ABSTRACT

METHOD, SYSTEM, AND DEVICE FOR SECURE DATA INTERACTION, AND STORAGE MEDIUM

A method, a system and a device for secure data interaction, as well as a storage medium are provided. First, the public parameter is set at both the client and the server, and the client and the server agree on the public function. Then, the data transmission protocol is performed a predetermined number of times between the client and the server. Each time the data transmission protocol is performed, the protocol message is inputted at the client, and a commitment value of the protocol message is calculated. The protocol message and the commitment value are transmitted to the server. After the data transmission protocol, some protocol messages are randomly selected at the server. The client opens the selected protocol messages and transmit the opened selected protocol messages to the server. The server performs security verification on the opened protocol messages. Private set intersection is performed by the client and the server in a case of successful security verification, and the client acquires an intersection of respective data of the client and the server. According to the embodiments of the present disclosure, security verification is added to the data transmission protocol so as to ensure security of data of the server under malicious attacks, thereby preventing the client from acquiring the data of the server via the malicious attacks.

Figure 2