CLAIMS

What is claimed is:

1. A communications system, comprising:

a target access network device configured to:

receive a radio resource control (RRC) resume request from a user equipment (UE), wherein the RRC resume request comprises an inactive–radio network temporary identifier (I-RNTI); and

send a context information obtaining request comprising the I-RNTI; and

a source access network device configured to:

receive the context information obtaining request from the target access network device;

obtain first indication information based on the I-RNTI, wherein the first indication information indicates a user plane security protection method used before the source access network device and the UE enter an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled; and

send a context information obtaining response to the target access network device, wherein the context information obtaining response comprises the first indication information,

wherein the target access network device is further configured to:

receive the context information obtaining response from the source access network device; and

activate, using the user plane security protection method, user plane security between the target access network device and the UE when the user plane security protection method can be supported.

2. The communications system according to claim 1, wherein the target access network device is further configured to send an RRC message to the UE when the user plane security protection method cannot be supported, and wherein the RRC message is configured to trigger the UE to re-establish an RRC connection to the target access network device.

3. The communications system according to claim 1, wherein the context information obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are

used by the source access network device and a new access stratum key (KgNB*) generated by the source access network device, and wherein the target access network device is further configured such that when the target access network device supports the encryption algorithm and the integrity protection algorithm, the target access network device determines a first user plane security key between the target access network device and the UE based on the KgNB*.

4. The communications system according to claim 1, wherein the target access network device is further configured to:

receive first uplink user plane data from the UE; and

perform user plane security deprotection on the first uplink user plane data to obtain uplink user plane data.

5. The communications system according to claim 1, wherein the context information obtaining response further comprises at least one user plane security policy of the UE, and wherein the at least one user plane security policy comprises at least one of a user plane encryption protection policy or a user plane integrity protection policy.

6. The communications system according to claim 1, wherein the context information obtaining response further comprises a protocol data unit (PDU) session identifier (ID) corresponding to the first indication information.

7. The communications system according to claim 1, wherein the source access network device is further configured to:

send an RRC release message to the UE, wherein the RRC release message indicates to the UE to enter the inactive state;

store the first indication information;

delete an RRC encryption key, a user plane encryption key, and a user plane integrity protection key; and

store an RRC integrity protection key and the first indication information.

8. The communications system according to claim 1, wherein the target access network device

is further configured to determine whether the user plane security protection method can be supported.

9. A target access network device, comprising:

at least one processor; and

a memory coupled to the at least one processor and configured to store program instructions, which when executed by the at least one processor, cause the target access network device to:

receive a radio resource control (RRC) resume request from a user equipment (UE), wherein the RRC resume request comprises an inactive–radio network temporary identifier (I-RNTI);

send a context information obtaining request comprising the I-RNTI to a source access network device;

receive a context information obtaining response from the source access network device, wherein the context information obtaining response comprises first indication information, wherein the first indication information indicates a user plane security protection method used before the UE enters an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled; and

activate, using the user plane security protection method, user plane security between the target access network device and the UE when the user plane security protection method can be supported.

10. The target access network device according to claim 9, wherein the program instructions further cause the target access network device to send an RRC message to the UE when the user plane security protection method cannot be supported, and wherein the RRC message is configured to trigger the UE to re-establish an RRC connection to the target access network device.

11. The target access network device according to claim 9, wherein the context information obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are used by the source access network device and a new access stratum key (KgNB*) generated by the source access network device, and wherein the program instructions further cause the target access network device to determine a first user plane security key between the target

access network device and the UE based on the KgNB* when the target access network device supports the encryption algorithm and the integrity protection algorithm.

12. The target access network device according to claim 9, wherein the program instructions further cause the target access network device to:

receive first uplink user plane data from the UE;

perform user plane security deprotection on the first uplink user plane data to obtain uplink user plane data; and

send the uplink user plane data.

13. The target access network device according to claim 9, wherein the context information obtaining response further comprises at least one user plane security policy of the UE, and wherein the at least one user plane security policy comprises at least one of a user plane encryption protection policy or a user plane integrity protection policy.

14. The target access network device according to claim 9, wherein the context information obtaining response further comprises a protocol data unit (PDU) session identifier (ID) corresponding to the first indication information.

15. The target access network device according to claim 9, wherein the program instructions further cause the target access network device to determine whether the user plane security protection method can be supported.

16. An apparatus, comprising:

at least one processor; and

a memory coupled to the at least one processor and configured to store program instructions, which when executed by the at least one processor, cause the apparatus to:

store first indication information, wherein the first indication information indicates a user plane security protection method used before the apparatus enters an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled;

send a radio resource control (RRC) resume request to a target access network device; and

activate, using the user plane security protection method, user plane security between the apparatus and the target access network device when receiving an RRC resume message from the target access network device.

17. The apparatus according to claim 16, wherein the program instructions further cause the apparatus to:

determine a first user plane security key between the apparatus and the target access network device;

perform user plane security protection on uplink user plane data based on the user plane security protection method and the first user plane security key;

obtain first uplink user plane data based on performing the user plane security protection on the uplink user plane data; and

send the first uplink user plane data to the target access network device.

18. The apparatus according to claim 17, wherein the program instructions further cause the apparatus to determine the first user plane security key between the apparatus and the target access network device according to the user plane security protection method.

19. The apparatus according to claim 16, wherein the program instructions further cause the apparatus to receive an RRC release message from a source access network device, and wherein the RRC release message indicates to the apparatus to enter the inactive state.

20. The apparatus according to claim 16, wherein the program instructions further cause the apparatus to receive an RRC connection reconfiguration message from a source access network device, and wherein the RRC connection reconfiguration message comprises the first indication information.

21. A method comprising:

receiving, by a target access network device, a radio resource control (RRC) resume request from a user equipment (UE), wherein the RRC resume request comprises an inactive–radio

network temporary identifier (I-RNTI);

sending, by the target access network device, a context information obtaining request comprising the I-RNTI to a source access network device;

receiving, by the target access network device, a context information obtaining response from the source access network device, wherein the context information obtaining response comprises first indication information, wherein the first indication information indicates a user plane security protection method used before the UE enters an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled; and

activating, by the target access network device using the user plane security protection method, user plane security between the target access network device and the UE when the user plane security protection method can be supported.

22. The method according to claim 21, further comprising sending, by the target access network device, an RRC message to the UE when the user plane security protection method cannot be supported, and wherein the RRC message is configured to trigger the UE to re-establish an RRC connection to the target access network device.

23. The method according to claim 21, wherein the context information obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are used by the source access network device and a new access stratum key (KgNB*) generated by the source access network device, and wherein the method further comprises determining, by the target access network device, a first user plane security key between the target access network device and the UE based on the KgNB* when the target access network device supports the encryption algorithm and the integrity protection algorithm.

24. The method according to claim 21, further comprising:

receiving, by the target access network device, first uplink user plane data from the UE;

performing, by the target access network device, user plane security deprotection on the first uplink user plane data to obtain uplink user plane data; and

sending, by the target access network device, the uplink user plane data.

25. The method according to claim 21, wherein the context information obtaining response further comprises at least one user plane security policy of the UE, and wherein the at least one user plane security policy comprises at least one of a user plane encryption protection policy or a user plane integrity protection policy.

26. The method according to claim 21, wherein the context information obtaining response further comprises a protocol data unit (PDU) session identifier (ID) corresponding to the first indication information.

27. The method according to claim 21, further comprising determining, by the target access network device, whether the user plane security protection method can be supported.

28. A method comprising:

storing, by an apparatus, first indication information, wherein the first indication information indicates a user plane security protection method used before the apparatus enters an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled;

sending, by the apparatus, a radio resource control (RRC) resume request to a target access network device; and

activating, by the apparatus using the user plane security protection method, user plane security between the apparatus and the target access network device when receiving an RRC resume message from the target access network device.

29. The method according to claim 28, further comprising:

determining, by the apparatus, a first user plane security key between the apparatus and the target access network device;

performing, by the apparatus, user plane security protection on uplink user plane data based on the user plane security protection method and the first user plane security key;

obtaining, by the apparatus, first uplink user plane data based on performing the user plane security protection on the uplink user plane data; and

sending, by the apparatus, the first uplink user plane data to the target access network device.

30. The method according to claim 29, wherein determining the first user plane security key comprises determining, by the apparatus, the first user plane security key between the apparatus and the target access network device according to the user plane security protection method.

31. The method according to claim 28, further comprising receiving, by the apparatus, an RRC connection reconfiguration message from a source access network device, wherein the RRC connection reconfiguration message comprises the first indication information.

32. A communications method, comprising:

receiving, by a target access network device, a radio resource control (RRC) resume request from a user equipment (UE), wherein the RRC resume request comprises an inactive–radio network temporary identifier (I-RNTI);

sending, by the target access network device, a context information obtaining request comprising the I-RNTI;

receiving, by the source access network device, the context information obtaining request from the target access network device;

obtaining, by the source access network device, first indication information based on the I-RNTI, wherein the first indication information indicates a user plane security protection method used before the source access network device and the UE enter an inactive state from a connected state, and wherein the user plane security protection method indicates whether at least one of user plane encryption protection or user plane integrity protection is enabled;

sending, by the source access network device, a context information obtaining response to the target access network device, wherein the context information obtaining response comprises the first indication information;

receiving, by the target access network device, the context information obtaining response from the source access network device; and

activating, by the target access network device using the user plane security protection method, user plane security between the target access network device and the UE when the user plane security protection method can be supported.

33. The communications method according to claim 32, further comprising sending, by the target access network device, an RRC message to the UE when the user plane security protection method cannot be supported, wherein the RRC message is configured to trigger the UE to re-establish an RRC connection to the target access network device.

34. The communications method according to claim 32, wherein the context information obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are used by the source access network device and a new access stratum key (KgNB*) generated by the source access network device, and wherein the communications method further comprises determining, by the target access network device, a first user plane security key between the target access network device and the UE based on the KgNB* when the target access network device supports the encryption algorithm and the integrity protection algorithm.

35. The communications method according to claim 32, wherein the context information obtaining response further comprises at least one user plane security policy of the UE, and wherein the at least one user plane security policy comprises at least one of a user plane encryption protection policy or a user plane integrity protection policy.

36. The communications method according to claim 32, wherein the context information obtaining response further comprises a protocol data unit (PDU) session identifier (ID) corresponding to the first indication information.

37. The communications method according to claim 32, further comprising:

sending, by the source access network device, an RRC release message to the UE, wherein the RRC release message indicates to the UE to enter the inactive state;

storing, by the source access network device, the first indication information;

deleting, by the source access network device, an RRC encryption key, a user plane encryption key, and a user plane integrity protection key; and

storing, by the source access network device, an RRC integrity protection key and the first indication information.

38. The communications method according to claim 32, further comprising determining, by the target access network device, whether the user plane security protection method can be supported.

~~1. A communication method, comprising:~~

~~obtaining, by a target access network device, first indication information after receiving a radio resource control, RRC, resume request from user equipment, UE, wherein the first indication information indicates a user plane security protection method used before the UE enters an inactive state from a connected state, and the user plane security protection method indicates whether user plane encryption protection is enabled and/or whether user plane integrity protection is enabled; and~~

~~when the user plane security protection method indicated by the first indication information can be supported, activating, by the target access network device, user plane security between the target access network device and the UE by using the user plane security protection method indicated by the first indication information.~~

~~2. The method according to claim 1, further comprising:~~

~~sending, by the target access network device, an RRC message to the UE when the user plane security protection method indicated by the first indication information cannot be supported, wherein the RRC message is used to trigger the UE to re-establish an RRC connection to the target access network device.~~

~~3. The method according to claim 1 or 2, wherein the obtaining first indication information comprises:~~

~~sending, by the target access network device, a context information obtaining request to a source access network device; and~~

~~obtaining, by the target access network device, a context information obtaining response from the source access network device, wherein the context information obtaining response comprises the first indication information.~~

~~4. The method according to claim 3, wherein the context information obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are used by the source access network device and a new access stratum key KgNB* generated by the source access network device; and the method further comprises:~~

~~when the target access network device supports the encryption algorithm and the integrity~~

protection algorithm that are used by the source access network device, determining, by the target access network device, a first user plane security key between the target access network device and the UE based on the KgNB*.

5. The method according to claim 1, 3, or 4, further comprising:

when receiving first uplink user plane data from the UE, performing, by the target access network device, user plane security deprotection on the first uplink user plane data to obtain uplink user plane data.

6. The method according to any one of claims 1 to 5, wherein the context information obtaining response further comprises a user plane security policy of the UE, and the user plane security policy comprises a user plane encryption protection policy and a user plane integrity protection policy.

7. A communication method, comprising:

sending, by a source access network device, a radio resource control, RRC, release message to user equipment, UE, wherein the RRC release message is used to indicate the UE to enter an inactive state; and

deleting, by the source access network device, an RRC encryption key, a user plane encryption key, and a user plane integrity protection key, and storing an RRC integrity protection key and first indication information, wherein the first indication information indicates a user plane security protection method used before the source access network device and the UE enter the inactive state from a connected state, and the user plane security protection method indicates whether user plane encryption protection is enabled and/or whether user plane integrity protection is enabled.

8. The method according to claim 7, further comprising:

receiving, by the source access network device, a context information obtaining request from a target access network device;

obtaining, by the source access network device, the first indication information based on the context information obtaining request; and

sending, by the source access network device, a context information obtaining response to the target access network device, wherein the context information obtaining response comprises the first indication information.

9. The method according to claim 7 or 8, wherein the context information obtaining response

further comprises a user plane security policy of the UE, and the user plane security policy comprises a user plane encryption protection policy and a user plane integrity protection policy.

10. A communication method, comprising:

receiving, by user equipment, UE, a radio resource control, RRC, release message, wherein the RRC release message indicates the UE to enter an inactive state;

storing first indication information, wherein the first indication information indicates a user plane security protection method used before the UE enters the inactive state from a connected state, and the user plane security protection method indicates whether user plane encryption protection is enabled and/or whether user plane integrity protection is enabled;

sending, by the UE, an RRC resume request to a target access network device;

receiving, by the UE, an RRC resume message from the target access network device; and

activating, by the UE, user plane security between the UE and the target access network device by using the user plane security protection method indicated by the first indication information.

11. The method according to claim 10, further comprising:

determining, by the UE, a first user plane security key between the UE and the target access network device;

performing, by the UE, user plane security protection on uplink user plane data based on the user plane security protection method and the first user plane security key, to obtain first uplink user plane data; and

sending, by the UE, the first uplink user plane data to the target access network device.

12. The method according to claim 11, wherein the determining, by the UE, a first user plane security key between the UE and the target access network device comprises:

determining, by the UE, the first user plane security key between the UE and the target access network device according to the user plane security protection method.

13. The method according to any one of claims 10 to 12, wherein the receiving, by UE, a radio resource control RRC release message comprises:

receiving, by the UE, the radio resource control, RRC, release message from a source access network device.

14. A communications system, comprising a target access network device and a source access network device, wherein

the target access network device is configured to: receive a radio resource control, RRC, resume request from user equipment, UE, and send a context information obtaining request to the source access network device;

the source access network device is configured to: receive the context information obtaining request from the target access network device; obtain first indication information based on the context information obtaining request, wherein the first indication information indicates a user plane security protection method used before the source access network device and the UE enter an inactive state from a connected state, and the user plane security protection method indicates whether user plane encryption protection is enabled and/or whether user plane integrity protection is enabled; and send a context information obtaining response to the target access network device, wherein the context information obtaining response comprises the first indication information; and

the target access network device is configured to: receive the context information obtaining response from the source access network device; and when the user plane security protection method indicated by the first indication information can be supported, activate user plane security between the target access network device and the UE by using the user plane security protection method indicated by the first indication information.

15. The system according to claim 14, wherein the target access network device is further configured to send an RRC message to the UE when the user plane security protection method indicated by the first indication information cannot be supported, wherein the RRC message is used to trigger the user equipment to re-establish an RRC connection to the target access network device.

16. The system according to claim 14, wherein the context information obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are used by the source access network device and a new access stratum key KgNB* generated by the source access network device; and

the target access network device is further configured to: when the target access network device supports the encryption algorithm and the integrity protection algorithm that are used by the source access network device, determine a first user plane security key between the target access network device and the UE based on the KgNB*.

17. The system according to claim 14 or 16, wherein the target access network device is further configured to: when receiving first uplink user plane data from the user equipment, perform

user plane security deprotection on the first uplink user plane data to obtain uplink user plane data.

18. The system according to any one of claims 14 to 17, wherein the context information obtaining response further comprises a user plane security policy of the user equipment, and the user plane security policy comprises a user plane encryption protection policy and a user plane integrity protection policy.

19. The system according to any one of claims 14 to 18, wherein the source access network device is configured to: send an RRC release message to the UE, wherein the RRC release message is used to indicate the UE to enter the inactive state; and store the first indication information.

20. A target access network device, comprising a processing unit and a transceiver unit, wherein

the transceiver unit is configured to obtain first indication information after receiving a radio resource control, RRC, resume request from user equipment UE, wherein the first indication information indicates a user plane security protection method used before the UE enters an inactive state from a connected state, and the user plane security protection method indicates whether user plane encryption protection is enabled and/or whether user plane integrity protection is enabled; and

the processing unit is configured to: when the user plane security protection method indicated by the first indication information can be supported, activate user plane security between the target access network device and the UE by using the user plane security protection method indicated by the first indication information.

21. The target access network device according to claim 20, wherein

the transceiver unit is further configured to send an RRC message to the UE when the user plane security protection method indicated by the first indication information cannot be supported, wherein the RRC message is used to trigger the user equipment to re-establish an RRC connection to the target access network device.

22. The target access network device according to claim 20 or 21, wherein when configured to obtain the first indication information, the transceiver unit is specifically configured to send a context information obtaining request to a source access network device; and receive a context information obtaining response from the source access network device, wherein the context information obtaining response comprises the first indication information.

23. The target access network device according to claim 22, wherein the context information

obtaining response further comprises an encryption algorithm and an integrity protection algorithm that are used by the source access network device and a new access stratum key KgNB* generated by the source access network device; and

the processing unit is further configured to: when the target access network device supports the encryption algorithm and the integrity protection algorithm that are used by the source access network device, determine a first user plane security key between the target access network device and the UE based on the KgNB*.

24. The target access network device according to claim 20, 22, or 23, wherein

the processing unit is further configured to: when the transceiver unit receives first uplink user plane data from the UE, perform user plane security deprotection on the first uplink user plane data to obtain uplink user plane data.

25. The target access network device according to any one of claims 20 to 24, wherein the context information obtaining response further comprises a user plane security policy of the UE, and the user plane security policy comprises a user plane encryption protection policy and a user plane integrity protection policy.

26. A source access network device, comprising a processing unit and a storage unit, wherein

the transceiver unit is configured to send a radio resource control RRC release message to user equipment UE, wherein the RRC release message is used to indicate the UE to enter an inactive state; and

the storage unit is configured to: delete an RRC encryption key, a user plane encryption key, and a user plane integrity protection key, and store an RRC integrity protection key and first indication information, wherein the first indication information indicates a user plane security protection method used before the source access network device and the UE enter the inactive state from a connected state, and the user plane security protection method indicates whether user plane encryption protection is enabled and/or whether user plane integrity protection is enabled.

27. The source access network device according to claim 26, wherein

the transceiver unit is further configured to receive a context information obtaining request from a target access network device, obtain the first indication information based on the context information obtaining request, and send a context information obtaining response to the target access network device, wherein the context information obtaining response comprises the first indication information.

28. The source access network device according to claim 26 or 27, wherein the context information obtaining response further comprises a user plane security policy of the UE, and the user plane security policy comprises a user plane encryption protection policy and a user plane integrity protection policy.

29. User equipment, comprising a transceiver unit, a storage unit, and a processing unit, wherein

the transceiver unit is configured to receive a radio resource control RRC release message, wherein the RRC release message is used to indicate the UE to enter an inactive state;

the storage unit is configured to store first indication information, wherein the first indication information indicates a user plane security protection method used before the UE enters the inactive state from a connected state, and the user plane security protection method indicates whether user plane encryption protection is enabled and/or whether user plane integrity protection is enabled;

the transceiver unit is further configured to: send an RRC resume request to a target access network device; and receive an RRC resume message from the target access network device; and

the processing unit is configured to activate user plane security between the UE and the target access network device by using the user plane security protection method indicated by the first indication information.

30. The user equipment according to claim 29, wherein

the processing unit is further configured to: determine a first user plane security key between the UE and the target access network device; and perform user plane security protection on uplink user plane data based on the user plane security protection method and the first user plane security key, to obtain first uplink user plane data; and

the transceiver unit is further configured to send the first uplink user plane data to the target access network device.

31. The user equipment according to claim 30, wherein the processing unit is specifically configured to determine the first user plane security key between the UE and the target access network device according to the user plane security protection method.

32. The user equipment according to any one of claims 29 to 31, wherein the transceiver unit is specifically configured to receive a radio resource control RRC release message from a source access network device.

33. A target access network device, wherein the target access network device comprises a memory and a processor, the memory is configured to store an instruction, and the processor is configured to execute the instruction in the memory, so that the method according to any one of claims 1 to 6 is implemented.

34. A source access network device, wherein the source access network device comprises a memory and a processor, the memory is configured to store an instruction, and the processor is configured to execute the instruction in the memory, so that the method according to any one of claims 7 to 9 is implemented.

35. User equipment, wherein the user equipment comprises a memory and a processor, the memory is configured to store an instruction, and the processor is configured to execute the instruction in the memory, so that the method according to any one of claims 10 to 13 is implemented.

36. A computer-readable storage medium, wherein the computer-readable storage medium comprises an instruction, and when the instruction is run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 6, the method according to any one of claims 7 to 9, or the method according to any one of claims 10 to 13.

37. A computer program product comprising an instruction, wherein when the computer program product runs on a computer, the computer is enabled to perform the method according to any one of claims 1 to 6, the method according to any one of claims 7 to 9, or the method according to any one of claims 10 to 13.

38. A computer chip, wherein the chip is connected to a memory, and the chip is configured to read and execute a software program stored in the memory, to perform the method according to any one of claims 1 to 6.

39. A computer chip, wherein the chip is connected to a memory, and the chip is configured to read and execute a software program stored in the memory, to perform the method according to any one of claims 7 to 9.

40. A computer chip, wherein the chip is connected to a memory, and the chip is configured to read and execute a software program stored in the memory, to perform the method according to any one of claims 10 to 13.

41. A communication method, comprising:

after receiving an RRC resume message from user equipment, determining, by a target access

network device, a first user plane security protection method between the target access network device and the user equipment based on a context information obtaining response from a source access network device, wherein the first user plane security protection method indicates whether user plane encryption protection between the target access network device and the user equipment is enabled and/or whether user plane integrity protection between the target access network device and the user equipment is enabled;

determining, by the target access network device, a first user plane security key between the target access network device and the user equipment;

when receiving first uplink user plane data from the user equipment, performing, by the target access network device, user plane security deprotection on the first uplink user plane data based on the first user plane security key and the first user plane security protection method, to obtain uplink user plane data; and

sending, by the target access network device, the uplink user plane data.

42. The method according to claim 41, wherein the context information obtaining response comprises a user plane security policy of the user equipment; and

the determining, by a target access network device, a first user plane security protection method between the target access network device and the user equipment based on a context information obtaining response from a source access network device comprises:

determining, by the target access network device, the first user plane security protection method between the target access network device and the user equipment based on the user plane security policy from the source access network device.

43. The method according to claim 41, wherein the context information obtaining response comprises a user plane security policy of the user equipment and first indication information, the first indication information indicates a second user plane security protection method used before the user equipment and the source access network device enter a third state from a connected state, and the second user plane security protection method indicates whether user plane encryption protection between the user equipment and the source access network device is enabled and/or whether user plane integrity protection between the user equipment and the source access network device is enabled, before the user equipment and the source access network device enter the third state from the connected state; and

the determining, by a target access network device, a first user plane security protection

method between the target access network device and the user equipment based on a context information obtaining response from a source access network device comprises:

determining, by the target access network device based on the first indication information from the source access network device, the second user plane security protection method as the first user plane security protection method between the target access network device and the user equipment.

44. The method according to claim 41, wherein the context information obtaining response comprises a user plane security policy of the user equipment and first indication information, the first indication information indicates a second user plane security protection method used before the user equipment and the source access network device enter a third state from a connected state, and the second user plane security protection method indicates whether user plane encryption protection between the user equipment and the source access network device is enabled and/or whether user plane integrity protection between the user equipment and the source access network device is enabled, before the user equipment and the source access network device enter the third state from the connected state; and

the determining, by a target access network device, a first user plane security protection method between the target access network device and the user equipment based on a context information obtaining response from a source access network device comprises:

when determining that the second user plane security protection method cannot be supported or the second user plane security protection method is not used, determining, by the target access network device, the first user plane security protection method between the target access network device and the user equipment based on the user plane security policy; or

when determining that the second user plane security protection method cannot be supported or the second user plane security protection method is not used, sending, by the target access network device, an RRC message to the user equipment, wherein the RRC message is used to trigger the user equipment to re-establish an RRC connection to the target access network device; and

during establishment of the RRC connection, determining, by the target access network device, the first user plane security protection method between the target access network device and the user equipment.

45. The method according to any one of claims 41 to 44, wherein the determining, by the

target access network device, a first user plane security key between the target access network device and the user equipment comprises:

determining, by the target access network device, the first user plane security key between the target access network device and the user equipment according to the first user plane security protection method.

46. The method according to any one of claims 41 to 44, further comprising:

sending, by the target access network device, an RRC resume message to the user equipment, wherein the RRC resume message comprises second indication information, and the second indication information indicates the first user plane security protection method.

47. A communication method, comprising:

after sending an RRC resume request to a target access network device, determining, by user equipment, a first user plane security protection method between the user equipment and the target access network device, wherein the first user plane security protection method indicates whether user plane encryption protection between the target access network device and the user equipment is enabled and/or whether user plane integrity protection between the target access network device and the user equipment is enabled;

determining, by the user equipment, a first user plane security key between the user equipment and the target access network device;

performing, by the user equipment, user plane security protection on uplink user plane data based on the first user plane security protection method and the first user plane security key, to obtain first uplink user plane data; and

sending, by the user equipment, the first uplink user plane data to the target access network device.

48. The method according to claim 47, wherein the determining, by user equipment, a first user plane security protection method between the user equipment and the target access network device comprises:

receiving, by the user equipment, an RRC resume message from the target access network device, wherein the RRC resume message comprises second indication information, and the second indication information indicates the first user plane security protection method; and

determining, by the user equipment, the first user plane security protection method between the user equipment and the target access network device based on the second indication

~~information.~~

~~49. The method according to claim 48, further comprising:~~

~~releasing, by the user equipment, an RRC connection after receiving the RRC resume message.~~

~~50. The method according to claim 47, further comprising:~~

~~storing, by the user equipment, first indication information after receiving an RRC release message from the target access network device, wherein the first indication information indicates a second user plane security protection method used before the user equipment and a source access network device enter a third state from a connected state, and the second user plane security protection method indicates whether user plane encryption protection between the user equipment and the source access network device is enabled and/or whether user plane integrity protection between the user equipment and the source access network device is enabled, before the user equipment and the source access network device enter the third state from the connected state.~~

~~51. The method according to claim 50, wherein the determining, by user equipment, a first user plane security protection method between the user equipment and the target access network device comprises:~~

~~determining, by the user equipment, the second user plane security protection method indicated by the first indication information as the first user plane security protection method between the user equipment and the target access network device.~~

~~52. The method according to claim 51, wherein before the determining, by the user equipment, the second user plane security protection method indicated by the first indication information as the first user plane security protection method between the user equipment and the target access network device, the method further comprises:~~

~~receiving, by the user equipment, an RRC resume message from the target access network device, wherein the RRC resume message does not comprise second indication information, and the second indication information indicates a user plane security protection method determined by the target access network device; and~~

~~performing, by the user equipment, the step of determining the second user plane security protection method indicated by the first indication information as the first user plane security protection method between the user equipment and the target access network device.~~

~~53. The method according to claim 48 or 51, wherein the determining, by the user equipment,~~

~~a first user plane security key between the user equipment and the target access network device comprises:~~

~~determining, by the user equipment, the first user plane security key between the user equipment and the target access network device according to the first user plane security protection method.~~

~~54. The method according to claim 47, further comprising:~~

~~after receiving an RRC release message from the target access network device, storing, by the user equipment, a second user plane security key, wherein the second user plane security key is used before the user equipment and the source access network device enter a third state from a connected state.~~

~~55. A target access network device, comprising a processing unit and a transceiver unit, wherein~~

~~the processing unit is configured to: after the transceiver unit receives an RRC resume message from user equipment, determine a first user plane security protection method between the target access network device and the user equipment based on a context information obtaining response from a source access network device, wherein the first user plane security protection method indicates whether user plane encryption protection between the target access network device and the user equipment is enabled and/or whether user plane integrity protection between the target access network device and the user equipment is enabled; determine a first user plane security key between the target access network device and the user equipment; and when the transceiver unit receives first uplink user plane data from the user equipment, perform user plane security deprotection on the first uplink user plane data based on the first user plane security key and the first user plane security protection method, to obtain uplink user plane data; and~~

~~the transceiver unit is configured to send the uplink user plane data.~~

~~56. The target access network device according to claim 55, wherein the context information obtaining response comprises a user plane security policy of the user equipment, and the processing unit is specifically configured to determine the first user plane security protection method between the target access network device and the user equipment based on the user plane security policy from the source access network device.~~

~~57. The target access network device according to claim 55, wherein the context information obtaining response comprises a user plane security policy of the user equipment and first indication~~

~~information, the first indication information indicates a second user plane security protection method used before the user equipment and the source access network device enter a third state from a connected state, and the second user plane security protection method indicates whether user plane encryption protection between the user equipment and the source access network device is enabled and/or whether user plane integrity protection between the user equipment and the source access network device is enabled, before the user equipment and the source access network device enter the third state from the connected state; and~~

~~the processing unit is specifically configured to determine, based on the first indication information from the source access network device, the second user plane security protection method as the first user plane security protection method between the target access network device and the user equipment.~~

~~58. The target access network device according to claim 55, wherein the context information obtaining response comprises a user plane security policy of the user equipment and first indication information, the first indication information indicates a second user plane security protection method used before the user equipment and the source access network device enter a third state from a connected state, and the second user plane security protection method indicates whether user plane encryption protection between the user equipment and the source access network device is enabled and/or whether user plane integrity protection between the user equipment and the source access network device is enabled, before the user equipment and the source access network device enter the third state from the connected state; and~~

~~the processing unit is specifically configured to: when determining that the second user plane security protection method cannot be supported or the second user plane security protection method is not used, determine the first user plane security protection method between the target access network device and the user equipment based on the user plane security policy; or when determining that the second user plane security protection method cannot be supported or the second user plane security protection method is not used, control the transceiver unit to send an RRC message to the user equipment, wherein the RRC message is used to trigger the user equipment to re-establish an RRC connection to the target access network device; and during establishment of the RRC connection, determine the first user plane security protection method between the target access network device and the user equipment.~~

~~59. The target access network device according to any one of claims 55 to 58, wherein the~~

processing unit is specifically configured to determine the first user plane security key between the target access network device and the user equipment according to the first user plane security protection method.

60. The target access network device according to any one of claims 55 to 58, wherein the transceiver unit is further configured to send an RRC resume message to the user equipment, wherein the RRC resume message comprises second indication information, and the second indication information indicates the first user plane security protection method.

61. User equipment, comprising a processing unit and a transceiver unit, wherein

the processing unit is configured to: after the transceiver unit sends an RRC resume request to a target access network device, determine a first user plane security protection method between the user equipment and the target access network device, wherein the first user plane security protection method indicates whether user plane encryption protection between the target access network device and the user equipment is enabled and/or whether user plane integrity protection between the target access network device and the user equipment is enabled; determine a first user plane security key between the user equipment and the target access network device; and perform user plane security protection on uplink user plane data based on the first user plane security protection method and the first user plane security key, to obtain first uplink user plane data; and

the transceiver unit is configured to send the first uplink user plane data to the target access network device.

62. The user equipment according to claim 61, wherein the processing unit is specifically configured to: control the transceiver unit to receive an RRC resume message from the target access network device, wherein the RRC resume message comprises second indication information, and the second indication information indicates the first user plane security protection method; and determine the first user plane security protection method between the user equipment and the target access network device based on the second indication information.

63. The user equipment according to claim 62, wherein the processing unit is further configured to release an RRC connection after the transceiver unit receives the RRC resume message.

64. The user equipment according to claim 62, further comprising a storage unit, wherein the storage unit is configured to store first indication information after the transceiver unit receives an RRC release message from the target access network device, wherein the first indication

~~information indicates second user plane security protection user equipment used before the user equipment and a source access network device enter a third state from a connected state, and the second user plane security protection method indicates whether user plane encryption protection between the user equipment and the source access network device is enabled and/or whether user plane integrity protection between the user equipment and the source access network device is enabled, before the user equipment and the source access network device enter the third state from the connected state.~~

~~65. The user equipment according to claim 64, wherein the processing unit is specifically configured to determine the second user plane security protection user equipment indicated by the first indication information as the first user plane security protection method between the user equipment and the target access network device.~~

~~66. The user equipment according to claim 65, wherein the transceiver unit is further configured to receive the RRC resume message from the target access network device, wherein the RRC resume message does not comprise the second indication information, and the second indication information indicates user plane security protection user equipment determined by the target access network device; and the processing unit performs the step of determining the second user plane security protection user equipment indicated by the first indication information as the first user plane security protection method between the user equipment and the target access network device.~~

~~67. The user equipment according to claim 62 or 65, wherein the processing unit is specifically configured to determine the first user plane security key between the user equipment and the target access network device based on the first user plane security protection method.~~

~~68. The user equipment according to claim 61, further comprising a storage unit, wherein the storage unit is configured to: after the transceiver unit receives an RRC release message from the target access network device, store a second user plane security key, wherein the second user plane security key is used before the user equipment and the source access network device enter a third state from a connected state.~~