Content in the discovery message is protected by code-receiving security parameters or code security parameters.

**[0110]** The discoveree UE self-selects a source layer 2 ID for the discovery procedure (such as 5G ProSe direct discovery, 5G ProSe U2N discovery/ranging, or SL positioning discovery), and sets a source layer 2 ID of the received discovery message as the destination layer 2 ID.

**[0111]** As an example, the discoveree UE may create and store the security context including the self-selected source layer 2 ID, the service code, and the security key associated with the service code after sending the response message.

**[0112]** As another example, the discoveree UE may create and store the security context including the self-selected source layer 2 ID, the service code, and the security key associated with the service code after selecting the source layer 2 ID.

**[0113]** As another example, the discoveree UE may create and store the security context including the self-selected source layer 2 ID, the service code, and the security key associated with the service code after completing the discovery procedure.

**[0114]** At S402, a DCR is received.

**[0115]** The DCR includes a destination layer 2 ID and encrypted information for the SL communication.

**[0116]** For a detailed description of step S402 and related details, reference may be made to the description of step S201 and related details, which is not repeated here.

**[0117]** At S403, a security context matching the destination layer 2 ID is determined from one or more pre-stored security contexts based on the destination layer 2 ID.

**[0118]** At S404, the security key is determined based on the matched security context.

**[0119]** At S405, the encrypted information is decrypted using the security key for performing the SL communication.

**[0120]** For detailed descriptions of steps S402 to S405 and related details, reference may be made to the descriptions of steps S301 to S303 and related details, which are not repeated here.

any one of: creating and storing the security context when determining the layer 2 ID for the discovery procedure; creating and storing the security context after sending a discovery message for the discovery procedure; or creating and storing the security context after completing the discovery procedure.

**[0137]** FIG. 8 is a block diagram illustrating a communication device 800 according to an embodiment of the disclosure. The communication device 800 may be UE, a chip, a system on chip or a processor that supports the communication device to implement the method, or a chip, a system on chip or a processor that supports the UE to implement the method. The communication device 800 may be configured to implement the method described in the method embodiments, which may refer to descriptions in the method embodiments.

**[0138]** The communication device 800 may include one or more processors 801. The processor 801 may include a general purpose processor or a dedicated processor. For example, the processor may be a baseband processor or a central processor. The baseband processor may be configured to process a communication protocol and communication data, and the central processor may be configured to control a communication device (e.g., a network side device, a baseband chip, a UE, a UE chip, a DU or CU, etc.), to execute a computer program, and process data of the computer program.

**[0139]** Optionally, the communication device 800 may further include one or more memories 802 with a computer program 804 stored. The processor 801 executes the computer program 804 so that the communication device 800 performs the method as described in the above method embodiments. Optionally, the memory 802 may further store data. The communication device 800 and the memory 802 may be independently configured or integrated together.

**[0140]** Optionally, the communication device 800 may further include a transceiver 805 and an antenna 806. The transceiver 805 may be referred to as a transceiving unit, a transceiver or a transceiving circuit, which may be configured to achieve a transceiving function. The transceiver 805 may include a receiver and a transmitter. The receiver may be referred to as a receiving unit or a receiving circuit, etc., for

**WHAT IS CLAIMED IS:**

1. A method for sidelink (SL) communication, performed by a user equipment (UE), comprising:

receiving a direct communication request (DCR), wherein the DCR comprises a destination layer 2 identification (ID) and encrypted information for the SL communication;

determining a security key for decrypting the encrypted information based on the destination layer 2 ID; and

decrypting the encrypted information using the security key for performing the SL communication.

2. The method according to claim 1, wherein determining the security key for decrypting the encrypted information based on the destination layer 2 ID comprises:

determining, based on the destination layer 2 ID, a security association matching the destination layer 2 ID from one or more pre-stored security associations; and

determining the security key based on the matched security association.

3. The method according to claim 2, wherein each security association comprises: a service code for identifying a connectivity service of the SL communication, a layer 2 ID corresponding to the service code, and a security key associated with the service code.

4. The method according to claim 3, wherein the service code comprises one of:

a relay service code (RSC);

a proximity based service (ProSe) restricted code;

a ProSe query code;

a ProSe response code; or

a ranging service code.

5. The method according to claim 3 or 4, wherein each security association further comprises at least one of:

a UE-to-network (U2N) relay layer indicator; or

a control plane security indicator.

6. The method according to any one of claims 2 to 5, further comprising:

creating and storing a security association based on a layer 2 ID, a service code, and a security key which are determined during a discovery procedure.

7. The method according to claim 6, wherein creating and storing the security association comprises one of:

creating and storing the security association when determining the layer 2 ID for the discovery procedure;

creating and storing the security association after sending a discovery message for the discovery procedure; or

creating and storing the security association after completing the discovery procedure.

8. A communication device (800), comprising: a transceiver (805); a memory (802); a processor (801) connected to both the transceiver (805) and the memory (802), configured to control wireless signal transmission/reception of the transceiver (805) by executing computer-executable instructions stored in the memory (802), and enable the method according to any one of claims 1 to 7 to be implemented.

9. A computer storage medium, storing computer-executable instructions thereon, wherein when the computer-executable instructions are executed by a processor, the method of any one of claims 1 to 7 is implemented.