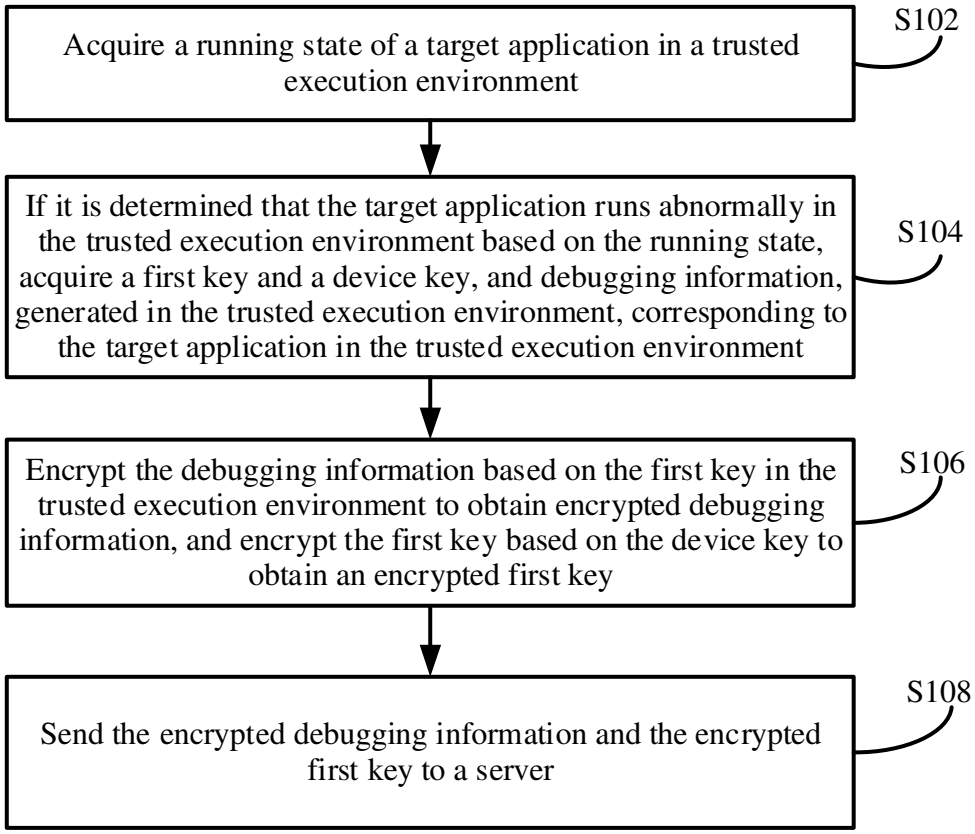

Acquire a running state of a target application in a trusted execution environment
S102
If it is determined that the target application runs abnormally in the trusted execution environment based on the running state, acquire a first key and a device key, and debugging information, generated in the trusted execution environment, corresponding to the target application in the trusted execution environment
S104
Encrypt the debugging information based on the first key in the trusted execution environment to obtain encrypted debugging information, and encrypt the first key based on the device key to obtain an encrypted first key
S106
Send the encrypted debugging information and the encrypted first key to a server
S108

FIG. 1A

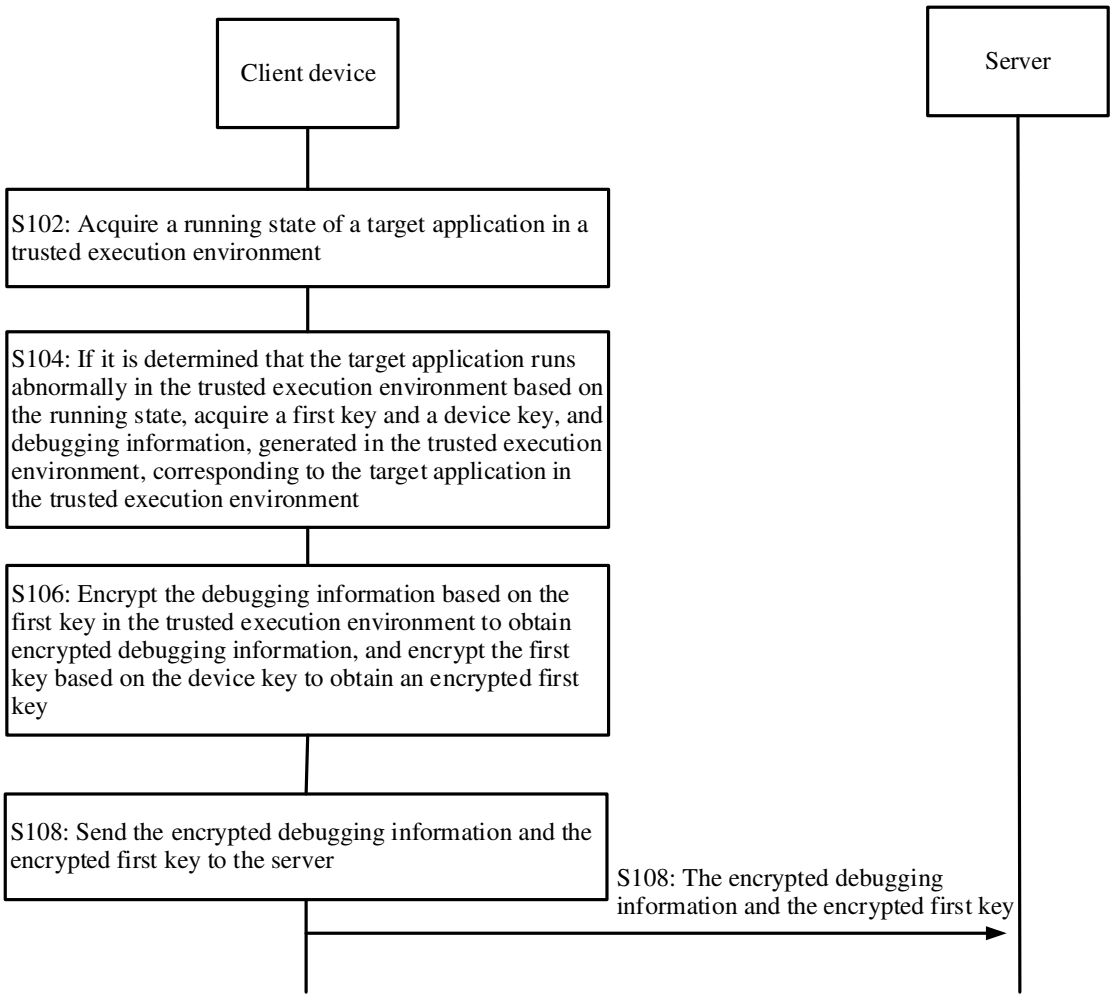

Client device
Server
S102: Acquire a running state of a target application in a trusted execution environment
S104: If it is determined that the target application runs abnormally in the trusted execution environment based on the running state, acquire a first key and a device key, and debugging information, generated in the trusted execution environment, corresponding to the target application in the trusted execution environment
S106: Encrypt the debugging information based on the first key in the trusted execution environment to obtain encrypted debugging information, and encrypt the first key based on the device key to obtain an encrypted first key
S108: Send the encrypted debugging information and the encrypted first key to the server
S108: The encrypted debugging information and the encrypted first key

FIG. 1B

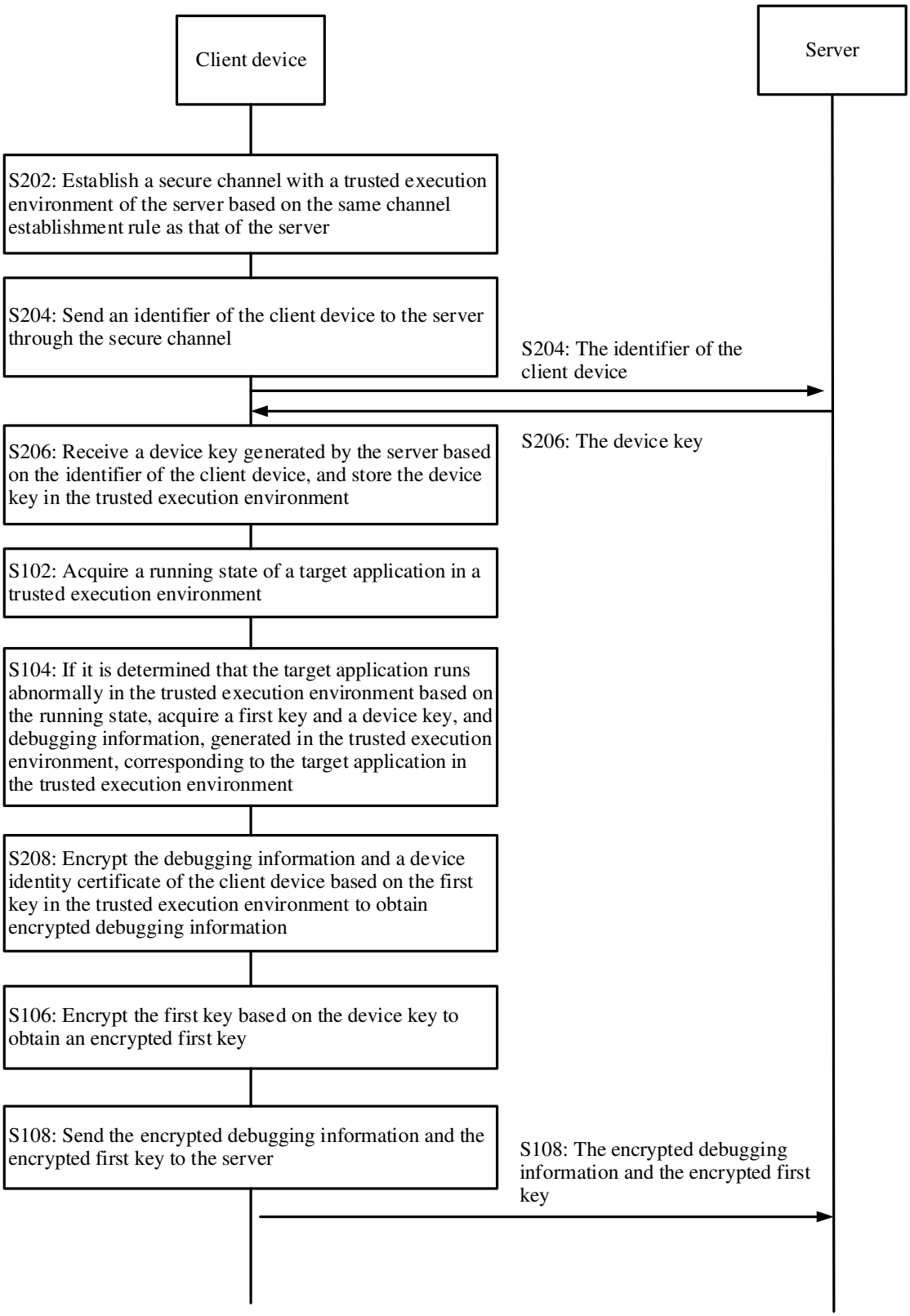

Client device
Server
S202: Establish a secure channel with a trusted execution environment of the server based on the same channel establishment rule as that of the server
S204: Send an identifier of the client device to the server through the secure channel
S204: The identifier of the client device
S206: The device key
S206: Receive a device key generated by the server based on the identifier of the client device, and store the device key in the trusted execution environment
S102: Acquire a running state of a target application in a trusted execution environment
S104: If it is determined that the target application runs abnormally in the trusted execution environment based on the running state, acquire a first key and a device key, and debugging information, generated in the trusted execution environment, corresponding to the target application in the trusted execution environment
S208: Encrypt the debugging information and a device identity certificate of the client device based on the first key in the trusted execution environment to obtain encrypted debugging information
S106: Encrypt the first key based on the device key to obtain an encrypted first key
S108: Send the encrypted debugging information and the encrypted first key to the server
S108: The encrypted debugging information and the encrypted first key

FIG. 2

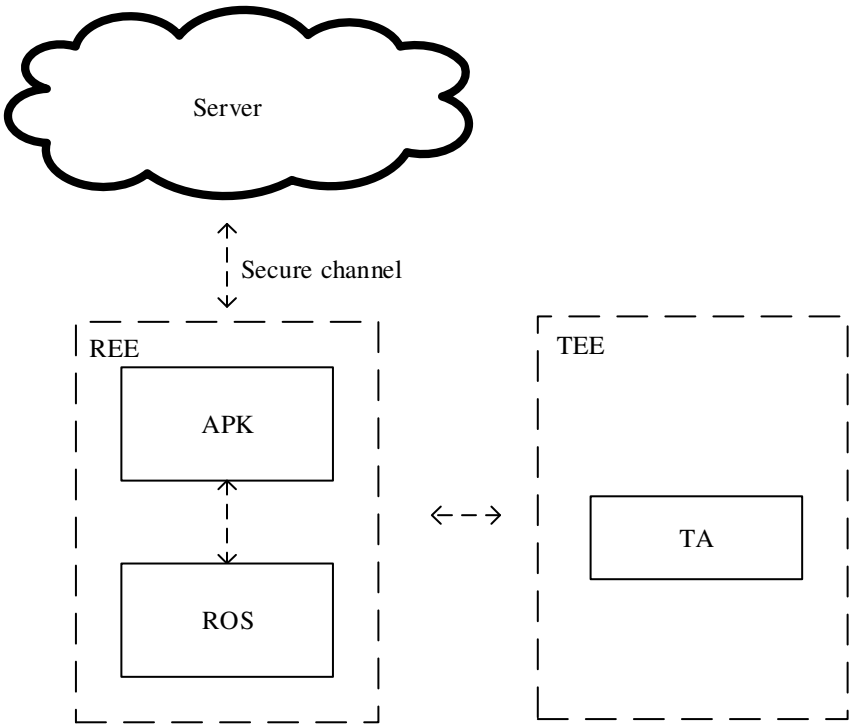

Server
Secure channel
REE
APK
ROS
TEE
TA

FIG. 3

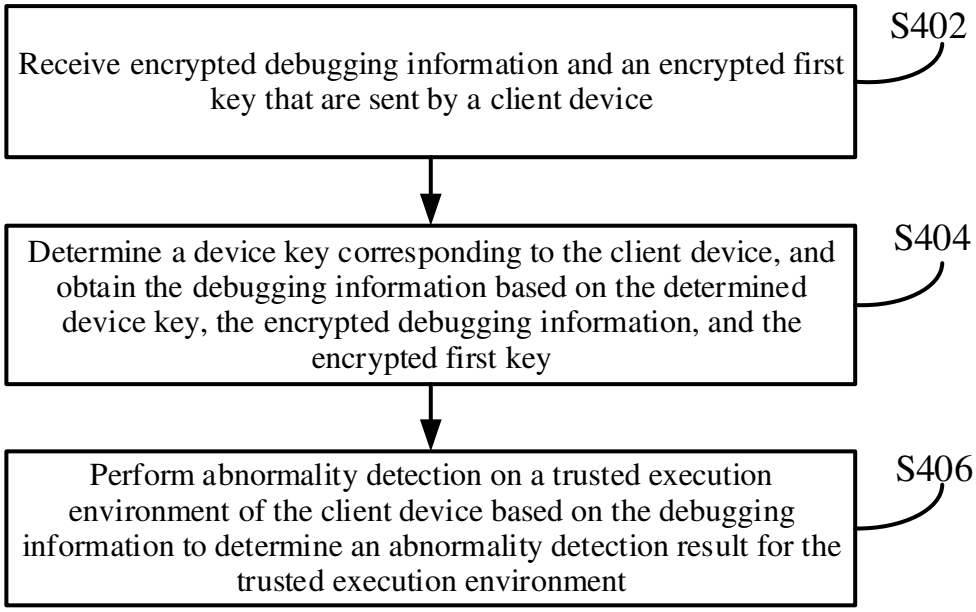

Receive encrypted debugging information and an encrypted first key that are sent by a client device
S402
Determine a device key corresponding to the client device, and obtain the debugging information based on the determined device key, the encrypted debugging information, and the encrypted first key
S404
Perform abnormality detection on a trusted execution environment of the client device based on the debugging information to determine an abnormality detection result for the trusted execution environment
S406

FIG. 4A

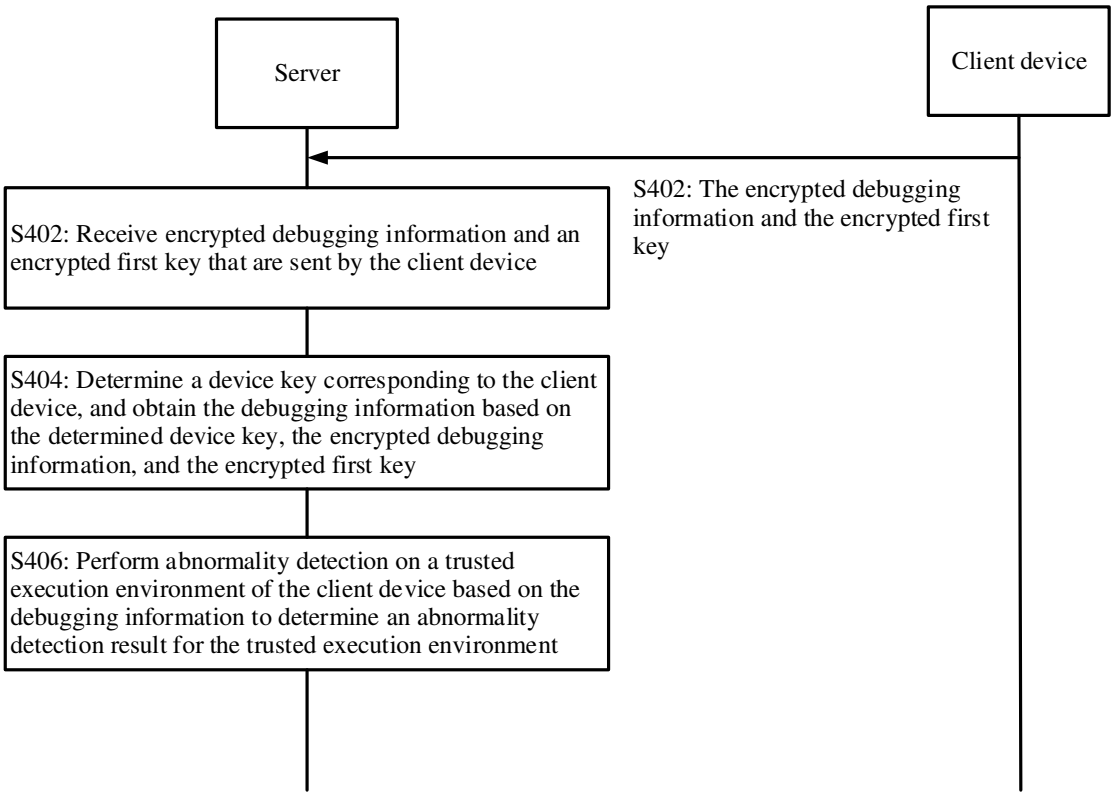

Server
Client device
S402: The encrypted debugging information and the encrypted first key
S402: Receive encrypted debugging information and an encrypted first key that are sent by the client device
S404: Determine a device key corresponding to the client device, and obtain the debugging information based on the determined device key, the encrypted debugging information, and the encrypted first key
S406: Perform abnormality detection on a trusted execution environment of the client device based on the debugging information to determine an abnormality detection result for the trusted execution environment

FIG. 4B

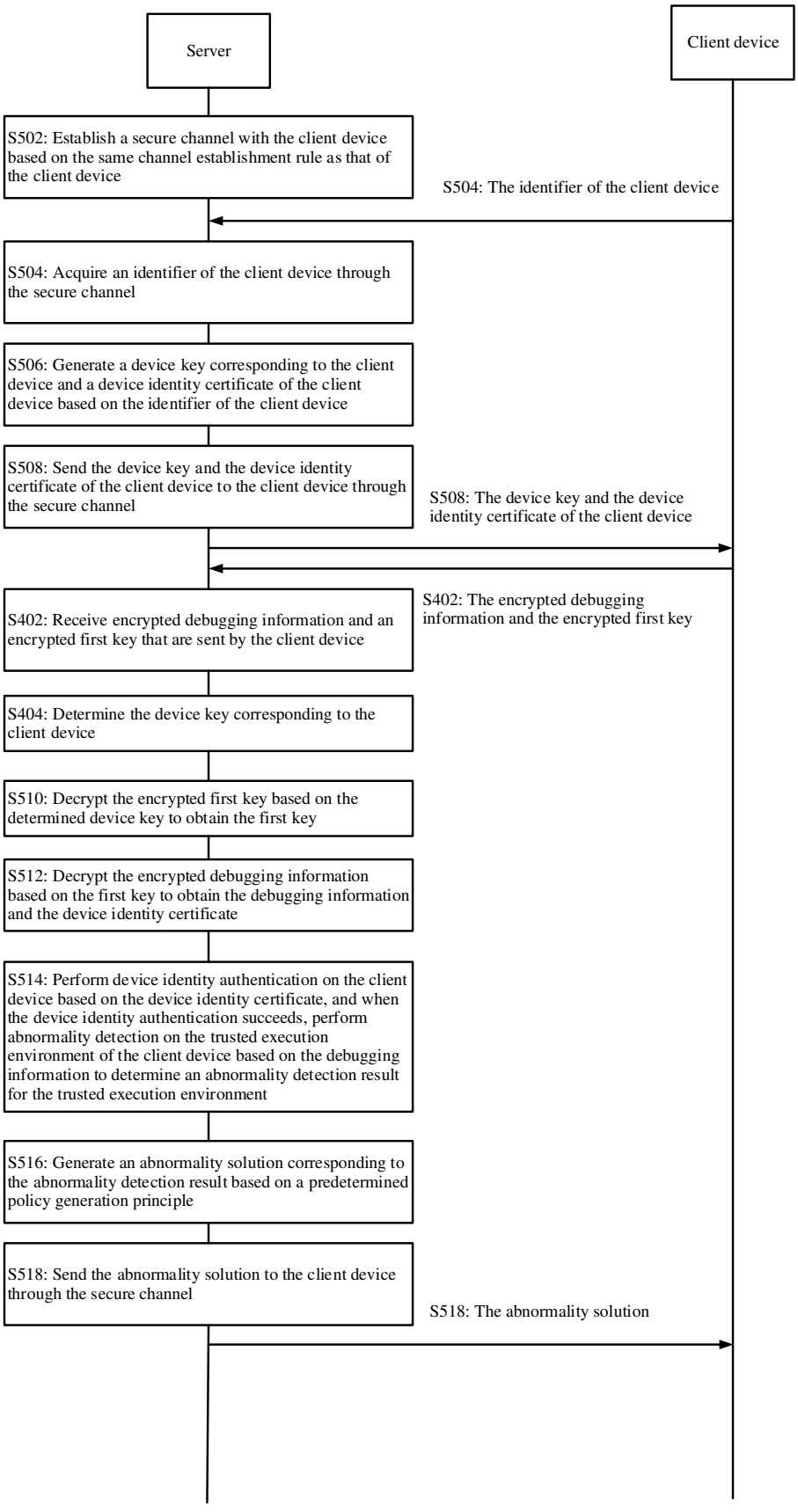

Server
Client device
S502: Establish a secure channel with the client device based on the same channel establishment rule as that of the client device
S504: The identifier of the client device
S504: Acquire an identifier of the client device through the secure channel
S506: Generate a device key corresponding to the client device and a device identity certificate of the client device based on the identifier of the client device
S508: Send the device key and the device identity certificate of the client device to the client device through the secure channel
S508: The device key and the device identity certificate of the client device
S402: Receive encrypted debugging information and an encrypted first key that are sent by the client device
S402: The encrypted debugging information and the encrypted first key
S404: Determine the device key corresponding to the client device
S510: Decrypt the encrypted first key based on the determined device key to obtain the first key
S512: Decrypt the encrypted debugging information based on the first key to obtain the debugging information and the device identity certificate
S514: Perform device identity authentication on the client device based on the device identity certificate, and when the device identity authentication succeeds, perform abnormality detection on the trusted execution environment of the client device based on the debugging information to determine an abnormality detection result for the trusted execution environment
S516: Generate an abnormality solution corresponding to the abnormality detection result based on a predetermined policy generation principle
S518: Send the abnormality solution to the client device through the secure channel
S518: The abnormality solution

FIG. 5

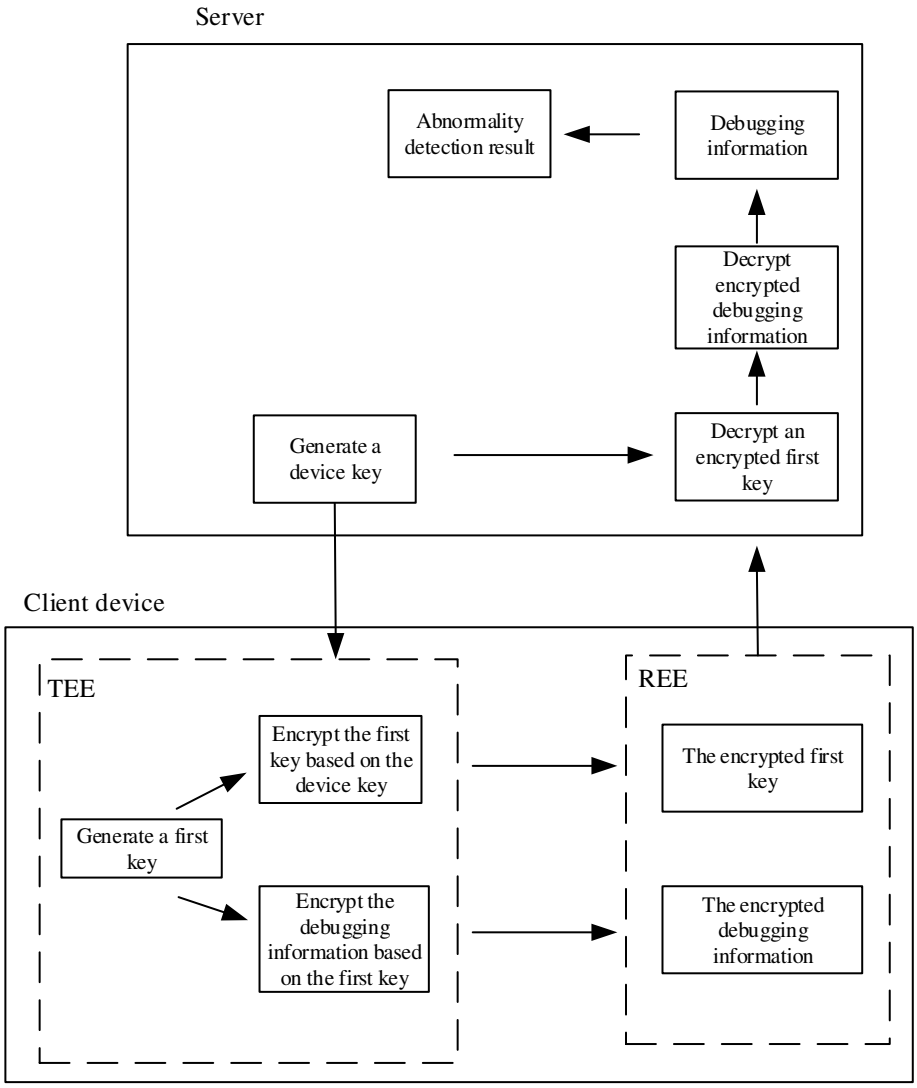

Server
Abnormality detection result
Debugging information
Decrypt encrypted debugging information
Generate a device key
Decrypt an encrypted first key
Client device
TEE
Encrypt the first key based on the device key
Generate a first key
Encrypt the debugging information based on the first key
REE
The encrypted first key
The encrypted debugging information

FIG. 6

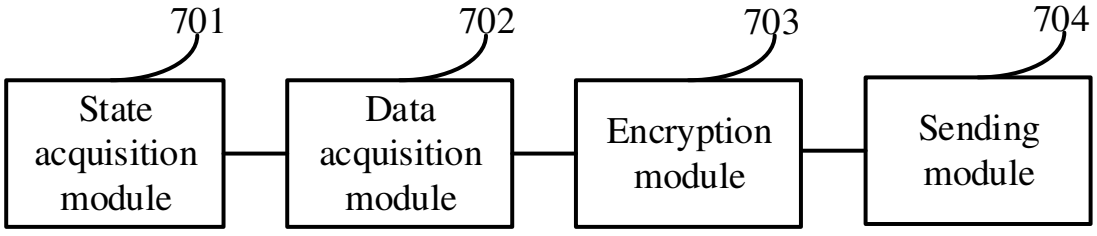

701
State acquisition module
702
Data acquisition module
703
Encryption module
704
Sending module

FIG. 7

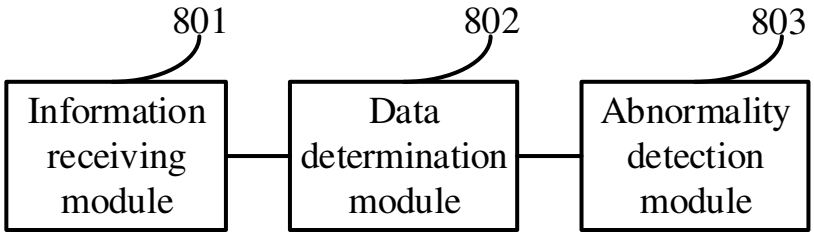

801
802
803
Information receiving module
Data determination module
Abnormality detection module

FIG. 8

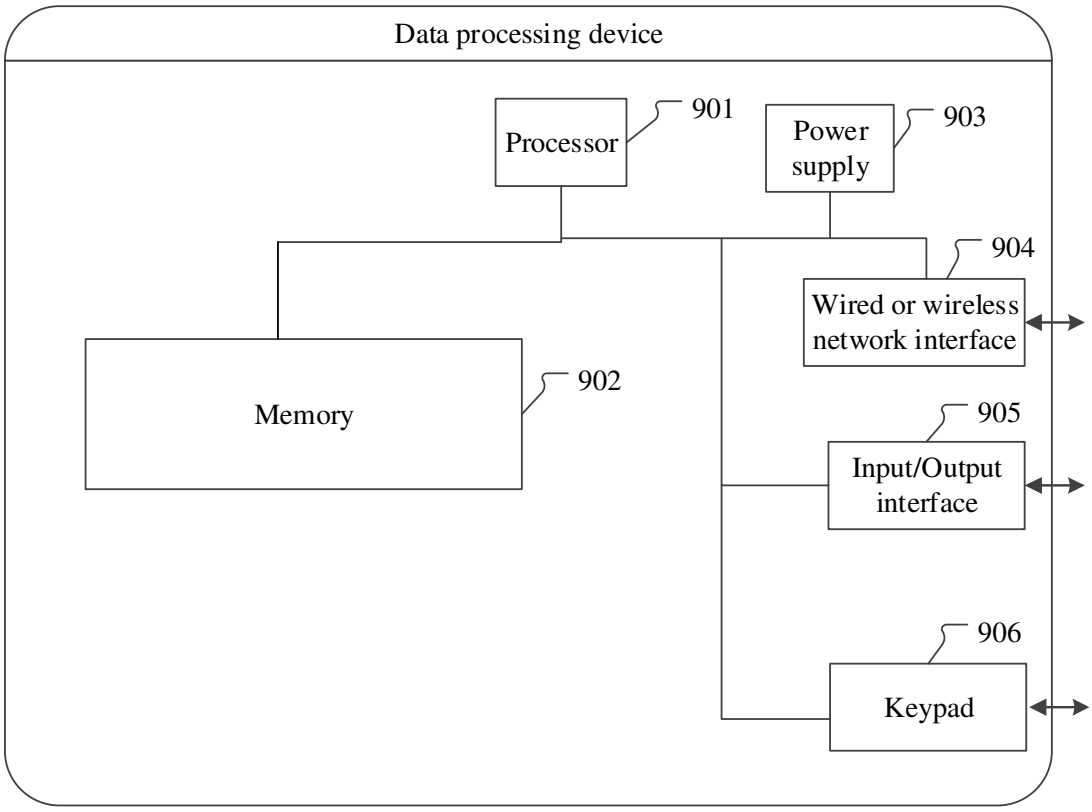

Data processing device
Processor
901
Power supply
903
904
Wired or wireless network interface
Memory
902
905
Input/Output interface
906
Keypad

FIG. 9