What is claimed is:

1. An encrypted communication method, applied to a first party, wherein the first party uses a new link protocol, NLP, stack, and the method comprises:

obtaining, by a first protocol layer of the first party, an MAC address of a second party according to a data transmission request from an application layer, wherein the data transmission request comprises an NLP address of the second party;

generating, by the first protocol layer, a first temporary key pair, wherein the first temporary key pair comprises a first temporary public key and a first temporary private key;

obtaining, by the first protocol layer, a second temporary public key of the second party according to the first temporary public key;

generating, by the first protocol layer, a shared key according to the second temporary public key and the first temporary private key; and

determining, by the first protocol layer, a data message, wherein the data message carries the MAC address of the second party and encrypted data obtained by encrypting using the shared key, and a receiving party of the data message is the second party;

wherein the obtaining, by the first protocol layer of the first party, the MAC address of the second party according to the data transmission request from the application layer, comprises:

generating, by the first protocol layer, an address resolution request message, wherein a source address of the address resolution request message is an NLP address of the first party, a destination address of the address resolution request message is the NLP address of the second party, the address resolution request message comprises the MAC address of the first party and a first signature, the first signature is generated based on a first private key of the first party, and the NLP address of the first party is a public key corresponding to the first private key;

obtaining, by the first protocol layer, a first response message from the second party, wherein the first response message is a response message corresponding to the address resolution request message, a source address of the first response message is the NLP address of the second party, a destination address of the response message is the NLP address of the first party, the response message comprises the MAC address of the second party and a second signature, the second signature is generated based on a second private

key of the second party, and the NLP address of the second party is a public key corresponding to the second private key;

obtaining, by the first protocol layer, the MAC address of the second party, after the first protocol layer determines that the second signature has been verified according to the NLP address of the second party;

wherein the address resolution request message is an extended Address Resolution Protocol, ARP, message, and the method further comprises:

encrypting, by the first party, to-be-signed content in the address resolution request message according to the first private key, to obtain the first signature.

2. The method according to claim 1, wherein the obtaining, by the first protocol layer of the first party, the MAC address of the second party according to the data transmission request from the application layer, the data transmission request comprising the NLP address of the second party, comprises:

determining, by the first protocol layer, the MAC address of the second party according to the NLP address of the second party and a first corresponding relationship, the first corresponding relationship comprising a corresponding relationship between the NLP address of the second party and the MAC address of the second party.

3. The method according to claim 1, wherein the obtaining, by the first protocol layer, the second temporary public key of the second party according to the first temporary public key, comprises:

generating, by the first protocol layer, a key negotiation request message, wherein the key negotiation request message comprises a third signature and the first temporary public key, a source address of the key negotiation request message is an NLP address of the first party, a destination address of the key negotiation request message is the NLP address of the second party, the third signature is generated based on a first private key of the first party, and the NLP address of the first party is a public key corresponding to the first private key;

obtaining, by the first protocol layer, a second response message, wherein the second response message is a response message corresponding to the key negotiation request message, the second response message comprises a fourth signature and the second temporary public key, a source address of the second response message is the NLP address of the second party, a destination address of the second response message is the

NLP address of the first party, the fourth signature is generated based on a second private key of the second party, and the NLP address of the second party is a public key corresponding to the second private key;

determining, by the first protocol layer, the shared key according to the first temporary private key and the second temporary public key, after the first protocol layer determines that the fourth signature has been verified according to the NLP address of the second party.

4. The method according to claim 3, further comprising:

generating, by the first party, the first private key randomly;

generating, by the first party, the public key corresponding to the first private key through elliptic curve cryptography according to the first private key;

using, by the first party, the public key corresponding to the first private key as the NLP address of the first party.

5. The method according to claim 1, wherein the to-be-signed content comprises a time stamp, and the time stamp is used for verifying timeliness of the address resolution request message.

6. The method according to claim 1, wherein before the first party sends the address resolution request message to the second party, the method further comprises:

determining, by the first party, that the MAC address of the second party is not stored in a neighbor list, wherein the neighbor list is used for storing a corresponding relationship between an NLP address and an MAC address of a communication device communicating with the first party.

7. An encrypted communication method, applied to a second party, wherein the second party uses a new link protocol, NLP, stack, and the method comprises:

obtaining, by a second protocol layer of the second party, a first temporary public key of a first party;

generating, by the second protocol layer, a second temporary key pair, wherein the second temporary key pair comprises a second temporary public key and a second temporary private key;

generating, by the second protocol layer, a shared key according to the first temporary public key and the second temporary private key;

generating, by the second protocol layer, a message carrying the second temporary public key, wherein a receiving party of the message is the first party, and the second temporary public key is used for the first party to generate the shared key; and

decrypting, by the first protocol layer, encrypted data carried in a data message according to the shared key, wherein a sending party of the data message is the first party, and the data message further carries an MAC address of the second party;

wherein the method further comprises:

receiving, by the second protocol layer, an address resolution request message from the first party, wherein a source address of the address resolution request message is an NLP address of the first party, a destination address of the address resolution request message is an NLP address of the second party, the address resolution request message comprises an MAC address of the first party and a first signature, the first signature is generated based on a first private key of the first party, and the NLP address of the first party is a public key corresponding to the first private key;

generating, by the second protocol layer, a first response message, wherein the first response message is a response message corresponding to the address resolution request message, a source address of the first response message is the NLP address of the second party, a destination address of the response message is the NLP address of the first party, the response message comprises the MAC address of the second party and a second signature, the second signature is generated based on a second private key of the second party, and the NLP address of the second party is a public key corresponding to the second private key;

wherein the first response message is an extended Address Resolution Protocol, ARP, message, and the method further comprises:

encrypting, by the second party, to-be-signed content in the first response message according to the second private key, to obtain the first signature.

8. The method according to claim 7, wherein the obtaining, by the second protocol layer of the second party, the first temporary public key of the first party, comprises:

obtaining, by the second protocol layer of the second party, a key negotiation request message from the first party, wherein the key negotiation request message comprises a third signature and the first temporary public key, a source address of the key negotiation request message is an NLP address of the first party, a destination address of

the key negotiation request message is an NLP address of the second party, the third signature is generated based on a first private key of the first party, and the NLP address of the first party is a public key corresponding to the first private key.

9. The method according to claim 8, wherein the generating, the second protocol layer, the second temporary key pair, comprises:

generating, the second protocol layer, the second temporary key pair, after the second protocol layer determines that the third signature has been verified according to the NLP address of the first party.

10. The method according to claim 9, wherein the generating, by the second protocol layer, the message carrying the second temporary public key, comprises:

generating, by the second protocol layer, a second response message, wherein the second response message is a response message corresponding to the key negotiation request message, the second response message comprises a fourth signature and the second temporary public key, a source address of the second response message is the NLP address of the second party, a destination address of the second response message is the NLP address of the first party, the fourth signature is generated based on a second private key of the second party, and the NLP address of the second party is a public key corresponding to the second private key.

11. The method according to claim 7, further comprising:

generating, by the second party, the second private key randomly;

generating, by the second party, the public key corresponding to the second private key through elliptic curve cryptography according to the second private key;

using, by the second party, the public key corresponding to the second private key as the NLP address of the second party.

12. The method according to claim 7, wherein the to-be-signed content comprises a time stamp, and the time stamp is used for verifying timeliness of the first response message.

13. An encrypted communication apparatus, applied to a first party, wherein the first party uses a new link protocol, NLP, stack, and the apparatus comprises:

an MAC address obtaining module, configured to obtain an MAC address of a second party according to a data transmission request from an application layer, wherein the data transmission request comprises an NLP address of the second party;

a key generating module, configured to generate a first temporary key pair, wherein the first temporary key pair comprises a first temporary public key and a first temporary private key; wherein the key generating module is further configured to obtain a second temporary public key of the second party according to the first temporary public key, and generate a shared key according to the second temporary public key and the first temporary private key; and

a determining module, configured to determine a data message, wherein the data message carries the MAC address of the second party and encrypted data obtained by encrypting using the shared key, and a receiving party of the data message is the second party;

wherein the MAC address obtaining module is further configured to generate an address resolution request message, wherein a source address of the address resolution request message is an NLP address of the first party, a destination address of the address resolution request message is the NLP address of the second party, the address resolution request message comprises the MAC address of the first party and a first signature, the first signature is generated based on a first private key of the first party, and the NLP address of the first party is a public key corresponding to the first private key; obtain a first response message from the second party, wherein the first response message is a response message corresponding to the address resolution request message, a source address of the first response message is the NLP address of the second party, a destination address of the response message is the NLP address of the first party, the response message comprises the MAC address of the second party and a second signature, the second signature is generated based on a second private key of the second party, and the NLP address of the second party is a public key corresponding to the second private key; obtain the MAC address of the second party, after determining that the second signature has been verified according to the NLP address of the second party;

wherein the address resolution request message is an extended Address Resolution Protocol, ARP, message, and the MAC address obtaining module is further configured to encrypt to-be-signed content in the address resolution request message according to the first private key, to obtain the first signature.

14. An encrypted communication apparatus, applied to a second party, wherein the second party uses a new link protocol, NLP, stack, and the apparatus comprises:

an obtaining module, configured to obtain a first temporary public key of a first party;

a key generating module, configured to generate a second temporary key pair, wherein the second temporary key pair comprises a second temporary public key and a second temporary private key; wherein the key generating module is further configured to generate a shared key according to the first temporary public key and the second temporary private key;

a message generating module, configured to generate a message carrying the second temporary public key, wherein a receiving party of the message is the first party, and the second temporary public key is used for the first party to generate the shared key; and

a decrypting module, configured to decrypt encrypted data carried in a data message according to the shared key, wherein a sending party of the data message is the first party, and the data message further carries an MAC address of the second party;

wherein the apparatus further comprises a module configured to receive an address resolution request message from the first party, wherein a source address of the address resolution request message is an NLP address of the first party, a destination address of the address resolution request message is an NLP address of the second party, the address resolution request message comprises an MAC address of the first party and a first signature, the first signature is generated based on a first private key of the first party, and the NLP address of the first party is a public key corresponding to the first private key; generate a first response message, wherein the first response message is a response message corresponding to the address resolution request message, a source address of the first response message is the NLP address of the second party, a destination address of the response message is the NLP address of the first party, the response message comprises the MAC address of the second party and a second signature, the second signature is generated based on a second private key of the second party, and the NLP address of the second party is a public key corresponding to the second private key;

wherein the first response message is an extended Address Resolution Protocol, ARP, message, and the apparatus further comprises a module configured to encrypt to-be-signed content in the first response message according to the second private key, to obtain the first signature.

15. The encrypted communication apparatus according to claim 13, wherein the apparatus further comprises:

a storing module, configured to store a corresponding relationship between the NLP address of the second party and the MAC address of the second party, after determining that the second signature has been verified according to the NLP address of the second party.