CLAIMS

What is claimed is:

1. A method for determining a user plane security algorithm, wherein the method is performed by a second terminal UE 2 or an apparatus in the UE 2, and the method comprises :

receiving 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 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 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 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 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, wherein the method is performed by a first terminal UE 1 or an apparatus in the UE 1, and the method comprises:

sending 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 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, 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 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.

5. The communication apparatus according to claim 4, 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.

6. 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, wherein the direct security mode complete message comprises a user plane security policy of the communication apparatus.

7. 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 3.

8. 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 3.

9. 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.

10. The system according to claim 9, 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.