CLAIMS

What is claimed is:

1. A method for determining a user plane security algorithm, comprising:

receiving, by a second terminal UE 2, a direct communication request message from a first terminal UE 1, wherein the direct communication request message comprises a security capability of the UE 1 and a control plane security policy of the UE 1;

determining, by the UE 2, a control plane security protection mode between the UE 2 and the UE 1 based on the control plane security policy of the UE 1 and a control plane security policy of the UE 2; and

when the control plane security protection mode is that control plane integrity protection is enabled and control plane confidentiality protection is not enabled:

sending, by the UE 2, a direct security mode command message to the UE 1, and

when receiving a direct security mode complete message carrying a user plane security policy of the UE 1 from the UE 1, regardless of the user plane security policy of the UE 1 and a user plane security policy of the UE 2, determining, by the UE 2, that user plane confidentiality protection between the UE 2 and the UE 1 is not enabled, wherein

the direct security mode command message comprises a non-null integrity protection algorithm and a null confidentiality protection algorithm.

2. The method according to claim 1, wherein the method further comprises:

selecting, by the UE 2, the non-null integrity protection algorithm and the null confidentiality protection algorithm based on a security capability of the UE 2 and the security capability of the UE 1.

3. A method for determining a user plane security algorithm, comprising:

sending, by a first terminal UE 1, a direct communication request message to a second terminal UE 2, wherein the direct communication request message comprises a security capability of the UE 1 and a control plane security policy of the UE 1;

receiving, by the UE 1, a direct security mode command message from the UE 2, wherein the direct security mode command message comprises a non-null integrity protection algorithm and a

null confidentiality protection algorithm, wherein

the direct security mode command message is sent by the UE 2 when the UE 2 determines, based on the control plane security policy of the UE 1 and a control plane security policy of the UE 2, that a control plane security protection mode is that control plane integrity protection is enabled and control plane confidentiality protection is not enabled; and

sending, by the UE 1 to the UE 2 based on the non-null integrity protection algorithm and the null confidentiality protection algorithm, a direct security mode complete message, wherein the direct security mode complete message comprises a user plane security policy of the UE 1.

4. A method for determining a user plane security algorithm, comprising:

selecting, by a second device, a non-null user plane confidentiality protection algorithm based on a security capability of a first device and a security capability of the second device in a case in which user plane confidentiality protection between the second device and the first device is enabled and control plane confidentiality protection between the second device and the first device is not enabled; and

sending, by the second device, a first message to the first device, wherein the first message comprises first algorithm indication information indicating the user plane confidentiality protection algorithm.

5. The method according to claim 4, wherein the first message further comprises indication information indicating to enable user plane confidentiality protection between the second device and the first device.

6. The method according to claim 4 or 5, wherein the method further comprises:

receiving, by the second device, a second message from the first device, wherein the second message comprises a user plane security policy of the first device; and

determining, by the second device based on the user plane security policy of the first device and a user plane security policy of the second device, that user plane confidentiality protection between the second device and the first device is enabled.

7. The method according to claim 6, wherein before the receiving, by the second device, a second message from the first device, the method further comprises:

receiving, by the second device, a third message from the first device, wherein the third message comprises a control plane security policy of the first device and the security capability of the first device; and

determining, by the second device based on the control plane security policy of the first device and a control plane security policy of the second device, that control plane confidentiality protection between the second device and the first device is not enabled.

8. The method according to claim 7, wherein the method further comprises:

sending, by the second device, a fourth message to the first device, wherein the fourth message comprises indication information indicating a null control plane confidentiality protection algorithm.

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

storing, by the second device, the security capability of the first device.

10. A method for determining a user plane security algorithm, comprising:

sending, by a first device, a third message to a second device, wherein the third message comprises a control plane security policy of the first device and a security capability of the first device;

receiving, by the first device, a fourth message from the second device, wherein the fourth message comprises indication information indicating a null control plane confidentiality protection algorithm;

sending, by the first device, a second message to the second device, wherein the second message comprises a user plane security policy of the first device;

receiving, by the first device, a first message from the second device, wherein the first message comprises first algorithm indication information indicating a non-null user plane confidentiality protection algorithm; and

confidentiality protecting, by the first device, user plane data between the first device and the second device based on the user plane confidentiality protection algorithm indicated by the first algorithm indication information.

11. The method according to claim 10, wherein the first message further comprises indication information indicating to enable user plane confidentiality protection between the second device and the first device.

12. The method according to claim 10 or 11, wherein the fourth message further comprises indication information indicating a control plane integrity protection algorithm; and

before the confidentiality protecting, by the first device, user plane data between the first device and the second device based on the user plane confidentiality protection algorithm indicated

by the first algorithm indication information, the method further comprises:

enabling, by the first device, control plane integrity protection between the first device and the second device based on the control plane integrity protection algorithm indicated by the indication information of the control plane integrity protection algorithm.

performing, by the first device, integrity verification on the first message; and

enabling, by the first device when the first message is successfully verified, user plane confidentiality protection between the first device and the second device based on the user plane confidentiality protection algorithm indicated by the first algorithm indication information.

13. A communication apparatus, comprising:

a transceiver module, configured to receive a direct communication request message from a first terminal UE 1, wherein the direct communication request message comprises a security capability of the UE 1 and a control plane security policy of the UE 1; and

a processing module, configured to determine a control plane security protection mode between the communication apparatus and the UE 1 based on the control plane security policy of the UE 1 and a control plane security policy of the communication apparatus, wherein

when the control plane security protection mode is that control plane integrity protection is enabled and control plane confidentiality protection is not enabled:

the transceiver module is further configured to send a direct security mode command message to the UE 1, and

when the transceiver modules receives, from the UE 1, a direct security mode complete message carrying a user plane security policy of the UE 1, regardless of the user plane security policy of the UE 1 and a user plane security policy of the UE 2, the processing module is further configured to determine that user plane confidentiality protection between the communication apparatus and the UE 1 is not enabled, wherein

the direct security mode command message comprises a non-null integrity protection algorithm and a null confidentiality protection algorithm.

14. The communication apparatus according to claim 13, wherein

the processing module is further configured to select the non-null integrity protection algorithm and the null confidentiality protection algorithm based on a security capability of the communication apparatus and the security capability of the UE 1.

15. A communication apparatus, comprising:

a transceiver module, configured to send a direct communication request message to a second terminal UE 2, wherein the direct communication request message comprises a security capability of the communication apparatus and a control plane security policy of the communication apparatus, wherein

the transceiver module is further configured to receive a direct security mode command message from the UE 2, wherein the direct security mode command message comprises a non-null integrity protection algorithm and a null confidentiality protection algorithm, wherein

the direct security mode command message is sent by the UE 2 when the UE 2 determines, based on the control plane security policy of the communication apparatus and a control plane security policy of the UE 2, that a control plane security protection mode is that control plane integrity protection is enabled and control plane confidentiality protection is not enabled; and

the transceiver module is further configured to send, to the UE 2 based on the non-null integrity protection algorithm and the null confidentiality protection algorithm, a direct security mode complete message carrying a user plane security policy of the communication apparatus, wherein the direct security mode complete message comprises the user plane security policy of the communication apparatus.

16. A communication apparatus, comprising a processing module and a transceiver module, wherein

the processing module is configured to select a non-null user plane confidentiality protection algorithm based on a security capability of a first device and a security capability of the communication apparatus in a case in which user plane confidentiality protection between the communication apparatus and the first device is enabled and control plane confidentiality protection between the communication apparatus and the first device is not enabled; and

the transceiver module is configured to send a first message to the first device, wherein the first message comprises first algorithm indication information indicating the user plane confidentiality protection algorithm.

17. The communication apparatus according to claim 16, wherein the first message further comprises indication information indicating to enable user plane confidentiality protection between the communication apparatus and the first device.

18. The communication apparatus according to claim 16 or 17, wherein

the transceiver module is further configured to receive a second message from the first device, wherein the second message comprises a user plane security policy of the first device; and

the processing module is further configured to determine, based on the user plane security policy of the first device and a user plane security policy of the communication apparatus, that user plane confidentiality protection between the second device and the first device is enabled.

19. The communication apparatus according to claim 18, wherein

the transceiver module is further configured to: receive, before the communication apparatus receives the second message from the first device, a third message from the first device, wherein the third message comprises a control plane security policy of the first device and the security capability of the first device; and

the processing module is further configured to determine, based on the control plane security policy of the first device and a control plane security policy of the communication apparatus, that control plane confidentiality protection between the communication apparatus and the first device is not enabled.

20. The communication apparatus according to claim 19, wherein

the transceiver module is further configured to send a fourth message to the first device, wherein the fourth message comprises indication information indicating a null control plane confidentiality protection algorithm.

21. The communication apparatus according to claim 19 or 20, wherein

the processing module is further configured to store the security capability of the first device.

22. A communication apparatus, comprising a processing module and a transceiver module, wherein

the transceiver module is configured to sending a third message to a second device, wherein the third message comprises a control plane security policy of the communication apparatus and a security capability of the communication apparatus;

the transceiver module is further configured to receiving a fourth message from the second device, wherein the fourth message comprises indication information indicating a null control plane confidentiality protection algorithm;

the transceiver module is further configured to send a second message to the second device, wherein the second message comprises a user plane security policy of the communication apparatus;

the transceiver module is further configured to receive a first message from the second device, wherein the first message comprises first algorithm indication information indicating a non-null user plane confidentiality protection algorithm; and

the processing module is configured to confidentiality protect user plane data between the communication apparatus and the second device based on the user plane confidentiality protection algorithm indicated by the first algorithm indication information.

23. The communication apparatus according to claim 22, wherein the first message further comprises indication information indicating to enable user plane confidentiality protection between the second device and the communication apparatus.

24. The communication apparatus according to claim 22 or 23, wherein the fourth message further comprises indication information indicating a control plane integrity protection algorithm;

the processing module is further configured to enable, before confidentiality protecting the user plane data between the communication apparatus and the second device based on the user plane confidentiality protection algorithm indicated by the first algorithm indication information, control plane integrity protection between the first device and the second device based on the control plane integrity protection algorithm indicated by the indication information of the control plane integrity protection algorithm;

the processing module is further configured to perform integrity verification on the first message; and

the processing module is further configured to: enable, when the first message is successfully verified, user plane confidentiality protection between the communication apparatus and the second device based on the user plane confidentiality protection algorithm indicated by the first algorithm indication information.

25. A communication apparatus, comprising a processor, wherein the processor is coupled to a memory, the memory is configured to store a program or instructions, and when the program or the instructions are executed by the processor, the apparatus is enabled to perform the method according to any one of claims 1 to 12.

26. A computer-readable storage medium, storing a computer program, wherein when the computer program is executed, a computer is enabled to perform the method according to any one of claims 1 to 12.

27. A communication system, comprising a first device and a second device, wherein

the second device is configured to select a non-null user plane confidentiality protection algorithm based on a security capability of a first device and a security capability of the second device in a case in which user plane confidentiality protection between the second device and the first device is enabled and control plane confidentiality protection between the second device and the first device is not enabled; and send a first message to the first device, wherein the first message comprises first algorithm indication information indicating the user plane confidentiality protection algorithm; and

the first device is configured to receive the first message.

28. The system according to claim 27, wherein the first message further comprises indication information indicating to enable user plane confidentiality protection between the second device and the first device.

29. The system according to claim 27 or 28, wherein

the first device is further configured to send a second message to the second device, wherein the second message comprises a user plane security policy of the first device;

the second device is further configured to determine, based on the user plane security policy of the first device and a user plane security policy of the second device, that user plane confidentiality protection between the second device and the first device is enabled.

30. The system according to claim 27, wherein

the first device is further configured to send a third message to a second device, wherein the third message comprises a control plane security policy of the first device and a security capability of the first device; and

the second device is further configured to determine, based on the control plane security policy of the first device and a control plane security policy of the second device, that control plane confidentiality protection between the second device and the first device is not enabled; and send a fourth message to the first device, wherein the fourth message comprises indication information indicating a null control plane confidentiality protection algorithm.

31. The system according to claim 29, wherein

the second device is further configured to store the security capability of the first device.

32. The system according to claim 29, wherein the fourth message further comprises indication information indicating a control plane integrity protection algorithm; and

the first device is configured to enable control plane integrity protection between the first

device and the second device based on the control plane integrity protection algorithm indicated by the indication information of the control plane integrity protection algorithm; perform integrity verification on the first message; and enable, when the first message is successfully verified, user plane confidentiality protection between the communication apparatus and the second device based on the user plane confidentiality protection algorithm indicated by the first algorithm indication information.

33. A communication system, comprising a first terminal UE 1 and a second terminal UE 2, wherein

the UE 1 is configured to send a direct communication request message to the UE 2, wherein the direct communication request message comprises a security capability of the UE 1 and a control plane security policy of the UE 1;

the UE 2 is configured to receive the direct communication request message;

the UE 2 is further configured to determine a control plane security protection mode between the UE 2 and the UE 1 based on the control plane security policy of the UE 1 and a control plane security policy of the UE 2; and send a direct security mode command message to the UE 1 when the control plane security protection mode is that control plane integrity protection is enabled and control plane confidentiality protection is not enabled, wherein

the direct security mode command message comprises a non-null integrity protection algorithm and a null confidentiality protection algorithm;

the UE 1 is further configured to receive the direct security mode command message and send, to the UE 2 based on the non-null integrity protection algorithm and the null confidentiality protection algorithm, a direct security mode complete message carrying a user plane security policy of the UE 1, wherein the direct security mode complete message comprises the user plane security policy of the UE 1; and

the UE 2 is further configured to receive, from the UE 1, a direct security mode complete message carrying a user plane security policy of the UE 1, and regardless of the user plane security policy of the UE 1 and a user plane security policy of the UE 2, determine that user plane confidentiality protection between the UE 2 and the UE 1 is not enabled.

34. The system according to claim 33, wherein

the UE 2 is further configured to select the non-null integrity protection algorithm and the null confidentiality protection algorithm based on a security capability of the UE 2 and the security

capability of the UE 1.