CLAIMS

1. A secure communication method, comprising:

sending, by a first secure communication apparatus, first information of the first secure communication apparatus to a second secure communication apparatus through a first message, wherein the first message comprises one or more of a first port number, a first security parameter index SPI, a first internet protocol IP address, a first security algorithm list, and a first random number;

receiving, by the first secure communication apparatus, a second message that comprises second information and that is from the second secure communication apparatus, wherein the second message comprises one or more of a second port number, a second security parameter index SPI, a second internet protocol IP address, a second security algorithm list, and a second random number; and

based on the first information and/or the second information, determining, by the first secure communication apparatus in a first calculation manner, a first salt value used for uplink transmission between the first secure communication apparatus and the second secure communication apparatus, and determining, in a second calculation manner, a second salt value used for downlink transmission between the first secure communication apparatus and the second secure communication apparatus,

wherein the determining the first salt value in the first calculation manner comprises: calculating the first salt value using a direction indicator of uplink transmission; and the determining the second salt value in the second calculation manner comprises: calculating the second salt value using a direction indicator of downlink transmission.

2. The method according to claim 1, wherein the first information is comprised in the first security algorithm listthat is in the first message; and/or

the second information is comprised in the second security algorithm list that is in the second message.

3. The method according to claim 1 or 2, wherein the first information indicates, in a form of an information element, a salt value calculation manner supported by the first secure communication apparatus; and/or wherein the second information indicates, in a form of an information element, a salt value calculation manner supported by the second secure communication apparatus.

4. The method according to claim 3, wherein the first information is an identifier or an indication of an algorithm.

5. The method according to any one of claims 1 to 4, wherein after receiving the second

message, the method further comprises:

determining, by the first secure communication apparatus, the first calculation manner and the second calculation manner, based on a salt value calculation manner that is supported by the second secure communication apparatus in the second information and a salt value calculation manner supported by the first secure communication apparatus.

6. The method according to any one of claims 1 to 5, wherein the first secure communication apparatus is a terminal device, or a chip or a circuit disposed in a terminal device;

wherein the second secure communication apparatus is a proxy call session control function network element, or a chip or a circuit disposed in a proxy call session control function network element.

7. The method according to claim 6, wherein after receiving the second information, the method further comprises:

determining, by the first secure communication apparatus, the second secure communication apparatus has received the first information, and the second secure communication apparatus supports a salt value calculation manner that is supported by the terminal device and that is in the first information.

8. The method according to any one of claims 1 to 5, wherein the second secure communication apparatus is a terminal device, or a chip or a circuit disposed in a terminal device;

wherein the first secure communication apparatus is a proxy call session control function network element, or a chip or a circuit disposed in a proxy call session control function network element.

9. The method according to claim 8, wherein after receiving the second information, the method further comprises:

determining, by the first secure communication apparatus, based on a salt value calculation manner that is supported by the second secure communication apparatus and that is in the second information and a salt value calculation manner that is supported by the first secure communication apparatus and that is in the first information, that the first secure communication apparatus supports the salt value calculation manner supported by the second secure communication apparatus.

10. A secure communication method, comprising:

the method according to any one of claims 1 to 8; and

receiving, by the second secure communication apparatus, the first information;

sending, by the second secure communication apparatus, the second information;

based on the first information and/or the second information, determining, by the second secure communication apparatus in the first calculation manner, the first salt value, and

determining, in the second calculation manner, the second salt value.

11. The method according to claim 10, wherein the sending, by the second secure communication apparatus, the second information comprises:

sending the second information when determining that the secure communication apparatus supports a salt value calculation manner of the first secure communication apparatus in the first informaiton.

12. A secure communication apparatus, configured to perform the method according to any one of claims 1 to 9.

13. A computer-readable storage medium, wherein the computer-readable storage medium stores 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 9.

14. A computer program product, wherein the computer program product comprises instructions used to perform the method according to any one of claims 1 to 9.

15. A system comprising a first secure communication apparatus and a second secure communication apparatus,

wherein the first secure communication apparatus is configured to perform the method according to any one of claims 1 to 9; and

wherein the second secure communication apparatus is configured to the method according to claim 10 or 11 of the second secure communication apparatus.

16. A chip, wherein the chip comprises a processor and a communication interface, and when the processor reads a computer program or instructions through the communication interface and runs the computer program or the instructions, the communication apparatus is enabled to perform the method according to any one of claims 1 to 9.

17. A secure communication apparatus, comprising a processor, wherein the processor is coupled to a memory, the memory is configured to store instructions, and the processor is configured to read the instructions stored in the memory, to enable the secure communication apparatus to implement the method according to any one of claims 1 to 9.