

SECURE COMMUNICATION METHOD AND APPARATUS

ABSTRACT

This application provides a secure communication method and apparatus. The method includes: A first device sends first information of the first device to a second device through a first message, where the first message includes one or more of a first port number, a first security parameter index SPI, a first internet protocol IP address, a first security algorithm list, and a first random number; the first device receives a second message that includes second information and that is from the second device, where the second message includes one or more of a second port number, a second SPI, a second IP address, a second security algorithm list, and a second random number; and based on the first information and/or the second information, the first device determines, in a first calculation manner, a first salt value used for uplink transmission between the first device and the second device, and/or determines, in a second calculation manner, a second salt value used for downlink transmission between the first device and the second device. This can ensure security of uplink and downlink communication between the first device and the second device.

FIG. 2