CLAIMS

1. A data transmission method, executed by a communication adapter, and the method comprising:

performing mutual authentication with a first interaction device;

receiving, after the mutual authentication is completed, encrypted interaction data obtained by encrypting interaction data using a working key and transmitted by the first interaction device, the working key being obtained by the first interaction device by mapping an authentication key used in the mutual authentication;

decrypting the encrypted interaction data using the working key obtained by mapping the authentication key by the communication adapter; and

transmitting interaction data obtained through the decryption to a second interaction device, through a simulated device node identifiable by the second interaction device and using a communication protocol of the second interaction device, the communication protocol being natively adapted to the device node;

wherein the performing mutual authentication with a first interaction device comprises:

receiving a first challenge code transmitted by the first interaction device;

decrypting the first challenge code using the authentication key to obtain a first random number, the first random number being a random number generated by the first interaction device;

performing a hash operation on the first random number to obtain a first hash value;

generating a second random number, and encrypting the first hash value and the second random number using the authentication key to obtain a second challenge code;

transmitting the second challenge code to the first interaction device, wherein the first interaction device decrypts the second challenge code using the authentication key to obtain the first hash value, compares the first hash value with a second hash value obtained by the first interaction device by encrypting the first random number using the authentication key, and in response to the first hash value being same as the second hash value, performs a hash operation on the second random number obtained by decrypting the second challenge code, and returns a second hash value obtained by the hash operation; and

receiving the second hash value returned by the first interaction device, comparing the second hash value with a third hash value obtained by the communication adapter by performing a hash

operation on the second random number using the authentication key, and in response to the second hash value being same as the third hash value, determining that the mutual authentication between the communication adapter and the first interaction device is complete.

2. The method according to claim 1, further comprising:

receiving a serial number obtaining request transmitted by the first interaction device;

obtaining a device serial number specified in the serial number obtaining request;

returning the obtained device serial number to the first interaction device, wherein the first interaction device generates an authentication key on the first interaction device based on the returned device serial number; and

generating an authentication key on the communication adapter according to the obtained device serial number, the authentication key on the first interaction device being same as the authentication key on the communication adapter.

3. The method according to claim 2, wherein the authentication key on the first interaction device is obtained by encrypting the returned device serial number using a serial number encryption key stored in the first interaction device; and

the generating an authentication key on the communication adapter according to the obtained device serial number comprises:

obtaining the serial number encryption key stored in the communication adapter; and

encrypting the obtained device serial number using the serial number encryption key to obtain the authentication key on the communication adapter.

4. The method according to claim 1, wherein both the communication adapter and the first interaction device store the authentication key; the authentication key is generated based on a device serial number of the communication adapter; the receiving encrypted interaction data obtained by encrypting interaction data using a working key and transmitted by the first interaction device comprises:

after the first interaction device obtains the working key by mapping the authentication key stored in the first interaction device and encrypts the interaction data with the obtained working key to obtain the encrypted interaction data, receiving the encrypted interaction data obtained by encrypting the interaction data and transmitted by the first interaction device; and

the decrypting the encrypted interaction data using the working key obtained by mapping the authentication key by the communication adapter comprises:

obtaining the working key by mapping the authentication key stored in the communication adapter, and decrypting the encrypted interaction data using the obtained working key.

5. The method according to claim 1, wherein the transmitting interaction data obtained through the decryption to a second interaction device, through a simulated device node identifiable by the second interaction device and using a communication protocol of the second interaction device, the communication protocol being natively adapted to the device node comprises:

converting the interaction data obtained through the decryption into target interaction data complying with the communication protocol natively adapted to the device node; and

transmitting the target interaction data obtained through the conversion to the second interaction device through the simulated device node identifiable by the second interaction device.

6. The method according to claim 5, wherein the device node comprises a human-machine interaction keyboard node and a human-machine interaction controller node; and the transmitting the target interaction data obtained through the conversion to the second interaction device through the simulated device node identifiable by the second interaction device comprises:

reporting the target interaction data to the human-machine interaction controller node in a case that the target interaction data is control type data, to transmit the target interaction data to the second interaction device through the human-machine interaction controller node; and

reporting the target interaction data to the human-machine interaction keyboard node in a case that the target interaction data is transaction type data, to transmit the target interaction data to the second interaction device through the human-machine interaction keyboard node.

7. The method according to any one of claims 1 to 6, wherein the device node comprises a human-machine interaction controller node; and the method further comprises:

receiving, through the human-machine interaction controller node, control data transmitted by the second interaction device;

converting the control data into serial port control data;

encrypting the serial port control data using the working key obtained by mapping the authentication key by the communication adapter to obtain encrypted control data; and

transmitting the encrypted control data to the first interaction device, the encrypted control data being used for instructing the first interaction device to decrypt the encrypted control data with a working key obtained by mapping the authentication key, and perform a control operation according to the control data obtained through the decryption.

8. The method according to any one of claims 1 to 6, wherein the method further comprises:

in a case that the encrypted interaction data or control data received from the second interaction device is a malicious attack packet, or a received network data packet originating from a network side terminal is a malicious attack packet,

triggering a security event, the security event being used for disabling the communication adapter.

9. A data transmission apparatus, comprising:

an authentication module, configured to perform mutual authentication with a first interaction device;

a receiving module, configured to receive, after the mutual authentication is completed, encrypted interaction data obtained by encrypting interaction data using a working key and transmitted by the first interaction device, the working key being obtained by the first interaction device by mapping an authentication key used in the mutual authentication;

a decryption module, configured to decrypt the encrypted interaction data using the working key obtained by mapping the authentication key by a communication adapter; and

a transmission module, configured to transmit interaction data obtained through the decryption to a second interaction device, through a simulated device node identifiable by the second interaction device and using a communication protocol of the second interaction device, the communication protocol being natively adapted to the device node;

wherein the authentication module is configured to:

receive a first challenge code transmitted by the first interaction device;

decrypt the first challenge code using the authentication key to obtain a first random number, the first random number being a random number generated by the first interaction device;

perform a hash operation on the first random number to obtain a first hash value;

generate a second random number, and encrypt the first hash value and the second random number using the authentication key to obtain a second challenge code;

transmit the second challenge code to the first interaction device, wherein the first interaction device decrypts the second challenge code using the authentication key to obtain the first hash value, compares the first hash value with a second hash value obtained by the first interaction device by encrypting the first random number using the authentication key, and in response to the first hash value being same as the second hash value, performs a hash operation on the second random

number obtained by decrypting the second challenge code, and returns a second hash value obtained by the hash operation; and

receive the second hash value returned by the first interaction device, compare the second hash value with a third hash value obtained by performing a hash operation on the second random number using the authentication key, and in response to the second hash value being same as the third hash value, determine that the mutual authentication between the communication adapter and the first interaction device is complete.

10. A data transmission system, comprising: a first interaction device, a second interaction device, and a communication adapter wirelessly connected to the first interaction device and electrically connected to the second interaction device,

the communication adapter being configured to authenticate the first interaction device;

the first interaction device being configured to authenticate the communication adapter when the communication adapter completes the authentication, and after completing the authentication of the communication adapter, encrypt interaction data using a working key obtained by mapping an authentication key used in mutual authentication to obtain encrypted interaction data;

the communication adapter being further configured to receive the encrypted interaction data obtained by encrypting the interaction data using the working key and transmitted by the first interaction device;

the communication adapter being further configured to decrypt the encrypted interaction data using the working key obtained by mapping the authentication key by the communication adapter;

the second interaction device being configured to identify a device node simulated by the communication adapter; and

the communication adapter being further configured to transmit the interaction data obtained through the decryption to the second interaction device through the simulated device node identifiable by the second interaction device and using a communication protocol of the second interaction device, the communication protocol being adapted to the device node;

wherein:

the communication adapter is further configured to receive a first challenge code transmitted by the first interaction device; decrypt the first challenge code using the authentication key to obtain a first random number, the first random number being a random number generated by the first interaction device; perform a hash operation on the first random number to obtain a first hash value; generate a second random number, and encrypt the first hash value and the second random number

using the authentication key to obtain a second challenge code; and transmit the second challenge code to the first interaction device;

the first interaction device is further configured to decrypt the received second challenge code using the authentication key to obtain the first hash value, compare the first hash value with a second hash value obtained by the first interaction device by encrypting the first random number using the authentication key, and in response to the first hash value being same as the second hash value, perform a hash operation on the second random number obtained by decrypting the second challenge code, and return a second hash value obtained by the hash operation; and

the communication adapter is further configured to receive the second hash value returned by the first interaction device, compare the second hash value with a third hash value obtained by the communication adapter by performing a hash operation on the second random number using the authentication key, and in response to the second hash value being same as the third hash value, determine that the mutual authentication between the communication adapter and the first interaction device is complete.

11. The system according to claim 10, wherein the communication adapter is further configured to convert the interaction data obtained through the decryption into target interaction data complying with the communication protocol natively adapted to the device node; and transmit the target interaction data obtained through the conversion to the second interaction device through the simulated device node identifiable by the second interaction device.

12. A computer device, comprising a memory and a processor, the memory storing computer-readable instructions, the computer-readable instructions, when executed by the processor, implementing the operations of the method according to any one of claims 1 to 8.

13. A computer-readable storage medium, storing computer-readable instructions, the computer-readable instructions, when executed by a processor, implementing the operations of the method according to any one of claims 1 to 8.