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;

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;

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.

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. The method according to any one of claims 1 to 6, wherein the master base station key is for performing security protection on communication between the master base station and the IAB node, and the secondary base station key is for performing security protection on communication between the secondary base station and the IAB node.

8. The method according to any one of claims 1 to 7, wherein the master base station key is K_{gNB}, and the secondary base station key is Ksn.

9. The method according to any one of claims 1 to 8, wherein both the master base station and the secondary base station are 5th generation 5G base stations.

10. 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;

wherein a master base station key is generated in a process in which the IAB node registers with a network through the master base station.

11. The method according to claim 10, 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.

12. The method according to claim 10 or 11, 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.

13. The method according to any one of claims 10 to 12, further comprises:

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

14. The method according to any one of claims 10 to 13, wherein the master base station key is for performing security protection on communication between the master base station and the IAB node, and the secondary base station key is for performing security protection on communication between the secondary base station and the IAB node.

15. The method according to any one of claims 10 to 14, wherein the master base station key is $K_{gN}B$, and the secondary base station key is Ksn.

16. The method according to any one of claims 10 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 10 to 16, 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 10 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 10 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.