CLAIMS

What is claimed is:

1. A key generation method, applied to a scenario where an integrated access and backhaul IAB node is connected to a master base station and a secondary base station, comprising:

determining, by the IAB node, that the master base station or the secondary base station serves as an IAB donor;

when the master base station serves as the IAB donor, generating, by the IAB node, an IAB key K_{IAB} based on a master base station key, wherein the master base station key is generated in a process in which the IAB node registers with a network through the master base station; or

when the secondary base station serves as the IAB donor, generating, by the IAB node, the IAB key K_{IAB} based on a secondary base station key, wherein the secondary base station key is generated by the IAB node based on the master base station key.

2. The method according to claim 1, wherein the determining, by the IAB node, that the master base station or the secondary base station serves as an IAB donor comprises:

receiving, by the IAB node, fourth indication information from the master base station;

determining, by the IAB node based on the fourth indication information, that the master base station serves as the IAB donor.

3. The method according to claim 2, wherein the fourth indication information is carried in an RRC reconfiguration message from the master base station.

4. The method according to claim 1, wherein the determining, by the IAB node, that the master base station or the secondary base station serves as an IAB donor comprises:

receiving, by the IAB node, fifth indication information from the secondary base station;

determining, by the IAB node based on the fifth indication information, that the secondary base station serves as the IAB donor.

5. The method according to claim 1, wherein the determining, by the IAB node, that the master base station or the secondary base station serves as an IAB donor comprises:

when a wireless backhaul link is established between the IAB node and the master base station, determining, by the IAB node, that the master base station serves as the IAB donor; or

when a wireless backhaul link is established between the IAB node and the secondary base station, determining, by the IAB node, that the secondary base station serves as the IAB donor.

6. The method according to any one of claims 1 to 5, further comprising:

establishing, by the IAB node based on K_{IAB}, a secure tunnel between the IAB node and the IAB donor.

7. A key generation method, comprising:

determining, by a first access network device through which a first device registers with a network, that the first device is an IAB node;

sending, by the first access network device, an SN addition/modification request message to a third access network device, wherein the third access network device is a secondary base station of the first device, the SN addition/modification request message carries a secondary base station key, and the secondary base station key is generated by the first access network device;

receiving, by the first access network device, an SN addition/modification request ACK message from the third access network device;

sending, by the first access network device, an RRC reconfiguration message to the first device, wherein the RRC reconfiguration message comprises fourth indication information, the first access network device is a master base station, and the fourth indication information indicates that the master base station is an IAB donor;

receiving, by the first access network device, an RRC reconfiguration complete message from the first device;

sending, by the first access network device, an SN reconfiguration complete message to the third access network device;

generating, by the first access network device, an IAB key K_{IAB} based on a master base station key, an IP address of the first access network device, and an IP address of the first device;

establishing, by the first access network device and by using the K_{IAB}, a secure tunnel between the first device and the first access network device.

8. The method according to claim 7, wherein the RRC reconfiguration message comprises the IP address of the first device, and the method further comprises:

assigning, by the first access network device, the IP address of the first device to the first device.

9. The method according to claim 7 or 8, further comprises:

when the first access network device has an IAB node function, sending, by the first access network device, a notification message to a second device, wherein the notification message

indicates that the first access network device serves as the IAB donor of the first device.

10. The method according to any one of claims 7 to 9, further comprises:

selecting, by the first access network device the third access network device as the secondary base station of the first device.

11. The method according to any one of claims 1 to 10， wherein the master base station key is for performing security protection on communication between the master base station and the IAB node.

12. The method according to any one of claims 1 to 11, wherein the master base station key is K_{gNB}.

13. The method according to any one of claims 1 to 12, wherein the secondary base station key is for performing security protection on communication between the secondary base station and the IAB node.

14. The method according to any one of claims 1 to 13, wherein the secondary base station key is Ksn.

15. The method according to any one of claims 1 to 14, wherein both the master base station and the secondary base station are 5th generation 5G base stations.

16. The method according to any one of claims 7 to 15, further comprising:

receiving, by the third access network device, the SN addition/modification request message;

sending, by the third access network device, the SN addition/modification request ACK message to the first access network device;

receiving, by the third access network device, the SN reconfiguration complete message.

17. The method according to any one of claims 7 to 15, further comprising:

when the first access network device has an IAB node function, sending, by the first access network device, a notification message to a second device, wherein the notification message indicates that the first access network device serves as the IAB donor of the first device;

receiving, by the second device, the notification message;

sending, by the second device, an IP address notification message to the first device, wherein the IP address notification message comprises an IP address of the first access network device.

18. The method according to any one of claims 7 to 17, further comprising:

registering, by the first device, with the network through the first access network device;

receiving, by the first device, the RRC reconfiguration messag;

sending, by the first device, the RRC reconfiguration complete message to the first access network device;

determining, by the first device based on the fourth indication information, that the master base station serves as the IAB donor;

generating, by the first device, the K_{IAB} based on the master base station key, the IP address of the first access network device, and the IP address of the first device; and

establishing, by the first device and by using the K_{IAB}, the secure tunnel between the first device and the first access network device.

19. A communication apparatus, wherein the communication apparatus comprises means for performing the method according to any one of claims 1 to 15.

20. A communication apparatus, comprising a processor, wherein the processor executes computer program instructions, the method according to any one of claims 1 to 15.

21. A computer-readable storage medium, wherein the computer-readable storage medium stores computer instructions, and when the computer instructions are run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 15.

22. A computer program product, wherein the computer program product comprises instructions, and when the instructions are run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 15.

23. A communication system, comprising: a first access network device configured to perform the method according to any one of claims 7 to 15, and a third access network device configured to:

receive the SN addition/modification request message;

send the SN addition/modification request ACK message to the first access network device;

receive the SN reconfiguration complete message.

24. The system according to claim 23, further comprising the second device configured to:

receive the notification message;

send an IP address notification message to the first device, wherein the IP address notification message comprises an IP address of the first access network device.

25. The system according to claim 23 or 24, further comprising the first device configured to:

register with the network through the first access network device;

receive the RRC reconfiguration messag;

send the RRC reconfiguration complete message to the first access network device;

determine, based on the fourth indication information, that the master base station serves as the IAB donor;

generate the K_{IAB} based on the master base station key, the IP address of the first access network device, and the IP address of the first device; and

establish, by using the K_{IAB}, the secure tunnel between the first device and the first access network device.

~~1. A key generation method, wherein the method comprises:~~

~~determining, by a first access network device, that a first device that registers with a 5G core network by using the first access network device is an integrated access and backhaul IAB node;~~

~~when a secondary base station needs to be selected for the first device, determining, by the first access network device, whether the first access network device has an IAB donor function;~~

~~if the first access network device does not have the IAB donor function, selecting, by the first access network device, a second access network device having the IAB donor function as the secondary base station of the first device;~~

~~obtaining, by the first access network device, a first key input parameter;~~

~~generating, by the first access network device, a first IAB key K_{IAB1} based on a master base station key and the first key input parameter, wherein the master base station key is used to perform security protection on communication between the first access network device and the first device, and K_{IAB1} is used to establish a secure tunnel between the second access network device and the first device; and~~

~~sending, by the first access network device, K_{IAB1} to the second access network device.~~

~~2. The method according to claim 1, wherein the selecting, by the first access network device, a second access network device having the IAB donor function as the secondary base station of the first device comprises:~~

~~sending, by the first access network device, a first request message to a second device, wherein the first request message comprises an identifier of the first device; and~~

~~receiving, by the first access network device, a first response message sent by the second device, wherein the first response message comprises an identifier of the second access network device.~~

~~3. The method according to claim 1 or 2, wherein the first key input parameter comprises a first IP address and a second IP address, the first IP address is an IP address used by the first device to communicate with an IAB donor, and the second IP address is an IP address used by the second access network device to communicate with an IAB node.~~

~~4. The method according to claim 3, wherein the obtaining, by the first access network device, a first key input parameter comprises:~~

~~sending, by the first access network device, a secondary base station configuration message to the second access network device, wherein the secondary base station configuration message is used to configure the second access network device as the secondary base station of the first device, the secondary base station configuration message comprises first indication information and/or second indication information, the first indication information is used to request the first IP address, and the second indication information is used to request the second IP address; and~~

~~receiving, by the first access network device, a secondary base station configuration response message sent by the second access network device, wherein the secondary base station configuration response message comprises the first IP address and/or the second IP address.~~

~~5. The method according to claim 4, wherein the secondary base station configuration message comprises a secondary base station key derived from the master base station key, and the secondary base station key is used to perform security protection on communication between the secondary base station and the first device.~~

~~6. The method according to claim 5, wherein the method further comprises:~~

~~sending, by the first access network device, the first IP address to the first device.~~

~~7. The method according to claim 3, wherein the obtaining, by the first access network device, a first key input parameter comprises:~~

~~receiving, by the first access network device, an IP address notification message sent by the first device, wherein the IP address notification message comprises the first IP address;~~

~~sending, by the first access network device, a secondary base station configuration message to the second access network device, wherein the secondary base station configuration message is used to configure the second access network device as the secondary base station of the first device, the secondary base station configuration message comprises second indication information, and the second indication information is used to request the second IP address; and~~

~~receiving, by the first access network device, a secondary base station configuration response~~

message sent by the second access network device, wherein the secondary base station configuration response message comprises the second IP address.

8. The method according to any one of claims 1 to 7, wherein the method further comprises:

if the first access network device has the IAB donor function, selecting, by the first access network device, a third access network device as the secondary base station of the first device;

obtaining, by the first access network device, a second key input parameter; and

generating, by the first access network device, a second IAB key K_{IAB2} based on the master base station key and the second key input parameter, wherein K_{IAB2} is used to establish a secure tunnel between the first access network device and the first device.

9. The method according to claim 8, wherein the second key input parameter comprises the first IP address and a third IP address, the first IP address is the IP address used by the first device to communicate with the IAB donor, and the third IP address is an IP address used by the first access network device to communicate with the IAB node.

10. The method according to claim 9, wherein the obtaining, by the first access network device, a second key input parameter comprises:

assigning, by the first access network device, the first IP address to the first device; and

obtaining, by the first access network device, the third IP address from a database.

11. The method according to claim 9, wherein the obtaining, by the first access network device, a second key input parameter comprises:

receiving, by the first access network device, the IP address notification message sent by the first device, wherein the IP address notification message comprises the first IP address; and

obtaining, by the first access network device, the third IP address from a database.

12. A key generation method, wherein the method comprises:

receiving, by a second access network device, a secondary base station configuration message sent by a first access network device, wherein the secondary base station configuration message is used to configure the second access network device as a secondary base station of a first device;

when the secondary base station configuration message comprises third indication information, determining, by the second access network device, whether the second access network device has an IAB donor function, wherein the third indication information indicates that the first device is an IAB node; and

when the second access network device has the IAB donor function, obtaining, by the second

access network device, a first IAB key K_{IAB1} from the first access network device, wherein K_{IAB1} is used to establish a secure tunnel between the second access network device and the first device, K_{IAB1} is generated based on a master base station key, and the master base station key is used to perform security protection on communication between the first access network device and the first device.

13. The method according to claim 12, wherein that K_{IAB1} is generated based on a master base station key comprises:

K_{IAB1} is generated based on the master base station key and a first key input parameter, wherein the first key input parameter comprises a first IP address and a second IP address, the first IP address is an IP address used by the first device to communicate with an IAB donor, and the second IP address is an IP address used by the second access network device to communicate with an IAB node.

14. The method according to claim 13, wherein the secondary base station configuration message further comprises first indication information and/or second indication information, the first indication information is used to request the first IP address, and the second indication information is used to request the second IP address.

15. The method according to claim 14, wherein the method further comprises:

sending, by the second access network device, a secondary base station configuration response message to the first access network device, wherein the secondary base station configuration response message comprises the first IP address and/or the second IP address.

16. The method according to claim 15, wherein the obtaining, by the second access network device, K_{IAB1} from the first access network device comprises:

receiving, by the second access network device, a secondary base station reconfiguration complete message sent by the first access network device, wherein the secondary base station reconfiguration complete message comprises K_{IAB1}.

17. The method according to claim 14, wherein the obtaining, by the second access network device, K_{IAB1} from the first access network device comprises:

sending, by the second access network device, a key request message to the first access network device, wherein the key request message is used to request K_{IAB1}; and

receiving, by the second access network device, a key response message sent by the first access network device, wherein the key response message comprises K_{IAB1}.

18. The method according to claim 17, wherein the key request message further comprises the first IP address and/or the second IP address.

19. A key generation method, wherein the method comprises:

determining, by a first access network device, that a first device that registers with a network by using the first access network device is an IAB node;

when a secondary base station needs to be selected for the first device, determining, by the first access network device, whether the first access network device has an IAB donor function;

if the first access network device has the IAB donor function, selecting, by the first access network device, a third access network device as the secondary base station of the first device; and

generating, by the first access network device, a second IAB key K_{IAB2} based on a secondary base station key, wherein K_{IAB2} is used to establish a secure tunnel between the first access network device and the first device, and the secondary base station key is used to perform security protection on communication between the secondary base station and the first device.

20. The method according to claim 19, wherein the secondary base station key is derived from a master base station key, and the master base station key is used to perform security protection on communication between the first access network device and the first device.

21. The method according to claim 19 or 20, wherein after the generating, by the first access network device, K_{IAB2} based on a secondary base station key, the method further comprises:

sending, by the first access network device, a secondary base station configuration message to a second access network device, wherein the secondary base station configuration message comprises the secondary base station key; and

receiving, by the first access network device, a secondary base station configuration response message sent by the second access network device.

22. The method according to claim 20 or 21, wherein the generating, by the first access network device, K_{IAB2} based on a secondary base station key comprises:

generating, by the first access network device, K_{IAB2} based on the secondary base station key after sending the secondary base station configuration message.

23. The method according to claim 20 or 21, wherein the generating, by the first access network device, K_{IAB2} based on a secondary base station key comprises:

generating, by the first access network device, K_{IAB2} based on the secondary base station key after receiving the secondary base station configuration response message.

~~24. The method according to any one of claims 19 to 23, wherein the method further comprises:~~

~~if the first access network device does not have the IAB donor function, selecting, by the first access network device, the second access network device having the IAB donor function as the secondary base station of the first device; and~~

~~sending, by the first access network device, the secondary base station configuration message to the second access network device, wherein the secondary base station configuration message comprises the secondary base station key.~~

~~25. A communication apparatus, wherein the communication apparatus comprises a module configured to perform the steps in the method according to any one of claims 1 to 24.~~

~~26. A computer-readable storage medium, wherein the computer-readable storage medium stores computer instructions, and when the computer instructions are run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 24.~~

~~27. A computer program product, wherein the computer program product comprises instructions, and when the instructions are run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 24.~~

~~28. A chip, wherein the chip comprises a processing unit and a transceiver pin, the processing unit is configured to perform a processing operation in the method according to any one of claims 1 to 24, and the transceiver pin is configured to perform a communication operation in the method according to any one of claims 1 to 24.~~