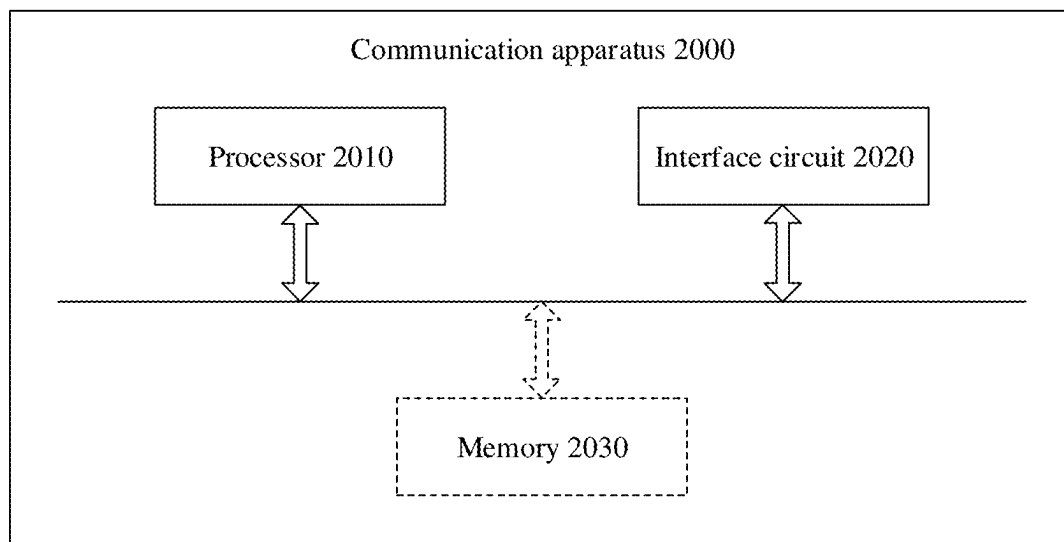


FIG. 20

COMMUNICATION METHOD AND APPARATUS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This is a continuation of International Application No. PCT/CN2022/128562, filed on Oct. 31, 2022, the disclosure of which is hereby incorporated by reference in its entirety.

TECHNICAL FIELD

[0002] Embodiments of this disclosure relate to the field of communication technologies, and in particular, to a communication method and apparatus.

BACKGROUND

[0003] Similar to a 4th generation (4G) mobile communication system, a 5th generation (5G) mobile communication system is characterized by two layers of security, and security mode command activation and security protection are respectively performed on a non-access stratum (NAS) and an access stratum (AS). After authenticating each other, a terminal device and a network agree on a security algorithm and key used for encryption and integrity protection of NAS signaling, radio resource control (RRC) signaling, and user data in a subsequent communication process. After agreement on a NAS security algorithm is completed, encryption and integrity protection are performed on all NAS signaling between an access and mobility management function (AMF) network element on a network side and the terminal device based on the agreed security algorithm and key used for encryption and integrity protection. In an AS security mode command exchange process, a network device on the network side and the terminal device agree on a security algorithm and key for AS encryption and integrity protection, and start encryption and integrity protection of RRC signaling and user data of the AS.

[0004] However, the foregoing security protection solution provides only security protection for NAS signaling and RRC signaling. For the 4G mobile communication system and the 5G mobile communication system, a packet data convergence protocol (PDCP) layer at the AS stratum provides a signaling transmission service for an RRC layer, implements encryption and integrity protection for RRC signaling, and implements decryption and integrity check for the RRC signaling in a reverse direction. However, no security protection is provided for signaling at each protocol sublayer below the PDCP layer. For example, no security protection is provided for physical (PHY) layer signaling and medium access control (MAC) layer signaling such as a media access control layer control element (MAC CE), uplink control information (UCI), and downlink control information (DCI). An attacker may eavesdrop and tamper with these pieces of underlying signaling, which may cause problems such as service interruption of an authorized terminal device, service performance deterioration of the terminal device, abnormal power consumption of the terminal device, and abnormal resource scheduling of the network device.

SUMMARY

[0005] This disclosure provides a communication method and apparatus, to improve security of underlying signaling

transmitted between a network device and a terminal device, and enhance security strength of anti-eavesdropping and anti-tampering of the underlying signaling.

[0006] According to a first aspect, an embodiment of this disclosure provides a communication method. The method may be performed by a terminal device, may be performed by a component (for example, a processor, a chip, or a chip system) of the terminal device, or may be implemented by a logical module or software that can implement all or some functions of the terminal device. The following provides descriptions by using an example in which the method is performed by the terminal device. The method includes: the terminal device generates, by using a random number generator, at least one random number based on a user-specific parameter of a physical channel from a network device and a specified historical message exchanged between the terminal device and the network device. The at least one random number includes a first random number. The terminal device generates a physical channel encryption key based on the first random number by using a key generator. The terminal device encrypts or decrypts the physical channel based on the physical channel encryption key.

[0007] Optionally, the physical channel may be a physical downlink control channel (PDCCH), a physical downlink shared channel (PDSCH), a physical uplink control channel (PUCCH), a physical uplink shared channel (PUSCH), or the like.

[0008] According to the foregoing method, the terminal device may extract the random number based on the user-specific parameter of the physical channel from the network device and the historical message exchanged with the network device, to generate the physical channel encryption key (for example, extract the random number based on a specific periodicity, to generate the physical channel encryption key), and encrypt or decrypt the physical channel, to provide protection for underlying signaling (for example, physical layer signaling) transmitted between the network device and the terminal device, improve security of the underlying signaling transmitted between the network device and the terminal device, and enhance security strength of anti-eavesdropping and anti-tampering of the underlying signaling. In addition, the random number is generated based on the exchanged historical message, to increase difficulty in cracking by an attacker, and prevent message spoofing and identity spoofing of the network device.

[0009] In some embodiments, the at least one random number further includes a second random number, and the method further includes: The terminal device updates, based on the second random number, a physical channel scrambling sequence corresponding to the physical channel; and the terminal device scrambles or descrambles the physical channel based on an updated physical channel scrambling sequence.

[0010] In the foregoing embodiments, the physical channel scrambling sequence may be updated (for example, updated based on a specific periodicity) based on the generated random number, to increase difficulty in correct descrambling by the attacker, thereby increasing costs such as calculation and time consumption of eavesdropping on signaling exchanged between the terminal device and the network device by the attacker.

[0011] In some embodiments, the at least one random number further includes a third random number, and the

method further includes: The terminal device updates, based on the third random number, a physical channel pilot sequence corresponding to the physical channel; and the terminal device performs resource mapping or channel estimation on the physical channel based on an updated physical channel pilot sequence.

[0012] In the foregoing embodiments, the physical channel pilot sequence may be updated (for example, updated based on a specific periodicity) based on the generated random number, to increase difficulty in correct channel estimation by the attacker, thereby increasing costs such as calculation and time consumption of eavesdropping on signaling exchanged between the terminal device and the network device by the attacker.

[0013] In some embodiments, the method further includes: The terminal device receives a scrambling-specific parameter of the physical channel from the network device. A quantity of bits included in the scrambling-specific parameter is greater than a first quantity threshold. The terminal device generates, based on a first sub-scrambling parameter, the physical channel scrambling sequence corresponding to the physical channel. The first sub-scrambling parameter is determined by the terminal device based on a first selection rule and the scrambling-specific parameter, and a quantity of bits included in the first sub-scrambling parameter is equal to the first quantity threshold. The terminal device generates, based on a second sub-scrambling parameter, the physical channel pilot sequence corresponding to the physical channel. The second sub-scrambling parameter is determined by the terminal device based on a second selection rule and the scrambling-specific parameter, and a quantity of bits included in the second sub-scrambling parameter is equal to the first quantity threshold.

[0014] In the foregoing embodiments, a length of the scrambling-specific parameter is increased, and the first sub-scrambling parameter and the second sub-scrambling parameter are extracted based on a preset rule, to update the physical channel scrambling sequence and the physical channel pilot sequence, thereby increasing random space of the scrambling-specific parameter and increasing difficulty in cracking by the attacker.

[0015] In some embodiments, that the terminal device generates, by using a random number generator, at least one random number based on a user-specific parameter of a physical channel from a network device and a specified historical message exchanged between the terminal device and the network device includes: The terminal device obtains, based on a specified periodicity, a specified historical message most recently exchanged with the network device; and the terminal device generates the at least one random number based on the user-specific parameter and the most recently exchanged specified historical message by using the random number generator.

[0016] In the foregoing embodiments, the terminal device may periodically obtain the user-specific parameter and a latest historical message, and generate the random number, to generate or update the physical channel encryption key, and the like. This can further increase difficulty in cracking the physical channel encryption key, and the like by the attacker, and improve security of signaling transmission between the network device and the terminal device.

[0017] In some embodiments, the user-specific parameter of the physical channel is randomly configured by the network device.

[0018] In the foregoing embodiments, the network device randomly configures the user-specific parameter of the physical channel, to further increase difficulty in cracking the user-specific parameter by the attacker, prevent the physical channel encryption key, and the like used by the network device and the terminal device from being cracked, and further improve security of signaling transmission between the network device and the terminal device.

[0019] According to a second aspect, an embodiment of this disclosure provides a communication method. The method may be performed by a network device, or may be performed by a component (for example, a processor, a chip, or a chip system) of the network device, or may be implemented by a logical module or software that can implement all or some functions of the network device. The following provides descriptions by using an example in which the method is performed by the network device. The method includes: the network device generates, by using a random number generator, at least one random number based on a user-specific parameter that is of a physical channel and that is sent to a terminal device and a specified historical message exchanged between the terminal device and the network device. The at least one random number includes a first random number. The network device generates a physical channel encryption key based on the first random number by using a key generator. The network device decrypts or encrypts the physical channel based on the physical channel encryption key.

[0020] Optionally, the physical channel may be a PDCCH, a PDSCH, a PUCCH, a PUSCH, or the like.

[0021] In some embodiments, the at least one random number further includes a second random number, and the method further includes: The network device updates, based on the second random number, a physical channel scrambling sequence corresponding to the physical channel; and the network device descrambles or scrambles the physical channel based on an updated physical channel scrambling sequence.

[0022] In some embodiments, the at least one random number further includes a third random number, and the method further includes: The network device updates, based on the third random number, a physical channel pilot sequence corresponding to the physical channel; and the network device performs channel estimation or resource mapping on the physical channel based on an updated physical channel pilot sequence.

[0023] In some embodiments, the method further includes: The network device sends a scrambling-specific parameter of the physical channel to the terminal device. A quantity of bits included in the scrambling-specific parameter is greater than a first quantity threshold. The network device generates, based on a first sub-scrambling parameter, the physical channel scrambling sequence corresponding to the physical channel. The first sub-scrambling parameter is determined by the network device based on a first selection rule and the scrambling-specific parameter, and a quantity of bits included in the first sub-scrambling parameter is equal to the first quantity threshold. The network device generates, based on a second sub-scrambling parameter, the physical channel pilot sequence corresponding to the physical channel. The second sub-scrambling parameter is determined by the network device based on a second selection rule and the

scrambling-specific parameter, and a quantity of bits included in the second sub-scrambling parameter is equal to the first quantity threshold.

[0024] In some embodiments, that the network device generates, by using a random number generator, at least one random number based on a user-specific parameter that is of a physical channel and that is sent to a terminal device and a specified historical message exchanged between the terminal device and the network device includes: The network device obtains, based on a specified periodicity, a specified historical message most recently exchanged with the terminal device; and the network device generates the at least one random number based on the user-specific parameter and the most recently exchanged specified historical message by using the random number generator.

[0025] In some embodiments, the user-specific parameter of the physical channel is randomly configured by the network device.

[0026] According to a third aspect, an embodiment of this disclosure provides a communication apparatus. The apparatus has a function of implementing the method in the first aspect. The function may be implemented by using hardware, or may be implemented by using hardware executing corresponding software. The hardware or software includes one or more modules corresponding to the function, for example, includes an interface unit and a processing unit.

[0027] In some embodiments, the apparatus may be a chip or an integrated circuit.

[0028] In some embodiments, the apparatus includes a processor. The processor may be coupled to a memory. The memory is configured to store instructions executed by the processor. When the instructions are executed by the processor, the apparatus may perform the method in the first aspect. "Coupling" means that two components are directly or indirectly connected or have a communication relationship.

[0029] In some embodiments, the apparatus may be an entire terminal device.

[0030] According to a fourth aspect, an embodiment of this disclosure provides a communication apparatus. The apparatus has a function of implementing the method in the second aspect. The function may be implemented by using hardware, or may be implemented by using hardware executing corresponding software. The hardware or software includes one or more modules corresponding to the function, for example, includes an interface unit and a processing unit. In some embodiments, the apparatus may be a chip or an integrated circuit.

[0031] In some embodiments, the apparatus includes a processor. The processor may be coupled to a memory. The memory is configured to store instructions executed by the processor. When the instructions are executed by the processor, the apparatus may perform the method in the second aspect. "Coupling" means that two components are directly or indirectly connected or have a communication relationship.

[0032] In some embodiments, the apparatus may be an entire network device.

[0033] According to a fifth aspect, an embodiment of this disclosure provides a communication apparatus. The communication apparatus includes an interface circuit and a processor, and the processor and the interface circuit are coupled to each other. The processor is configured to implement the method in the first aspect by using a logic circuit

or executing instructions. The interface circuit is configured to: receive a signal from a communication apparatus other than the communication apparatus and transmit the signal to the processor, or send a signal from the processor to a communication apparatus other than the communication apparatus. It can be understood that the interface circuit may be a transceiver, a transceiver machine, or an input/output interface.

[0034] Optionally, the communication apparatus may further include a memory, configured to store instructions executed by the processor, or store input data required for running instructions by the processor, or store data generated after the processor runs instructions. The memory may be a physically independent unit, or may be coupled to the processor, or the processor includes the memory.

[0035] According to a sixth aspect, an embodiment of this disclosure provides a communication apparatus. The communication apparatus includes an interface circuit and a processor, and the processor and the interface circuit are coupled to each other. The processor is configured to implement the method in the second aspect by using a logic circuit or executing instructions. The interface circuit is configured to: receive a signal from a communication apparatus other than the communication apparatus and transmit the signal to the processor, or send a signal from the processor to a communication apparatus other than the communication apparatus. It can be understood that the interface circuit may be a transceiver, a transceiver machine, or an input/output interface.

[0036] Optionally, the communication apparatus may further include a memory, configured to: store instructions executed by the processor, or store input data required for running instructions by the processor, or store data generated after the processor runs instructions. The memory may be a physically independent unit, or may be coupled to the processor, or the processor includes the memory.

[0037] According to a seventh aspect, an embodiment of this disclosure provides a communication system. The communication system includes a terminal device and a network device. The terminal device may implement the method in the first aspect, and the network device may implement the method in the second aspect.

[0038] According to an eighth aspect, an embodiment of this disclosure provides a computer-readable storage medium. The computer-readable storage medium stores a computer program or instructions. When the computer program or the instructions are executed by a processor, the method in the first aspect or the second aspect can be implemented.

[0039] According to a ninth aspect, an embodiment of this disclosure further provides a computer program product, including a computer program or instructions. When the computer program or the instructions are executed by a processor, the method in the first aspect or the second aspect can be implemented.

[0040] According to a tenth aspect, an embodiment of this disclosure further provides a chip system. The chip system includes a processor. The processor is configured to be coupled to a memory. The memory is configured to store a program or instructions. When the program or the instructions are executed by the processor, the method in the first aspect or the second aspect can be implemented.

[0041] For technical effects that can be achieved in the second aspect to the tenth aspect, refer to technical effects that can be achieved in the first aspect.

BRIEF DESCRIPTION OF DRAWINGS

[0042] FIG. 1 is a diagram of an architecture of a communication system according to an example embodiment of this disclosure;

[0043] FIG. 2 is a diagram of a control plane protocol stack of 5G NR according to an example embodiment of this disclosure;

[0044] FIG. 3 is a diagram of a signaling interaction procedure between a terminal device and each of a network device and a core network in an access phase according to an example embodiment of this disclosure;

[0045] FIG. 4 shows a procedure in which an attacker eavesdrops on a PDCCH resource configuration and spoofs DCI according to an example embodiment of this disclosure;

[0046] FIG. 5 is a diagram of a communication method according to an example embodiment of this disclosure;

[0047] FIG. 6 is a diagram of scrambling ID allocation according to an example embodiment of this disclosure;

[0048] FIG. 7 is a diagram of a measurement report according to an example embodiment of this disclosure;

[0049] FIG. 8 is a diagram of an encryption key generation process according to an example embodiment of this disclosure;

[0050] FIG. 9 is a diagram 1 of a scrambling ID selection rule according to an example embodiment of this disclosure;

[0051] FIG. 10 is a diagram 2 of a scrambling ID selection rule according to an example embodiment of this disclosure;

[0052] FIG. 11 is a diagram 3 of a scrambling ID selection rule according to an example embodiment of this disclosure;

[0053] FIG. 12 is a diagram of a conflict between scrambling-specific parameters according to an example embodiment of this disclosure;

[0054] FIG. 13 is a diagram of enhancing PDCCH security protection according to an example embodiment of this disclosure;

[0055] FIG. 14 is a diagram of physical layer PDCCH encryption according to an example embodiment of this disclosure;

[0056] FIG. 15 is a diagram of constellation phase rotation encryption according to an example embodiment of this disclosure;

[0057] FIG. 16 is a diagram of data and pilot subcarrier hybrid interleaving encryption according to an example embodiment of this disclosure;

[0058] FIG. 17 is a diagram of enhancing PDSCH security protection according to an example embodiment of this disclosure;

[0059] FIG. 18 is a diagram of enhancing PUSCH security protection according to an example embodiment of this disclosure;

[0060] FIG. 19 is a diagram 1 of a structure of a communication apparatus according to an example embodiment of this disclosure; and

[0061] FIG. 20 is a diagram 2 of a structure of a communication apparatus according to an example embodiment of this disclosure.

DESCRIPTION OF EMBODIMENTS

[0062] Technical solutions in embodiments of this disclosure may be applied to various communication systems such as a 4th generation (4G) mobile communication system and a 5th generation (5G) new radio (NR) mobile communication system. The technical solutions provided in this disclosure may be further applied to a future communication system, for example, a 6th generation mobile communication system. Alternatively, the communication system may be an internet of things (IoT) network or another network.

[0063] An architecture of a communication system to which embodiments of this disclosure are applied may be shown in FIG. 1. The communication system includes a radio access network 100 and a core network 200. Optionally, the communication system may further include an internet 300. The radio access network 100 may include at least one network device, for example, 110a and 110b in FIG. 1, and may further include at least one terminal device, for example, 120a to 120j in FIG. 1. 110a is a base station, 110b is a micro base station, 120a, 120e, 120f, and 120j are mobile phones, 120b is a vehicle, 120c is a fuel dispenser, 120d is a home access point (HAP) deployed indoors or outdoors, 120g is a notebook computer, 120h is a printer, and 120i is an uncrewed aerial vehicle. A same terminal device or network device may provide different functions in different application scenarios. For example, the mobile phones in FIG. 1 include 120a, 120e, 120f, and 120j. The mobile phone 120a may access the base station 110a, be connected to the vehicle 120b, directly communicate with the mobile phone 120e, and access the HAP. The mobile phone 120e may access the HAP and directly communicate with the mobile phone 120a. The mobile phone 120f may access the micro base station 110b, be connected to the notebook computer 120g, and be connected to the printer 120h. The mobile phone 120j may control the uncrewed aerial vehicle 120i.

[0064] Wireless communication is performed between the terminal device and the network device, and the network device is connected to the core network (for example, an evolved packet core (EPC) in a 4G mobile communication system or a core network (e.g. a 5G core (5GC)) in a 5G mobile communication system). A core network device and the network device may be different physical devices independent of each other; or functions of a core network device and logical functions of the network device may be integrated into a same physical device; or some functions of a core network device and some functions of the network device may be integrated into one physical device. Terminal devices may be connected to each other and network devices may be connected to each other in a wired or wireless manner. FIG. 1 is merely a diagram. The communication system may further include another device, for example, a wireless relay device and a wireless backhaul device, which are not drawn in FIG. 1.

[0065] The network device may also be referred to as a radio access network device, and may be a base station, an evolved NodeB (eNodeB), a NodeB, a transmission reception point (TRP), an access point, a base station transceiver, a transceiver function, a radio transceiver, a basic service set (BSS), an extended service set (ESS), a next generation NodeB (gNB) in the 5th generation (5G) mobile communication system, a base station in a future mobile communication system, an access node in a Wi-Fi system, or the like; or may be a module or a unit that completes some functions

of a base station, for example, may be a central unit (CU), or may be a distributed unit (DU). The CU herein implements functions of a radio resource control protocol and a packet data convergence protocol (PDCP) of the base station, and may further implement a function of a service data adaptation protocol (SDAP). The DU implements functions of a radio link control layer and a medium access control (MAC) layer of the base station, and may further implement a part or all of functions of a physical layer. For specific descriptions of the foregoing protocol layers, refer to technical specifications related to the 3rd generation partnership project (3GPP). The network device may be a macro base station (for example, 110a in FIG. 1), may be a micro base station or an indoor base station (for example, 110b in FIG. 1), or may be a relay node, a donor node, or the like. A specific technology and a specific device form that are used for the network device are not limited in embodiments of this disclosure.

[0066] The network device may perform one or more of the following functions: user data and control signaling transmission, user data or air interface signaling encryption and decryption, integrity protection, header compression, a mobility control function (for example, a handover or dual connectivity), inter-cell interference coordination, connection establishment and release, load balancing, NAS message distribution, NAS node selection, synchronization, paging, positioning and transferring warning information, radio access network (RAN) sharing, multimedia broadcast multicast service (MBMS), user and device tracking, RAN information management (RIM), and the like. A plurality of network devices may directly or indirectly communicate with each other through a backhaul network (an X2 or Xn interface). The network device may perform wireless communication with the terminal device, and provide the terminal device with an access point to an EPC or a 5GC core network. Each network device may provide a communication service for a terminal device user in a corresponding geographical coverage area.

[0067] The terminal device may also be referred to as a terminal, user equipment (UE), a station, a mobile station, a subscriber station, a mobile unit, a subscriber unit, a wireless unit, a remote unit, a mobile device, a wireless device, a wireless communication device, a remote device, a mobile subscriber station, an access terminal, a mobile terminal, a wireless terminal, a remote terminal, a user agent, a mobile client, a client, or the like. The terminal device may be widely used in various scenarios such as device-to-device (D2D), vehicle to everything (V2X) communication, machine-type communication (MTC), an IoT, virtual reality, augmented reality, industrial control, self-driving, telemedicine, smart grid, smart furniture, smart office, smart wear, smart transportation, and smart city. The terminal device may be a cellular phone, a mobile phone, a session initiation protocol (SIP) phone, a tablet computer, a computer with a wireless transceiver function, a personal digital assistant (PDA), a wearable device, a vehicle, an uncrewed aerial vehicle, a helicopter, an airplane, a ship, a robot, a robot arm, a smart home device, a medical care device, or the like; or may be an IoT device such as a parking timer, a smart meter, a fuel pump, a vehicle, or a Holter monitor. A specific technology and a specific device form that are used for the terminal device are not limited in embodiments of this disclosure.

[0068] The network device and the terminal device may be at fixed locations, or may be movable. The network device and the terminal device may be deployed on the land, including an indoor device, an outdoor device, a handheld device, or a vehicle-mounted device; may be deployed on the water surface; or may be deployed on a plane, a balloon, and a satellite in the air. An application scenario of the network device and the terminal device is not limited in embodiments of this disclosure.

[0069] Communication between the network device and the terminal device, between network devices, or between terminal devices may be performed by using a licensed spectrum, an unlicensed spectrum, or both a licensed spectrum and an unlicensed spectrum; may be performed by using a spectrum below 6 gigahertz (GHz); may be performed by using a spectrum above 6 GHz; or may be performed by using both a spectrum below 6 GHz and a spectrum above 6 GHz. A spectrum resource for wireless communication is not limited in embodiments of this disclosure.

[0070] In embodiments of this disclosure, the function of the network device may alternatively be performed by a module (for example, a chip) in the network device, or may be performed by a control subsystem including the function of the network device. The control subsystem including the function of the network device may be a control center in the foregoing application scenarios such as smart grid, industrial control, intelligent transportation, and smart city. The function of the terminal device may alternatively be performed by a module (for example, a chip or a modem) in the terminal device, or may be performed by an apparatus including a function of the terminal device.

[0071] In this disclosure, the network device sends a downlink signal or downlink information to the terminal device, and the downlink information is carried on a downlink channel. The terminal device sends an uplink signal or uplink information to the network device, and the uplink information is carried on an uplink channel. To communicate with the network device, the terminal device needs to establish a wireless connection to a cell controlled by the network device. The cell that establishes the wireless connection to the terminal device is referred to as a serving cell of the terminal device. When communicating with the serving cell, the terminal device is further interfered with by a signal from a neighboring cell.

[0072] A control plane protocol stack of 5G NR is the same as a control plane protocol stack of 4G long term evolution (LTE). FIG. 2 is a diagram of a control plane protocol stack of 5G NR according to an embodiment of this disclosure. As shown in FIG. 2, the control plane protocol stack includes a physical (PHY) layer (which may also be referred to as an L1 layer), a medium access control (MAC) layer, a radio link control (RLC) layer, a packet data convergence protocol (PDCP) layer, a radio resource control (RRC) layer, and a non-access stratum (NAS). A layer other than the NAS stratum may be referred to as an access stratum (AS). On a terminal device side, all protocol stacks are located in the terminal device. On a network side, the NAS stratum is not located on the network device, but is located on an AMF entity in the core network.

[0073] FIG. 3 is a diagram of a signaling interaction procedure between a terminal device and each of a network device and a core network in an access phase. The terminal device performs cell selection in an initial access phase, and

then performs random access to establish a connection to the network device, to complete RRC connection establishment. Then, the terminal device and the core network (for example, the AMF entity in the core network) perform bidirectional identity authentication. After authentication succeeds, key derivation and agreement at the NAS and the AS stratum are started. Before NAS security and AS security modes are completed (SecurityModeComplete), security protection is provided for none of air interface signaling, including RRC signaling and NAS signaling. After the NAS security and AS security modes are completed, encryption and integrity protection can be enabled for RRC, NAS signaling, and user-plane data.

[0074] However, the foregoing security protection solution provides only security protection for NAS signaling and RRC signaling. For the 4G mobile communication system and the 5G mobile communication system, a PDCP layer at the AS stratum provides a signaling transmission service for an RRC layer, implements encryption and integrity protection for RRC signaling, and implements decryption and integrity check for RRC signaling in a reverse direction. However, no security protection is provided for signaling at each protocol sublayer below the PDCP layer. For example, no security protection is provided for PHY layer signaling and MAC layer signaling such as MAC CE, UCI, and DCI. An attacker may eavesdrop and tamper with these pieces of underlying signaling, which may cause problems such as service interruption of an authorized terminal device, service performance deterioration of the terminal device, abnormal power consumption of the terminal device, and abnormal resource scheduling of the network device.

[0075] The DCI is taken as an example. No security protection is provided for DCI that serves as a message carried on a PDCCH. The attacker may eavesdrop and tamper with the message, which may cause problems such as service interruption of an authorized terminal device, service performance deterioration of the terminal device, abnormal power consumption of the terminal device, and abnormal resource scheduling of the network device. The network device is a base station, and the terminal device is UE. As shown in FIG. 4, a procedure in which the attacker eavesdrops on a PDCCH resource configuration and spoofs DCI includes the following steps.

[0076] **S401:** The attacker listens, on a physical broadcast channel (PBCH), to a master information block (MIB) sent by an authorized base station, and obtains information element parameters, namely, a control resource set (CORESET) 0 and search space (SearchSpace) 0 in the MIB, where the MIB may carry a physical cell identifier (PCI).

[0077] **S402:** The attacker listens to DCI of a system information block (SIB) 1 on a PDCCH CORESET 0 and SearchSpace 0, and obtains information such as a time-frequency resource location of the SIB 1; listens to the SIB 1 on a physical downlink shared channel (PDSCH), to obtain an information element RACH-ConfigCommon in the SIB 1, indicating a configuration such as a random access channel time-frequency resource/preamble/response window; and calculates a possible value (used to receive a random access message 2 (Msg2)) of a random access radio network temporary identifier (RA-RNTI) based on these parameters.

[0078] **S403:** The attacker listens to Msg2 based on the RA-RNTI, and obtains a temporary cell radio network temporary identifier (TC-RNTI) carried in Msg2.

[0079] **S404:** The attacker listens to a random access message 4 (Msg4) based on the TC-RNTI, and obtains a parameter such as user-level CORESET/SearchSpace of an information element bandwidth part (BWP) 0 in Msg4. The UE contends for random access. After contention succeeds, the TC-RNTI is upgraded to a cell radio network temporary identifier (C-RNTI). The attacker can obtain, through listening, a C-RNTI allocated by the authorized base station to a user.

[0080] **S405:** The authorized base station delivers an encrypted RRC reconfiguration message, where the user-level CORESET and SearchSpace parameters may be the same as those delivered in a plaintext form in Msg4.

[0081] **S406:** Optionally, the attacker continues to listen to key DCI delivered by the authorized base station, performs blind detection for a plurality of times, and further guesses a parameter configuration of user-level CORESET and SearchSpace.

[0082] **S407:** The attacker spoofs the key DCI based on the user-level CORESET and SearchSpace parameters obtained in the foregoing steps.

[0083] In the foregoing procedure, a DCI format includes downlink PDSCH scheduling, uplink PUSCH scheduling, a slot format indication, a resource preemption indication, transmission power control, sidelink scheduling, multicast broadcast service (MBS) scheduling, and the like. For different DCI formats, refer to section 7.3.1 in the 3rd generation partnership project (3GPP) standard TS38.212.

[0084] PDCCH SearchSpace includes common SearchSpace and UE-specific SearchSpace. Common SearchSpace is mainly used to transmit scheduling DCI of system information, a random access response (RAR), a paging message, and the like. UE-specific SearchSpace is mainly used to transmit user-specific information, for example, uplink/downlink user data scheduling or an uplink (UL) grant. For common SearchSpace, the attacker may determine a location of common SearchSpace based on a cell common parameter delivered by the authorized base station, and then perform attacks such as interference, spoofing, and tampering on authorized UE. UE-dedicated SearchSpace is mainly delivered through Msg4 and the RRC reconfiguration message. If UE-specific CORESET and SearchSpace information element parameters delivered through the RRC reconfiguration message are completely the same as or partially the same as those delivered through Msg4, the attacker can perform blind detection on UE-specific DCI delivered by the authorized base station, and guess the UE-specific CORESET and SearchSpace information element parameters. Consequently, the attacker can easily perform attacks such as interference, spoofing, and tampering on the authorized UE.

[0085] The attacker can spoof DCI format 1_0 scrambled by using the P-RNTI at a paging occasion (PO) location. The DCI includes a short message indicating a system message change. A tampered system message may be used to further prohibit calling and called services of the authorized UE. The attacker may alternatively spoof a DCI instruction of a PDCCH order based on the C-RNTI, so that the authorized UE continuously initiates random access and cannot obtain a normal network service. The attacker may alternatively listen to a DCI activation instruction of a UL grant type 2 delivered by the authorized base station, and obtain UE-specific parameters such as a configured scheduling RNTI (CS-RNTI) and user-level CORESET/SearchSpace by per-

forming blind detection for a plurality of times. In this way, the attacker spoofs a DCI deactivation instruction, so that the user cannot use a grant-free scheduling resource, and the UE cannot reach a short-delay performance indicator.

[0086] The attacker may eavesdrop the MIB, the SIB 1, Msg2, and Msg4, to obtain common CORESET and SearchSpace, or obtain user-specific CORESET and SearchSpace of a BWP 0 delivered in Msg4 in a plaintext form, and obtain a temporary identifier such as a C-RNTI of an authorized user. Therefore, key DCI signaling can be spoofed and tampered with. Although user-specific CORESET and SearchSpace are re-delivered through the RRC reconfiguration message with encryption and integrity protection, if user-specific CORESET and SearchSpace parameters in the RRC reconfiguration message are partially the same as user-specific CORESET and SearchSpace parameters in Msg4, for example, a PDCCH demodulation reference signal (DMRS) scrambling ID (pdcch-DMRS-ScramblingID) parameter, the attacker can easily crack user-specific DCI with a small amount of time and low costs. The attacker may alternatively spoof the authorized UE to access a base station and obtain user-specific CORESET and SearchSpace configurations. If a plurality of users served by a same base station have many same CORESET and SearchSpace parameter configurations, for example, a same parameter such as a frequency domain resource (frequencyDomainResources) in the CORESET information element, the attacker can easily crack and spoof DCI sent to other UE.

[0087] In view of this, this disclosure provides a communication method and apparatus, to improve security of underlying signaling transmitted between a network device and a terminal device, and enhance security strength of anti-eavesdropping and anti-tampering of the underlying signaling. The following describes in detail embodiments of this disclosure with reference to accompanying drawings.

[0088] In addition, it should be understood that ordinal numbers such as “first” and “second” mentioned in embodiments of this disclosure are used to distinguish between a plurality of objects, and are not used to limit sizes, content, a sequence, a time sequence, priorities, importance degrees, or the like of the plurality of objects. For example, a first random number and a second random number do not indicate different priorities, importance degrees, or the like corresponding to the two random numbers.

[0089] In embodiments of this disclosure, unless otherwise specified, a quantity of nouns represents “a singular noun or a plural noun”, that is, “one or more”. “At least one” means one or more, and “a plurality of” means two or more. “And/or” describes an association relationship between associated objects and indicates that at least three relationships may exist. For example, A and/or B may indicate the following three cases: Only A exists, both A and B exist, and only B exists, where A and B may be singular or plural. The character “/” usually indicates an “or” relationship between the associated objects. For example, A/B indicates A or B. “At least one of the following items (pieces)” or a similar expression thereof indicates any combination of these items, including a single item (piece) or any combination of a plurality of items (pieces). For example, at least one item (piece) of a, b, or c indicates: a, b, c, a and b, a and c, b and c, or a, b, and c, where a, b, and c may be singular or plural.

[0090] FIG. 5 is a diagram of a communication method according to an embodiment of this disclosure. In FIG. 5, the

method is described by using an example in which a terminal device and a network device serve as execution bodies. This disclosure does not limit an execution body of the method. For example, the terminal device in FIG. 5 may alternatively be a chip, a chip system, or a processor that can support the terminal device in implementing the method, or may be a logical module or software that can implement all or some of functions of the terminal device. Alternatively, the network device in FIG. 5 may be a chip, a chip system, or a processor that supports the network device in implementing the method, or may be a logical module or software that can implement all or some of functions of the network device. In addition, in FIG. 5, descriptions are provided by using an example in which a physical channel is a PDCCH. It may be understood that the physical channel may alternatively be a PDSCH, a PUCCH, a PUSCH, or the like. The method includes the following steps.

[0091] S501: The terminal device generates, by using a random number generator, at least one random number based on a user-specific parameter of the PDCCH from the network device and a specified historical message exchanged between the terminal device and the network device, where the at least one random number includes a first random number.

[0092] In this embodiment of this disclosure, the user-specific parameter that is of the PDCCH and that is sent by the network device to the terminal device may be information element parameters such as a PDCCH scrambling ID (for example, pdcch-DMRS-ScramblingID) and time-frequency resource information of user-level CORESET/SearchSpace that are delivered by the network device to the terminal device by using an RRC reconfiguration message. Optionally, to prevent an attacker from learning of the user-specific parameter of the PDCCH, the user-specific parameter that is of the PDCCH and that is sent by the network device to the terminal device is not the same as a user-specific parameter that is of the PDCCH and that is sent by the network device in a plaintext form, and is randomly configured by the network device, to increase randomness and unpredictability of the user-specific parameter that is of the PDCCH and that is sent by the network device to the terminal device. For example, when the user-specific parameter of the PDCCH is pdcch-DMRS-ScramblingID in the RRC reconfiguration message, a value of pdcch-DMRS-ScramblingID in the RRC reconfiguration message is different from a value of pdcch-DMRS-ScramblingID in a random access message (Msg4) sent by the network device, and is randomly configured by the network device, to increase randomness and unpredictability of pdcch-DMRS-ScramblingID, and prevent pdcch-DMRS-ScramblingID from being obtained or predicted by the attacker.

[0093] For example, the user-specific parameter of the PDCCH is pdcch-DMRS-ScramblingID delivered by the network device by using the RRC reconfiguration message. pdcch-DMRS-ScramblingID is related to generation of a PDCCH scrambling sequence and a PDCCH pilot sequence (for example, a PDCCH DMRS sequence). To avoid confusion between DCI sent to different terminal devices in a cell, it needs to be ensured as much as possible that PDCCH scrambling sequences and PDCCH pilot sequences of different terminal devices in a same cell do not conflict simultaneously. Usually, during cell deployment, physical shared channel (PSCH) mod 3 interference of different cells

is avoided. In other words, cells with a same physical cell identifier (PCI) mod 3 usually are not deployed together.

[0094] To ensure randomness and unpredictability of pdcch-DMRS-ScramblingID in the RRC reconfiguration message, the network device may configure pdcch-DMRS-ScramblingID in the following manner. Currently, pdcch-DMRS-ScramblingID in the 3GPP standard has a length of 16 bits, and has 65536 value spaces. The network device may first remove a pdcch-DMRS-ScramblingID set configured and used in Msg4 in a plaintext form. For example, there are 4800 pdcch-DMRS-ScramblingID. Then, a remaining pdcch-DMRS-ScramblingID value set is divided into three groups based on a case in which PCI mod 3 is equal to 0, 1, or 2. A quantity of pdcch-DMRS-ScramblingID in each group is floor $(65536-4800)/3=24245$. Herein, floor indicates rounding down. Each cell of the network device selects a corresponding pdcch-DMRS-ScramblingID value set based on PCI mod 3 of the cell, to allocate a value of pdcch-DMRS-ScramblingID of a user in the cell. In addition, random allocation is maintained as much as possible. FIG. 6 is a diagram of scrambling ID (for example, pdcch-DMRS-ScramblingID) allocation. The network device may periodically perform random scrambling on a scrambling ID queue that is not allocated in a cell in which the terminal device is located, and extract a new scrambling ID from a head of the queue when the new scrambling ID is delivered to a user by using the RRC reconfiguration message. After an RRC connection of the user is released, a corresponding scrambling ID is placed at a tail of the queue.

[0095] The specified historical message exchanged between the terminal device and the network device may be sent by the terminal device to the network device, and the network device confirms a received historical message; or the specified historical message may be delivered by the network device to the terminal device, and the terminal device confirms a received message. For example, the specified historical message may be a measurement value in a measurement report (MR) in RRC signaling reported by the terminal device to the network device, or may be a NAS message, for example, a dedicated NAS message (DedicatedNAS-Message) for transmitting UE-specific NAS stratum signaling.

[0096] For example, the specified historical message exchanged between the terminal device and the network device is an L3 layer measurement value in the measurement report. A measurement object is a serving cell and a neighboring cell. The measurement value includes beam measurement values (for example, a beam ID, reference signal received power (RSRP), reference signal received quality (RSRQ), a signal to interference plus noise ratio (SINR), and the like) of the serving cell and the neighboring cell. The network device may configure the measurement report to be periodically fed back. When the random number is generated, a specified historical message used by the terminal device or the network device is a most recently exchanged specified historical message obtained by the terminal device or the network device based on a specified periodicity (for example, a periodicity configured by the network device). As shown in FIG. 7, a measurement value in an L3 RRC signaling MR measurement report may include RSRP, RSRQ, and an SINR at a cell (for example, a serving cell of the terminal device) level, and RSRP, RSRQ, and an SINR at a beam (for example, one or more beams corresponding to the serving cell of the terminal device) level.

[0097] For example, the specified historical message exchanged between the terminal device and the network device is an L1 layer measurement value in the measurement report. A measurement object is a serving cell of the terminal device, and the measurement value (namely, a measurement feedback amount) includes a channel measurement amount (including a precoding matrix indication (PMI), a channel quality indicator (CQI), a rank indicator (RI), and the like) and a beam measurement amount (for example, a beam ID and corresponding RSRP) of the serving cell. The L1 measurement feedback amount usually includes frequency-domain subband-level measurement information. There is richer feedback information and a shorter feedback period. Therefore, it is difficult for the attacker to always perform eavesdropping and tracing.

[0098] The random number generator may be referred to as a randomness extractor, and may be a hash algorithm, a deterministic random bit generator (DRBG), a one-way hash algorithm deterministic random bit generator (Hash-DRBG), a hash information authentication code deterministic random bit generator (hash-based message authentication code DRBG (HMAC-DRBG)), a counter mode deterministic random bit generator (counter DRBG (CTR-DRBG)), and the like. The DRBG is also referred to as a pseudo random number generator (PRNG).

[0099] After obtaining the user-specific parameter of the PDCCH from the network device and the specified historical message exchanged between the terminal device and the network device, the terminal device may generate the at least one random number based on the user-specific parameter and the specified historical message by using the random number generator.

[0100] S502: The terminal device generates a PDCCH encryption key based on the first random number by using a key generator.

[0101] In this embodiment of this disclosure, the key generator may derive (or generate) the PDCCH encryption key by using a cryptographic key derivation algorithm, a chaotic mathematical model, or the like.

[0102] In an example, the key generator may use a password-based key derivation function 2 (PBKDF2), a script key derivation algorithm, or the like, or may use a key-based key derivation algorithm (e.g. use a key-based key derivation function (KBKDF)) with a relatively faster computing speed, for example, a key derivation algorithm such as a counter mode-based KDF, a feedback mode-based KDF, and a double-pipeline iteration mode-based KDF mentioned in SP800 (SP800 is a series of guidelines on information security released by the national institute of standards and technology (NIST)). As shown in FIG. 8, when the PDCCH encryption key is generated based on the key derivation algorithm, two random numbers (for example, two first random numbers used to generate the PDCCH encryption key) generated by using the random number generator may be respectively used as a key material (also referred to “key”): Q and a salt value (also referred to “salt”): P, and the key derivation algorithm is input to generate the PDCCH encryption key.

[0103] In another example, the key generator may use, as a chaotic parameter based on a specific combination rule by using a mathematical model such as chaotic distribution, one or more first random numbers output by the random number generator to generate the PDCCH encryption key, to generate “long random chaotic sequence x” based on chaotic

mapping. A length of the long random chaotic sequence may support different physical layer encryption keys of each signaling within a PDCCH encryption key updating period. For example, if the updating period is 20 ms, there are a total of 40 slots, and physical layer encryption needs to be performed on 5000 constellation points in each slot, a length of a long random chaotic sequence that may be generated is $200000=40*5000$. In this case, different physical layer encryption keys are used in all the slots. The mathematical model such as the chaotic distribution may be a chaotic logistic model, a chaotic Chebyshev model, or the like.

[0104] (1) The chaotic logistic model is used, and it may be set that $y_0=P$ (Chaotic initial value=First random number 1), and $\mu=Q$ (Bifurcation parameter-First random number 2). An element value (x) in the long random chaotic sequence may be determined based on the following formula, and is used as the PDCCH encryption key. A value of x ranges from -1 to 1 .

$$y_{n+1} = \mu * y_n(1 - y_n), y \in (0.0, 1.0), 3.569945672 < \mu \leq 4.0; \text{ and} \\ x = 1 - 2 * y, x \in (-1.0, 1.0).$$

[0105] (2) The chaotic Chebyshev model is used, and it may be chosen to set that $x_0=P$ (Chaotic initial value=First random number 1), and $\mu=Q$ (Bifurcation parameter-First random number 2). A value of each element (x_{n+1}) in the long random chaotic sequence may be determined based on the following formula, and is used as the PDCCH encryption key.

$$x_{n+1} = \cos(\mu * \cos^{-1}(x_n)), x \in (-1.0, 1.0), 2.0 < \mu$$

[0106] It may be understood that the terminal device may periodically generate the PDCCH encryption key based on a key generation period, and update a used PDCCH encryption key, to improve security. In some implementations, to avoid a repetition of the generated PDCCH encryption key, the terminal device may further add anti-replay information to the PDCCH encryption key generated by using the key generator. The anti-replay information may be a transmit frequency, a PCI, a timestamp, or the like. The timestamp may be time domain information such as a system frame number and a slot number when the PDCCH encryption key is updated. The terminal device may also use the anti-reply information as an input into the key generator, for example, splice the anti-replay information with the salt value: P as a new salt value: P; or may splice the anti-replay information with the PDCCH encryption key output by the key generator to obtain a new PDCCH encryption key.

[0107] S503: The terminal device decrypts the PDCCH based on the PDCCH encryption key, and correspondingly, the network device encrypts the PDCCH based on the PDCCH encryption key.

[0108] In this embodiment of this disclosure, the network device may generate the PDCCH encryption key in a manner similar to that of the terminal device. For a specific process of generating the PDCCH encryption key, refer to an implementation on a terminal device side.

[0109] After determining the PDCCH encryption key, the terminal device and the network device may encrypt and

decrypt the PDCCH based on the PDCCH encryption key. For example, the network device may encrypt the PDCCH (for example, DCI carried on the PDCCH) based on the PDCCH encryption key, and the terminal device may also decrypt the PDCCH based on the PDCCH encryption key, to provide protection for the PDCCH (for example, the DCI carried on the PDCCH).

[0110] In some embodiments, a quantity of bits of a scrambling-specific parameter (for example, pdcch-DMRS-ScramblingID) that is of the PDCCH and that is sent by the network device to the terminal device may also be increased, and random space of the user-specific parameter is increased, to increase difficulty in cracking by the attacker.

[0111] For example, the scrambling-specific parameter of the PDCCH is pdcch-DMRS-ScramblingID, and a bit length of an information element parameter pdcch-DMRS-ScramblingID included in CORESET in a current 3GPP standard is 16 bits. In this embodiment of this disclosure, 16 bits may be used as a first threshold, and a quantity of bits of pdcch-DMRS-ScramblingID is increased, so that a length of pdcch-DMRS-ScramblingID is greater than the first threshold, for example, is 24, 28, or 32 bits. pdcch-DMRS-ScramblingID is used for generation of the PDCCH scrambling sequence and generation of the PDCCH pilot sequence at a physical layer. When the length of pdcch-DMRS-ScramblingID is increased, in this embodiment of this disclosure, a selection rule of selecting a value of pdcch-DMRS-ScramblingID may be separately configured for the PDCCH scrambling sequence and the PDCCH pilot sequence, to generate the PDCCH scrambling sequence and the PDCCH pilot sequence. For example, for the PDCCH scrambling sequence, a configured first selection rule may be selecting first 16 bits, last 16 bits, or the like of pdcch-DMRS-ScramblingID, and a second selection rule may be selecting last 16 bits, first 16 bits, or the like of pdcch-DMRS-ScramblingID. The first selection rule and the second selection rule may be the same or different.

[0112] For example, the length of pdcch-DMRS-ScramblingID is 32 bits. As shown in FIG. 9, the first selection rule may be that the first 16 bits of pdcch-DMRS-ScramblingID are selected as a first sub-scrambling parameter to generate the PDCCH scrambling sequence, and the second selection rule may be that the last 16 bits of pdcch-DMRS-ScramblingID are selected as a second sub-scrambling parameter to generate the PDCCH pilot sequence (for example, a PDCCH DMRS sequence). As shown in FIG. 10, the first selection rule may be that the last 16 bits of pdcch-DMRS-ScramblingID are selected as a first sub-scrambling parameter to generate the PDCCH scrambling sequence, and the second selection rule may be that the first 16 bits of pdcch-DMRS-ScramblingID are selected as a second sub-scrambling parameter to generate the PDCCH pilot sequence (for example, a PDCCH DMRS sequence). As shown in FIG. 11, the first selection rule may be that pdcch-DMRS-ScramblingID is divided into a plurality of subblocks based on M bits (M may be 2, 4, 6, 8, or the like). For example, when M=4, pdcch-DMRS-ScramblingID is divided into eight subblocks, and each subblock has 4 bits. Even-numbered index blocks are recombined into 16 bits and used as the first sub-scrambling parameter to generate the PDCCH scrambling sequence. The second selection rule may be that pdcch-DMRS-ScramblingID is divided into a plurality of subblocks based on M bits (M may be 2, 4, 6, 8, or the like). Odd-numbered index blocks are recombined

into 16 bits and used as the second sub-scrambling parameter, to generate the PDCCH pilot sequence (for example, the PDCCH DMRS sequence).

[0113] In an example, the PDCCH scrambling sequence may be a pseudo-random sequence, and initialization for generation of the PDCCH scrambling sequence may be as follows:

$$c_{init} = (n_{RNTI} \cdot 2^{16} + n_{ID}) \bmod 2^{31}$$

[0114] First sub-scrambling parameter n_{ID} : For terminal device-specific search space, if a higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$ is configured, $n_{ID} \in \{0, 1, \dots, 65535\}$ is equal to first 16 bits of the higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$; and for a case in which an RNTI for scrambling a cyclic redundancy check (CRC) of the PDCCH in common search space is a G-RNTI, a G-CS-RNTI, an MCCH-RNTI, or the like, if a higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$ is configured on a common MBS frequency domain resource, $n_{ID} \in \{0, 1, \dots, 65535\} \in \{0, 1, \dots, 65535\}$ is equal to first 16 bits of the higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$.

[0115] n_{RNTI} : If the higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$ is configured, n_{RNTI} is equal to a C-RNTI in search space. In another case, $n_{RNTI} = 0$.

[0116] c_{init} indicates an initial value of the PDCCH scrambling sequence.

[0117] The foregoing provides descriptions by using an example in which the first selection rule is selecting the first 16 bits of $\text{pdccch-DMRS-ScramblingID}$ as the first sub-scrambling parameter. It may be understood that the first selection rule is not limited to selecting the first 16 bits of $\text{pdccch-DMRS-ScramblingID}$ as the first sub-scrambling parameter. Alternatively, the last 16 bits of $\text{pdccch-DMRS-ScramblingID}$ may be selected as the first sub-scrambling parameter, or the like.

[0118] The PDCCH pilot sequence (for example, the PDCCH DMRS sequence) $r_f(m)$ is generated as follows:

$$r_f(m) = \frac{1}{\sqrt{2}}(1 - 2 \cdot c(2m)) + j \frac{1}{\sqrt{2}}(1 - 2 \cdot c(2m + 1))$$

[0119] Initialization (c_{init}) of the pseudo-random sequence $c(i)$ is as follows:

$$c_{init} = (2^{17} (N_{slot}^{slot} n_{s,f}^{\mu} + l + 1) (2N_{ID} + 1) + 2N_{ID}) \bmod 2^{31}$$

blingID is configured, $N_{ID} \in \{0, 1, \dots, 65535\}$ is equal to the last 16 bits of the higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$; and if the higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$ is configured in the common search space on the common MBS frequency domain resource, $N_{ID} \in \{0, 1, \dots, 65535\}$ is equal to the last 16 bits of the higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$. In another case, $N_{ID} = N_{ID}^{cell}$.

[0122] The foregoing provides descriptions by using an example in which the second selection rule is selecting the last 16 bits of $\text{pdccch-DMRS-ScramblingID}$ as the second sub-scrambling parameter. It may be understood that the second selection rule is not limited to selecting the last 16 bits of $\text{pdccch-DMRS-ScramblingID}$ as the second sub-scrambling parameter. Alternatively, the first 16 bits of $\text{pdccch-DMRS-ScramblingID}$ may be selected as the second sub-scrambling parameter, or the like.

[0123] Different cells independently configure and deliver scrambling-specific parameters. There is a specific conflict probability. FIG. 12 is a diagram of a conflict between scrambling-specific parameters. A horizontal axis represents a quantity of cells, and a vertical axis represents a conflict probability of the scrambling-specific parameter. In FIG. 12, the scrambling-specific parameter is $\text{pdccch-DMRS-ScramblingID}$. It can be learned from FIG. 12 that when the bit length of $\text{pdccch-DMRS-ScramblingID}$ is 16 bits, a conflict probability of $\text{pdccch-DMRS-ScramblingID}$ of cells is $1.526\text{e-}5$. When the bit length of $\text{pdccch-DMRS-ScramblingID}$ is 32 bits, the conflict probability of $\text{pdccch-DMRS-ScramblingID}$ of cells is $2.328\text{e-}10$. The bit length of $\text{pdccch-DMRS-ScramblingID}$ is increased, so that the conflict probability of $\text{pdccch-DMRS-ScramblingID}$ of the cells is greatly reduced, and inter-cell DCI sending interference is reduced.

[0124] If there are four candidate sets in the terminal device-specific search space, blind detection needs to be performed for four times. It is assumed that one time of DCI blind detection takes 5 microseconds (μs). Cracking time used when a single attacker may concurrently perform 64 threads is shown in the following formula. The attacker does not learn of the value of $\text{pdccch-DMRS-ScramblingID}$ delivered in an encryption manner. Therefore, the attacker needs to perform traversal to try all possible values. When the bit length of $\text{pdccch-DMRS-ScramblingID}$ is 16 bits, it needs to take the attacker approximately 0.02 seconds to crack the DCI. When the bit length of $\text{pdccch-DMRS-ScramblingID}$ is 32 bits, it needs to take the attacker 1342 seconds to crack the DCI. A random bit length of $\text{pdccch-DMRS-ScramblingID}$ is increased, so that security of the DCI can be greatly improved.

$$16 \text{ bits: } \sim 5 \mu\text{s} * (2^{16}) * 4 \text{ candidate sets} / 64 / 1000 / 1000 = 0.02 \text{ seconds.}$$

$$32 \text{ bits: } \sim 5 \mu\text{s} * (2^{32}) * 4 \text{ candidate sets} / 64 / 1000 / 1000 = 1342 \text{ seconds.}$$

[0120] Herein, l is an OFDM symbol index in a slot, $n_{s,f}^{\mu}$ is a slot index number in a system frame, and j is an imaginary unit.

[0121] The second sub-scrambling parameter N_{ID} is defined as follows: For the terminal device-specific search space, if the higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$ is configured, $N_{ID} \in \{0, 1, \dots, 65535\}$ is equal to the last 16 bits of the higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$; and if the higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$ is configured in the common search space on the common MBS frequency domain resource, $N_{ID} \in \{0, 1, \dots, 65535\}$ is equal to the last 16 bits of the higher-layer parameter $\text{pdccch-DMRS-ScramblingID}$. In another case, $N_{ID} = N_{ID}^{cell}$.

[0125] In some implementations, to further improve security, the terminal device may further update the PDCCH update the PDCCH pilot sequence corresponding to the PDCCH based on the random number generated by the random number generator. scrambling sequence corresponding to the PDCCH and/or

[0126] In an example, when generating, by using the random number generator, the at least one random number based on the user-specific parameter of the PDCCH and the specified historical message exchanged between the terminal device and the network device, the terminal device may further generate a second random number used to update the PDCCH scrambling sequence. The second random number may be the same as or different from the first random number used to generate the PDCCH encryption key. After obtaining the second random number, the terminal device may update the PDCCH scrambling sequence based on the second random number. For example, the second random number is used as a new scrambling ID parameter to generate a new PDCCH scrambling sequence, or the first sub-scrambling parameter is selected from the second random number based on the first selection rule. The first sub-scrambling parameter is used to generate the new PDCCH scrambling sequence.

[0127] Similarly, when generating, by using the random number generator, the at least one random number based on the user-specific parameter of the PDCCH and the specified historical message exchanged between the terminal device and the network device, the terminal device may further generate a third random number used to update the PDCCH pilot sequence (for example, the PDCCH DMRS sequence). The third random number may be the same as the first random number or the second random number, or may be different from both the first random number and the second random number. After obtaining the third random number, the terminal device may update the PDCCH scrambling sequence based on the third random number. For example, the third random number is used as a new scrambling ID parameter to generate a new PDCCH scrambling sequence, or the second sub-scrambling parameter is selected from the third random number based on the second selection rule. The second sub-scrambling parameter is used to generate the new PDCCH scrambling sequence.

[0128] FIG. 13 is a diagram of enhancing PDCCH security protection according to an embodiment of this disclosure. The terminal device may periodically generate, by using the random number generator, the at least one random number based on the user-specific parameter that is of the PDCCH and that is delivered by the network device by using the RRC reconfiguration message and the specified historical message exchanged between the terminal device and the network device. The user-specific parameter of the PDCCH may be a parameter such as `pdccch-DMRS-ScramblingID` in user-level CORESET, and the specified historical message exchanged between the terminal device and the network device may be an RRC message, for example, `MeasurementReport` reported by the terminal device by using an RRC message; or may be a NAS message, for example, a `DedicatedNAS-Message`.

[0129] The terminal device may generate, by using the key generator, the PDCCH encryption key based on the random number (for example, the first random number) generated by using the random number generator; or may update the PDCCH scrambling sequence and the PDCCH pilot sequence (for example, the PDCCH DMRS sequence) based on random numbers (for example, the second random number and the third random number) generated by using the random number generator. Similarly, the network device may also determine the PDCCH encryption key in a manner similar to that of the terminal device, and update the PDCCH

scrambling sequence and the PDCCH pilot sequence (for example, the PDCCH DMRS sequence).

[0130] FIG. 14 is a diagram of physical layer PDCCH encryption. The network device may send PDCCH to-be-transmitted information (for example, the DCI) through an air interface by performing one or more items of processing such as adding a cyclic redundancy check (CRC), a radio network temporary identifier (RNTI) masking, polar encoding, rate matching/interleaving, scrambling, quadrature amplitude modulation (QAM), resource mapping, inverse fast Fourier transform (IFFT), and adding a cyclic prefix (CP). The terminal device performs processing such as removing the CP, fast Fourier transform (FFT), demapping, channel estimation, multiple input multiple output (MIMO) decoding, QAM demodulation, descrambling/rate de-matching, polar decoding, RNTI de-masking, and a CRC check on a received signal, to obtain transmitted information (for example, the DCI). The network device may encrypt the PDCCH to-be-transmitted information (for example, the DCI) based on the PDCCH encryption key before the CRC is added, or before resource mapping, or after resource mapping. The terminal device may decrypt the PDCCH to-be-transmitted information based on the PDCCH encryption key after the CRC check, or after demapping, or before demapping.

[0131] In addition, the terminal device and the network device may further update the PDCCH scrambling sequence and the PDCCH pilot sequence based on the random numbers (for example, the second random number and the third random number) generated by the random number generator. The network device performs scrambling and resource mapping on the PDCCH based on a last obtained PDCCH scrambling sequence and PDCCH pilot sequence. The terminal device performs descrambling and channel estimation on the physical channel based on the last obtained PDCCH scrambling sequence and PDCCH pilot sequence.

[0132] The PDCCH to-be-transmitted information (for example, the DCI) may be encrypted through bit-level encryption by using the PDCCH encryption key. For example, before the CRC is added, a bit sequence of the transmitted information may be encrypted based on a conventional cryptographic encryption algorithm (for example, AES, Zuc, or Snow).

[0133] Certainly, the PDCCH to-be-transmitted information (for example, the DCI) may alternatively be encrypted by using a complex field and the PDCCH encryption key. For example, complex field encryption may be performed on the PDCCH to-be-transmitted information by performing an operation such as constellation phase rotation or data and pilot subcarrier hybrid interleaving. As shown in FIG. 15, when encryption is performed through constellation phase rotation, a constellation phase encryption key K may be first calculated. Herein, $K = x * 2\pi$, and $K \in (-2\pi, 2\pi)$. Then, constellation phase rotation is performed based on K . $S' = S * ejK$. Herein, S' is an encrypted constellation point, x represents an element in the PDCCH encryption key, and S is a constellation point existing before encryption, for example, data obtained after encoding and QAM modulation are performed on a PDCCH physical transmission payload. As shown in FIG. 16, when data and pilot subcarrier hybrid interleaving encryption is performed, the PDCCH encryp-

tion key may be processed and converted into an encrypted interleaving index, and the data and pilot subcarrier coordinate information is re-arranged and disordered, to implement encryption.

[0134] It may be understood that the foregoing provides descriptions by using an example in which the physical channel is a PDCCCH. It may be understood that the physical channel may alternatively be a PDSCH, a PUCCH, a PUSCH, or the like.

[0135] For example, the physical channel is a PDSCH. FIG. 17 is a diagram of enhancing PDSCH security protection according to an embodiment of this disclosure. The terminal device may periodically generate, by using the random number generator, the at least one random number based on a user-specific parameter that is of a PDSCH and that is delivered by the network device by using the RRC reconfiguration message and the specified historical message exchanged between the terminal device and the network device. The user-specific parameter of the PDSCH may be an information element parameter such as a scrambling ID (for example, a data scrambling identity PDSCH (dataScramblingIdentityPDSCH)) in a user-level PDSCH configuration (PDSCH-Config), or a scrambling ID 0 and a scrambling ID 1 in a DMRS downlink configuration (DMRS-DownlinkConfig). The user-specific parameter of the PDSCH needs to be random and unpredictable, and cannot be the same as those sent in a plaintext form. The specified historical message exchanged between the terminal device and the network device may be an RRC message, for example, MeasurementReport reported by the terminal device by using the RRC message; or may be a NAS message, for example, DedicatedNAS-Message; or may be PDSCH payload data received by the terminal device in a same downlink HARQ process.

[0136] The terminal device may generate, by using the key generator, the PDSCH encryption key based on the random number (for example, the first random number) generated by using the random number generator; or may update the PDSCH scrambling sequence and the PDSCH pilot sequence (for example, the PDSCH DMRS sequence) based on random numbers (for example, the second random number and the third random number) generated by using the random number generator. Similarly, the network device may also determine the PDSCH encryption key in a manner similar to that of the terminal device, and update the PDSCH scrambling sequence and the PDSCH pilot sequence (for example, the PDSCH DMRS sequence).

[0137] For example, the physical channel is a PUSCH. FIG. 18 is a diagram of enhancing PUSCH security protection according to an embodiment of this disclosure. The terminal device may periodically generate, by using the random number generator, the at least one random number based on a user-specific parameter that is of a PUSCH and that is delivered by the network device by using the RRC reconfiguration message and the specified historical message exchanged between the terminal device and the network device. The user-specific parameter of the PUSCH may be an information element parameter such as a scrambling ID (for example, a data scrambling identity PUSCH (dataScramblingIdentityPUSCH)) in a user-level PUSCH configuration (PUSCH-Config), or a scrambling ID 0 and a scrambling ID 1 in a DMRS uplink configuration (DMRS-UplinkConfig). The user-specific parameter of the PUSCH needs to be random and unpredictable, and cannot be the

same as those sent in a plaintext form. The specified historical message exchanged between the terminal device and the network device may be an RRC message, for example, MeasurementReport reported by the terminal device by using the RRC message; or may be a NAS message, for example, DedicatedNAS-Message; or may be PUSCH payload data received by the terminal device in a same downlink HARQ process.

[0138] The terminal device may generate, by using the key generator, the PUSCH encryption key based on the random number (for example, the first random number) generated by using the random number generator; or may update the PUSCH scrambling sequence and the PUSCH pilot sequence (for example, the PUSCH DMRS sequence) based on random numbers (for example, the second random number and the third random number) generated by using the random number generator. Similarly, the network device may also determine the PUSCH encryption key in a manner similar to that of the terminal device, and update the PUSCH scrambling sequence and the PUSCH pilot sequence (for example, the PUSCH DMRS sequence).

[0139] It can be understood that, to implement the functions in the foregoing embodiments, the terminal device and the network device include corresponding hardware structures and/or software modules for performing the functions. A person skilled in the art should be easily aware that, in this disclosure, the units and method steps in the examples described with reference to embodiments disclosed in this disclosure can be implemented by hardware or a combination of hardware and computer software. Whether a function is performed by hardware or hardware driven by computer software depends on particular application scenarios and implementation constraint conditions of the technical solutions.

[0140] FIG. 19 and FIG. 20 each are a diagram of a structure of a possible communication apparatus according to an embodiment of this disclosure. The communication apparatus may be configured to implement the functions of the terminal device or the network device in the foregoing method embodiments. Therefore, beneficial effects of the foregoing method embodiments can also be implemented. In a possible implementation, the communication apparatus may be a terminal device or a network device, or may be a module (for example, a chip) applied to the terminal device or the network device.

[0141] As shown in FIG. 19, the communication apparatus 1900 includes a processing unit 1910 and an interface unit 1920. The interface unit 1920 may alternatively be a transceiver unit or an input/output interface. The communication apparatus 1900 may be configured to implement the functions of the terminal device or the network device in the method embodiment shown in FIG. 7.

[0142] When the communication apparatus 1900 is configured to implement the function of the terminal device in the method embodiment shown in FIG. 5, the interface unit 1920 is configured to receive a user-specific parameter of a physical channel from a network device; the processing unit 1910 is configured to: generate, by using a random number generator, at least one random number based on the user-specific parameter and a specified historical message exchanged with the network device, where the at least one random number includes a first random number; and generate a physical channel encryption key based on the first random number by using a key generator; and the processing

unit **1910** is further configured to encrypt or decrypt the physical channel based on the physical channel encryption key.

[0143] In some embodiments, the at least one random number further includes a second random number, and the processing unit **1910** is further configured to: update, based on the second random number, a physical channel scrambling sequence corresponding to the physical channel; and scramble or descramble the physical channel based on an updated physical channel scrambling sequence.

[0144] In some embodiments, the at least one random number further includes a third random number, and the processing unit **1910** is further configured to: update, based on the third random number, a physical channel pilot sequence corresponding to the physical channel; and perform resource mapping or channel estimation on the physical channel based on an updated physical channel pilot sequence.

[0145] In some embodiments, the interface unit **1920** is further configured to receive a scrambling-specific parameter of the physical channel from the network device. A quantity of bits included in the scrambling-specific parameter is greater than a first quantity threshold. The processing unit **1910** is further configured to: generate, based on a first sub-scrambling parameter, the physical channel scrambling sequence corresponding to the physical channel, where the first sub-scrambling parameter is determined by the processing unit **1910** based on a first selection rule and the scrambling-specific parameter, and a quantity of bits included in the first sub-scrambling parameter is equal to the first quantity threshold; and generate, based on a second sub-scrambling parameter, the physical channel pilot sequence corresponding to the physical channel. The second sub-scrambling parameter is determined by the processing unit **1910** based on a second selection rule and the scrambling-specific parameter, and a quantity of bits included in the second sub-scrambling parameter is equal to the first quantity threshold.

[0146] In some embodiments, when generating, by using the random number generator, the at least one random number based on the user-specific parameter and the specified historical message exchanged between the interface unit **1920** and the network device, the processing unit **1910** is specifically configured to: obtain, through the interface unit **1920** based on a specified periodicity, a specified historical message most recently exchanged with the network device; and generate the at least one random number based on the user-specific parameter and the most recently exchanged specified historical message by using the random number generator.

[0147] In some embodiments, the user-specific parameter of the physical channel may be randomly configured by the network device.

[0148] For example, the physical channel may be a PDCCH, a PDSCH, a PUCCH, a PUSCH, or the like.

[0149] When the communication apparatus **1900** is configured to implement the function of the network device in the method embodiment shown in FIG. 5, the interface unit **1920** is configured to send a user-specific parameter of a physical channel to a terminal device; the processing unit **1910** is configured to generate, by using a random number generator, at least one random number based on the user-specific parameter and a specified historical message exchanged with the terminal device, where the at least one

random number includes a first random number; and generate a physical channel encryption key based on the first random number by using a key generator; and the processing unit **1910** is further configured to decrypt or encrypt the physical channel based on the physical channel encryption key.

[0150] In some embodiments, the at least one random number further includes a second random number, and the processing unit **1910** is further configured to: update, based on the second random number, a physical channel scrambling sequence corresponding to the physical channel; and descramble or scramble the physical channel based on an updated physical channel scrambling sequence.

[0151] In some embodiments, the at least one random number further includes a third random number, and the processing unit **1910** is further configured to: update, based on the third random number, a physical channel pilot sequence corresponding to the physical channel; and perform channel estimation or resource mapping on the physical channel based on an updated physical channel pilot sequence.

[0152] In some embodiments, the interface unit **1920** is further configured to send a scrambling-specific parameter of the physical channel to the terminal device. A quantity of bits included in the scrambling-specific parameter is greater than a first quantity threshold. The processing unit **1910** is further configured to: generate, based on a first sub-scrambling parameter, the physical channel scrambling sequence corresponding to the physical channel, where the first sub-scrambling parameter is determined by the processing unit **1910** based on a first selection rule and the scrambling-specific parameter, and a quantity of bits included in the first sub-scrambling parameter is equal to the first quantity threshold; and generate, based on a second sub-scrambling parameter, the physical channel pilot sequence corresponding to the physical channel. The second sub-scrambling parameter is determined by the processing unit **1910** based on a second selection rule and the scrambling-specific parameter, and a quantity of bits included in the second sub-scrambling parameter is equal to the first quantity threshold.

[0153] In some embodiments, when generating, by using the random number generator, the at least one random number based on the user-specific parameter and the specified historical message exchanged with the terminal device, the processing unit **1910** is specifically configured to: obtain, through the interface unit **1920** based on a specified periodicity, a specified historical message most recently exchanged with the terminal device; and generate the at least one random number based on the user-specific parameter and the most recently exchanged specified historical message by using the random number generator.

[0154] In some embodiments, the user-specific parameter of the physical channel may be randomly configured by the processing unit **1910**.

[0155] For example, the physical channel may be a PDCCH, a PDSCH, a PUCCH, a PUSCH, or the like.

[0156] As shown in FIG. 20, this disclosure further provides a communication apparatus **2000**, including a processor **2010** and an interface circuit **2020**. The processor **2010** and the interface circuit **2020** are coupled to each other. It can be understood that the interface circuit **2020** may be a transceiver, an input/output interface, an input interface, an output interface, a communication interface, or the like.

Optionally, the communication apparatus **2000** may further include a memory **2030**, configured to: store instructions executed by the processor **2010**, or store input data required for running the instructions by the processor **2010**, or store data generated after the processor **2010** runs the instructions. Optionally, the memory **2030** may be further integrated with the processor **2010**.

[0157] When the communication apparatus **2000** is configured to implement the method shown in FIG. 7, the processor **2010** may be configured to implement a function of the processing unit **1910**, and the interface circuit **2020** may be configured to implement a function of the interface unit **1920**.

[0158] It should be noted that the processor in embodiments of this disclosure may be a central processing unit (CPU), or may be another general-purpose processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a logic circuit, a field programmable gate array (FPGA), or another programmable logic device, a transistor logic device, a hardware component, or any combination thereof. The general purpose processor may be a microprocessor, or may be any regular processor, or the like.

[0159] The method steps in embodiments of this disclosure may be implemented by using hardware, or may be implemented by executing software instructions by the processor. The software instructions may include a corresponding software module. The software module may be stored in a random access memory, a flash memory, a read-only memory, a programmable read-only memory, an erasable programmable read-only memory, an electrically erasable programmable read-only memory, a register, a hard disk, a removable hard disk, a CD-ROM, or any other form of storage medium well-known in the art. For example, a storage medium is coupled to a processor, so that the processor can read information from the storage medium and write information into the storage medium. Certainly, the storage medium may be a component of the processor. The processor and the storage medium may be disposed in an ASIC. In addition, the ASIC may be located in a network device or a terminal device. Certainly, the processor and the storage medium may alternatively exist as discrete components in a network device or a terminal device.

[0160] All or some of the foregoing embodiments may be implemented by using software, hardware, firmware, or any combination thereof. When software is used to implement the foregoing embodiments, all or a part of the embodiments may be implemented in a form of a computer program product. The computer program product includes one or more computer programs or instructions. When the computer programs or the instructions are loaded and executed on a computer, the procedures or functions in embodiments of this disclosure are all or partially executed. The computer may be a general-purpose computer, a dedicated computer, a computer network, a network device, user equipment, or another programmable apparatus. The computer program or instructions may be stored in a computer-readable storage medium, or transmitted from one computer-readable storage medium to another computer-readable storage medium. For example, the computer program or instructions may be transmitted from one network device, terminal, computer, server, or data center to another network device, terminal, computer, server, or data center in a wired or wireless manner. The computer-readable storage medium may be any

usable medium that can be accessed by the computer, or a data storage device, for example, a server or a data center, integrating one or more usable media. The usable medium may be a magnetic medium, for example, a floppy disk, a hard disk, or a magnetic tape; or may be an optical medium, for example, a digital video disc; or may be a semiconductor medium, for example, a solid-state drive. The computer-readable storage medium may be a volatile or non-volatile storage medium, or may include two types of storage media: a volatile storage medium and a non-volatile storage medium.

[0161] In embodiments of this disclosure, unless otherwise specified or there is a logic conflict, terms and/or descriptions in different embodiments are consistent and may be mutually referenced, and technical features in different embodiments may be combined to form a new embodiment based on internal logical relationships of different embodiments.

[0162] In addition, it can be understood that the term “for example” in embodiments of this disclosure is used to represent giving an example, an illustration, or a description. Any embodiment or implementation scheme described as an “example” in this disclosure should not be explained as being more preferred or having more advantages than another embodiment or implementation scheme. Exactly, the term “example” is for presenting a concept in a specific manner.

[0163] It may be understood that various numbers in embodiments of this disclosure are merely used for differentiation for ease of description, and are not used to limit the scope of embodiments of this disclosure. Sequence numbers of the foregoing processes do not mean an execution sequence, and the execution sequence of the processes should be determined based on functions and internal logic of the processes.

What is claimed is:

1. A communication method, comprising:

generating, by a terminal, at least a first random number based on a user-specific parameter, of a physical channel from a network side, and a specified historical message exchanged between the terminal and the network side;

generating, by the terminal, a physical channel encryption key based on the first random number; and

encrypting or decrypting, by the terminal, the physical channel based on the physical channel encryption key.

2. The method according to claim 1, wherein the terminal generates a second random number, and the method further comprises:

updating, by the terminal based on the second random number, a physical channel scrambling sequence corresponding to the physical channel; and

scrambling or descrambling, by the terminal, the physical channel based on an updated physical channel scrambling sequence.

3. The method according to claim 1, wherein the terminal generates a third random number, and the method further comprises:

updating, by the terminal based on the third random number, a physical channel pilot sequence corresponding to the physical channel; and

performing, by the terminal, resource mapping or channel estimation on the physical channel based on an updated physical channel pilot sequence.

4. The method according to claim 1, further comprising: receiving, by the terminal, a scrambling-specific parameter of the physical channel from the network side, wherein a quantity of bits comprised in the scrambling-specific parameter is greater than a first quantity threshold; generating, by the terminal and based on a first sub-scrambling parameter, the physical channel scrambling sequence corresponding to the physical channel, wherein the first sub-scrambling parameter is associated with a first selection rule and the scrambling-specific parameter, and a quantity of bits comprised in the first sub-scrambling parameter is equal to the first quantity threshold; and generating, by the terminal and based on a second sub-scrambling parameter, the physical channel pilot sequence corresponding to the physical channel, wherein the second sub-scrambling parameter is associated with a second selection rule and the scrambling-specific parameter, and a quantity of bits comprised in the second sub-scrambling parameter is equal to the first quantity threshold.
5. The method according to claim 1, further comprising: obtaining, by the terminal and based on a specified periodicity, a specified historical message most recently exchanged with the network side; and generating, by the terminal, the first random number based on the user-specific parameter and the most recently exchanged specified historical message.
6. The method according to claim 1, wherein the user-specific parameter of the physical channel is randomly configured.
7. The method according to claim 1, wherein the physical channel comprises at least one of: a physical downlink control channel (PDCCH), a physical downlink shared channel (PDSCH), a physical uplink control channel (PUCCH), or a physical uplink shared channel (PUSCH).
8. A communication method, comprising: generating, by a network side, at least a first random number based on a user-specific parameter of a physical channel and sent to a terminal, and a specified historical message exchanged between the terminal and the network side; generating, by the network side, a physical channel encryption key based on the first random number; and decrypting or encrypting, by the network side, the physical channel based on the physical channel encryption key.
9. The method according to claim 8, wherein the network side generates a second random number, and the method further comprises: updating, by the network side and based on the second random number, a physical channel scrambling sequence corresponding to the physical channel; and descrambling or scrambling, by the network side, the physical channel based on an updated physical channel scrambling sequence.
10. The method according to claim 8, wherein the network side generates a third random number, and the method further comprises: updating, by the network side and based on the third random number, a physical channel pilot sequence corresponding to the physical channel; and performing, by the network side, channel estimation or resource mapping on the physical channel based on an updated physical channel pilot sequence.
11. The method according to claim 8, further comprising: sending, by the network side, a scrambling-specific parameter of the physical channel to the terminal, wherein a quantity of bits comprised in the scrambling-specific parameter is greater than a first quantity threshold; generating, by the network side and based on a first sub-scrambling parameter, the physical channel scrambling sequence corresponding to the physical channel, wherein the first sub-scrambling parameter is associated with a first selection rule and the scrambling-specific parameter, and a quantity of bits comprised in the first sub-scrambling parameter is equal to the first quantity threshold; and generating, by the network side and based on a second sub-scrambling parameter, the physical channel pilot sequence corresponding to the physical channel, wherein the second sub-scrambling parameter is associated with a second selection rule and the scrambling-specific parameter, and a quantity of bits comprised in the second sub-scrambling parameter is equal to the first quantity threshold.
12. The method according to claim 8, further comprising: obtaining, by the network side and based on a specified periodicity, a specified historical message most recently exchanged with the terminal; and generating, by the network side, the first random number based on the user-specific parameter and the most recently exchanged specified historical message.
13. The method according to claim 8, wherein the user-specific parameter of the physical channel is randomly configured.
14. The method according to claim 8, wherein the physical channel comprises at least one of: a physical downlink control channel (PDCCH), a physical downlink shared channel (PDSCH), a physical uplink control channel (PUCCH), or a physical uplink shared channel (PUSCH).
15. A communication apparatus, comprising: an interface; and processing circuitry, wherein the interface is configured to receive a user-specific parameter of a physical channel from a network side, and the processing circuitry is configured to: generate at least a first random number based on the user-specific parameter and a specified historical message exchanged with the network side; generate a physical channel encryption key based on the first random number; and encrypt or decrypt the physical channel based on the physical channel encryption key.
16. The apparatus according to claim 15, wherein the processing circuitry generates a second random number, and the processing circuitry is further configured to: update, based on the second random number, a physical channel scrambling sequence corresponding to the physical channel; and scramble or descramble the physical channel based on an updated physical channel scrambling sequence.

17. The apparatus according to claim **15**, wherein the processing circuitry generates a third random number; and the processing circuitry is further configured to:

update, based on the third random number, a physical channel pilot sequence corresponding to the physical channel; and

perform resource mapping or channel estimation on the physical channel based on an updated physical channel pilot sequence.

18. The apparatus according to claim **15**, wherein the interface is further configured to receive a scrambling-specific parameter of the physical channel from the network side, and a quantity of bits comprised in the scrambling-specific parameter is greater than a first quantity threshold; and

the processing circuitry is further configured to:

generate, based on a first sub-scrambling parameter, the physical channel scrambling sequence corresponding to the physical channel, wherein the first sub-scrambling parameter is associated with a first selection rule and the scrambling-specific parameter, and

a quantity of bits comprised in the first sub-scrambling parameter is equal to the first quantity threshold; and

generate, based on a second sub-scrambling parameter, the physical channel pilot sequence corresponding to the physical channel, wherein the second sub-scrambling parameter is associated with a second selection rule and the scrambling-specific parameter, and a quantity of bits comprised in the second sub-scrambling parameter is equal to the first quantity threshold.

19. The apparatus according to claim **15**, wherein the processing circuitry is further configured to:

obtain, through the interface and based on a specified periodicity, a specified historical message most recently exchanged with the network side; and

generate the first random number based on the user-specific parameter and the most recently exchanged specified historical message.

20. The apparatus according to claim **15**, wherein the user-specific parameter of the physical channel is randomly configured.

* * * * *