CLAIMS

What is claimed is:

1. An authentication method, comprising:

receiving an authentication vector request message from a serving call session control function network element;

calculating a first hash value of a security parameter based on a first security algorithm;

calculating a second hash value of the security parameter based on a second security algorithm; and

returning an authentication vector request response to the serving call session control function network element, wherein the authentication vector request response carries the first hash value and the second hash value.

2. The method according to claim 1, wherein the authentication vector request response comprises the first hash value and the second hash value that are carried in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm.

3. The method according to claim 1 or 2, wherein the first security algorithm is a secure hash algorithm SHA256 or a secure hash algorithm SHA512, and the second security algorithm is message digest 5 algorithm.

4. An authentication method, comprising:

receiving a first registration request message from a terminal device;

sending an authentication vector request message to a home subscriber server;

receiving an authentication vector request response returned by the home subscriber server, wherein the authentication vector request response carries a first hash value and a second hash value, the first hash value is calculated based on a first security algorithm, and the second hash value is calculated based on a second security algorithm;

sending an authentication challenge request message to the terminal device, wherein the authentication challenge request message carries information about the first security algorithm and information about the second security algorithm;

receiving a second registration request message from the terminal device, wherein the second registration request message comprises a first authentication response and information about a

third security algorithm, the first authentication response is calculated based on the third security algorithm, and the third security algorithm is the first security algorithm or the second security algorithm;

selecting, from the first hash value and the second hash value, a hash value corresponding to the third security algorithm;

calculating a second authentication response based on the third security algorithm and the hash value corresponding to the third security algorithm; and

checking the first authentication response by using the second authentication response, to obtain an authentication result of the terminal device.

5. The method according to claim 4, wherein the authentication vector request response comprises the first hash value and the second hash value that are carried in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm; and

the selecting, from the first hash value and the second hash value, a hash value corresponding to the third security algorithm comprises: selecting, based on the preset order from the first hash value and the second hash value, the hash value corresponding to the third security algorithm.

6. The method according to claim 4 or 5, wherein the authentication challenge request message comprises the information about the first security algorithm and the information about the second security algorithm that are carried in a preset order, and the preset order is determined based on the priority of the first security algorithm and the priority of the second security algorithm.

7. The method according to any one of claims 3 to 6, wherein the first security algorithm is a secure hash algorithm SHA256 or a secure hash algorithm SHA512, and the second security algorithm is message digest 5 algorithm.

8. An authentication method, comprising:

receiving an authentication challenge request message from a serving call session control function network element, wherein the authentication challenge request message carries information about a first security algorithm and information about a second security algorithm;

determining a third security algorithm, wherein the third security algorithm is the first security algorithm or the second security algorithm;

calculating a hash value of a security parameter based on the third security algorithm;

calculating an authentication response based on the third security algorithm and the hash

value; and

sending a registration request message to the serving call session control function network element, wherein the registration request message carries the authentication response, and the authentication response is used to authenticate the terminal device.

9. The method according to claim 8, wherein the authentication challenge request message comprises the information about the first security algorithm and the information about the second security algorithm that are carried in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm.

10. The method according to claim 8 or 9, wherein the determining a third security algorithm comprises: determining as the third security algorithm, a 1st security algorithm that can be identified by the terminal device and that is in the authentication challenge request message.

11. The method according to any one of claims 8 to 10, wherein the first security algorithm is a secure hash algorithm SHA256 or a secure hash algorithm SHA512, and the second security algorithm is message digest 5 algorithm.

12. A communication apparatus, comprising:

a receiving unit, configured to receive an authentication vector request message from a serving call session control function network element;

a processing unit, configured to: calculate a first hash value of a security parameter based on a first security algorithm, and

calculate a second hash value of the security parameter based on a second security algorithm; and

a sending unit, configured to return an authentication vector request response to the serving call session control function network element, wherein the authentication vector request response carries the first hash value and the second hash value.

13. The apparatus according to claim 12, wherein the authentication vector request response comprises the first hash value and the second hash value that are carried in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm.

14. The apparatus according to claim 12 or 13, wherein the first security algorithm is a secure hash algorithm SHA256 or a secure hash algorithm SHA512, and the second security algorithm is message digest 5 algorithm.

15. A communication apparatus, comprising:

a receiving unit, configured to receive a first registration request message from a terminal device;

a sending unit, configured to send an authentication vector request message to a home subscriber server, wherein

the receiving unit is further configured to receive an authentication vector request response returned by the home subscriber server, wherein the authentication vector request response carries a first hash value and a second hash value, the first hash value is calculated based on a first security algorithm, and the second hash value is calculated based on a second security algorithm;

the sending unit is further configured to send an authentication challenge request message to the terminal device, wherein the authentication challenge request message carries information about the first security algorithm and information about the second security algorithm; and

the receiving unit is further configured to receive a second registration request message from the terminal device, wherein the second registration request message comprises a first authentication response and information about a third security algorithm, the first authentication response is calculated based on the third security algorithm, and the third security algorithm is the first security algorithm or the second security algorithm; and

a processing unit, configured to select, from the first hash value and the second hash value, a hash value corresponding to the third security algorithm, wherein

the processing unit is further configured to calculate a second authentication response based on the third security algorithm and the hash value corresponding to the third security algorithm; and

the processing unit is further configured to check the first authentication response by using the second authentication response, to obtain an authentication result of the terminal device.

16. The apparatus according to claim 15, wherein the authentication vector request response comprises the first hash value and the second hash value that are carried in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm; and the processing unit is specifically configured to select, based on the preset order from the first hash value and the second hash value, the hash value corresponding to the third security algorithm.

17. The apparatus according to claim 15 or 16, wherein the authentication challenge request

message comprises the information about the first security algorithm and the information about the second security algorithm that are carried in a preset order, and the preset order is determined based on the priority of the first security algorithm and the priority of the second security algorithm.

18. The apparatus according to claim 15, 16, or 17, wherein the first security algorithm is a secure hash algorithm SHA256 or a secure hash algorithm SHA512, and the second security algorithm is message digest 5 algorithm.

19. A communication apparatus, comprising:

a receiving unit, configured to receive an authentication challenge request message from a serving call session control function network element, wherein the authentication challenge request message carries information about a first security algorithm and information about a second security algorithm;

a processing unit, configured to determine a third security algorithm, wherein the third security algorithm is the first security algorithm or the second security algorithm, wherein

the processing unit is further configured to calculate a hash value of a security parameter based on the third security algorithm, and

the processing unit is further configured to calculate an authentication response based on the third security algorithm and the hash value; and

a sending unit, configured to send a registration request message to the serving call session control function network element, wherein the registration request message carries the authentication response, and the authentication response is used to authenticate the communication apparatus.

20. The apparatus according to claim 19, wherein the authentication challenge request message comprises the information about the first security algorithm and the information about the second security algorithm that are carried in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm.

21. The apparatus according to claim 19 or 20, wherein the processing unit is specifically configured to determine, as the third security algorithm, a 1st security algorithm that can be identified by the processing unit and that is in the authentication challenge request message.

22. The apparatus according to any one of claims 19 to 21, wherein the first security algorithm is a secure hash algorithm SHA256 or a secure hash algorithm SHA512, and the second security algorithm is a message digest MD5 algorithm.

23. An authentication method, comprising:

sending a first registration request message to a serving call session control function network element, wherein the first registration request message carries information about security algorithms that can be supported by the terminal device, and the security algorithms comprise at least one of the following: a first security algorithm or a second security algorithm;

receiving an authentication challenge message from the serving call session control function network element, wherein the authentication challenge message comprises information about a third security algorithm, and the third security algorithm is one of the security algorithms that can be supported by the terminal device;

calculating a hash value of a security parameter based on the third security algorithm;

calculating an authentication response based on the third security algorithm and the hash value; and

sending a second registration request message to the serving call session control function network element, wherein the second registration request message carries the authentication response, and the authentication response is used to authenticate the terminal device.

24. An authentication method, comprising:

receiving a first registration request message from a terminal device, wherein the first registration request message comprises information about security algorithms that can be supported by the terminal device, and the security algorithms comprise at least one of the following: a first security algorithm or a second security algorithm;

sending an authentication vector request message to a home subscriber server, wherein the authentication vector request message comprises the information about the security algorithms that can be supported by the terminal device;

receiving an authentication vector request response returned by the home subscriber server, wherein the authentication vector request response comprises a hash value and information about a third security algorithm, the hash value is obtained through calculation based on the third security algorithm, and the third security algorithm is one of the security algorithms that can be supported by the terminal device;

sending an authentication challenge message to the terminal device, wherein the authentication challenge message comprises the information about the third security algorithm;

receiving a second registration request message from the terminal device, wherein the second

registration request message carries a first authentication response;

calculating a second authentication response based on the third security algorithm and the hash value; and

checking the first authentication response by using the second authentication response, to obtain an authentication result of the terminal device.

25. An authentication method, comprising:

receiving an authentication vector request message from a serving call session control function network element, wherein the authentication vector request message comprises information about security algorithms that can be supported by a terminal device, and the security algorithms comprise at least one of the following: a first security algorithm or a second security algorithm;

calculating a hash value of a security parameter based on a third security algorithm, wherein the third security algorithm is one of the security algorithms that can be supported by the terminal device; and

returning an authentication vector request response to the serving call session control function network element, wherein the authentication vector request response carries the hash value and information about the third security algorithm.

26. A communication apparatus, comprising:

a sending unit, configured to send a first registration request message to a serving call session control function network element, wherein the first registration request message carries information about security algorithms that can be supported by the communication apparatus, and the security algorithms comprise at least one of the following: a first security algorithm or a second security algorithm;

a receiving unit, configured to receive an authentication challenge message from the serving call session control function network element, wherein the authentication challenge message comprises information about a third security algorithm, and the third security algorithm is one of the security algorithms that can be supported by the communication apparatus; and

a processing unit, configured to calculate a hash value of a security parameter based on the third security algorithm, wherein

the processing unit is further configured to calculate an authentication response based on the third security algorithm and the hash value; and

the sending unit is further configured to send a second registration request message to the serving call session control function network element, wherein the second registration request message carries the authentication response, and the authentication response is used to authenticate the communication apparatus.

27. A communication apparatus, comprising:

a receiving unit, configured to receive a first registration request message from a terminal device, wherein the first registration request message comprises information about security algorithms that can be supported by the terminal device, and the security algorithms comprise at least one of the following: a first security algorithm or a second security algorithm;

a sending unit, configured to send an authentication vector request message to a home subscriber server, wherein the authentication vector request message comprises the information about the security algorithms that can be supported by the terminal device, wherein

the receiving unit is further configured to receive an authentication vector request response returned by the home subscriber server, wherein the authentication vector request response comprises a hash value and information about a third security algorithm, the hash value is obtained through calculation based on the third security algorithm, and the third security algorithm is one of the security algorithms that can be supported by the terminal device;

the sending unit is further configured to send an authentication challenge message to the terminal device, wherein the authentication challenge message comprises the information about the third security algorithm; and

the receiving unit is further configured to receive a second registration request message from the terminal device, wherein the second registration request message carries a first authentication response; and

a processing unit, configured to calculate a second authentication response based on the third security algorithm and the hash value, wherein

the processing unit is further configured to check the first authentication response by using the second authentication response, to obtain an authentication result of the terminal device.

28. A communication apparatus, comprising:

a receiving unit, configured to receive an authentication vector request message from a serving call session control function network element, wherein the authentication vector request message comprises information about security algorithms that can be supported by a terminal

device, and the security algorithms comprise at least one of the following: a first security algorithm or a second security algorithm;

a processing unit, configured to calculate a hash value of a security parameter based on a third security algorithm, wherein the third security algorithm is one of the security algorithms that can be supported by the terminal device; and

a sending unit, configured to return an authentication vector request response to the serving call session control function network element, wherein the authentication vector request response carries the hash value and information about the third security algorithm.

29. The method according to any one of claims 23 to 25, or the apparatus according to any one of claims 26 to 28, wherein the first security algorithm is a secure hash algorithm SHA256, and the second security algorithm is a secure hash algorithm SHA512.

30. A communication apparatus, comprising a processor and a transceiver, wherein the processor is configured to perform a processing operation in the method according to any one of claims 1 to 11, and the transceiver is configured to perform a communication operation in the method according to any one of claims 1 to 11; or the processor is configured to perform a processing operation in the method according to any one of claims 23 to 25, and the transceiver is configured to perform a communication operation in the method according to any one of claims 23 to 25.

31. 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 11, or the computer is enabled to perform the method according to any one of claims 23 to 25.

32. A computer program product, 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 11, or the computer is enabled to perform the method according to any one of claims 23 to 25.

33. A chip, wherein the chip comprises a processing circuit and a transceiver pin, the processing circuit is configured to perform a processing operation in the method according to any one of claims 1 to 11, and the transceiver pin is configured to perform a communication operation in the method according to any one of claims 1 to 11; or the processing circuit is configured to perform a processing operation in the method according to any one of claims 23 to 25, and the transceiver pin is configured to perform a communication operation in the method according to

any one of claims 23 to 25.

34. An authentication method, comprising:

receiving, by a serving call session control function network element, a first registration request message from a terminal device;

sending, by the serving call session control function network element, an authentication vector request message to a home subscriber server;

receiving, by the home subscriber server, the authentication vector request message;

calculating, by the home subscriber server, a first hash value of a security parameter based on a first security algorithm;

calculating, by the home subscriber server, a second hash value of the security parameter based on a second security algorithm; and

returning, by the home subscriber server, an authentication vector request response to the serving call session control function network element, wherein the authentication vector request response carries the first hash value and the second hash value.

receiving, by the serving call session control function network element, the authentication vector request response returned by the home subscriber server,

sending, by the serving call session control function network element, an authentication challenge request message to the terminal device, wherein the authentication challenge request message carries information about the first security algorithm and information about the second security algorithm;

receiving, by the serving call session control function network element, a second registration request message from the terminal device, wherein the second registration request message comprises a first authentication response and information about a third security algorithm, the first authentication response is calculated based on the third security algorithm, and the third security algorithm is the first security algorithm or the second security algorithm;

selecting, by the serving call session control function network element from the first hash value and the second hash value, a hash value corresponding to the third security algorithm;

calculating, by the serving call session control function network element, a second authentication response based on the third security algorithm and the hash value corresponding to the third security algorithm; and

checking, by the serving call session control function network element, the first authentication

response by using the second authentication response, to obtain an authentication result of the terminal device.

35. The method according to claim 34, wherein the authentication vector request response comprises the first hash value and the second hash value that are carried in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm .

36. The method according to claim 34 or 35, wherein the authentication vector request response comprises the first hash value and the second hash value that are carried in a preset order, and the preset order is determined based on a priority of the first security algorithm and a priority of the second security algorithm; and

the selecting, by the serving call session control function network element from the first hash value and the second hash value, a hash value corresponding to the third security algorithm comprises: selecting, by the serving call session control function network element based on the preset order from the first hash value and the second hash value, the hash value corresponding to the third security algorithm.

37. The method according to claim 34, 35 or 36, wherein the authentication challenge request message comprises the information about the first security algorithm and the information about the second security algorithm that are carried in a preset order, and the preset order is determined based on the priority of the first security algorithm and the priority of the second security algorithm.

38. The method according to any one of claims 34 to 37, further comprising:

sending, by the terminal device, the first registration request message to the serving call session control function network element;

receiving, by the terminal device, the authentication challenge request message;

determining, by the terminal device, the third security algorithm;

calculating, by the terminal device, the hash value of the security parameter based on the third security algorithm;

calculating, by the terminal device, the first authentication response based on the third security algorithm and the hash value; and

sending, by the terminal device, the second registration request message to the serving call session control function network element, wherein the second registration request message carries the first authentication response, and the first authentication response is used to authenticate the

terminal device.

39. The method according to claim 38, wherein the determining, by the terminal device, the third security algorithm comprises: determining, by the terminal device, as the third security algorithm, a 1st security algorithm that can be identified by the terminal device and that is in the authentication challenge request message.

40. The method according to any one of claims 34 to 39, wherein the first security algorithm is a secure hash algorithm SHA256 or a secure hash algorithm SHA512, and the second security algorithm is message digest 5 algorithm.

41. A wireless communication system, comprising: a communication apparatus according to any one of claims 12 to 14, and a communication apparatus according to any one of claims 15 to 18; or a communication apparatus according to claim 26 or 27.

42. The system according to claim 41, wherein the system further comprises: a communication apparatus according to any one of claims 19 to 22, or a communication apparatus according to claim 28.