

SECURE MULTI-PARTY COMPUTATION METHOD AND APPARATUS, AND ELECTRONIC DEVICE

ABSTRACT

A secure multi-party computation method, applicable to any one computing node deployed in a distributed network. A plurality of computing nodes are deployed in the distributed network, the plurality of computing nodes jointly participate in a secure multi-party computation based on respectively held private data, and the computing node is connected to a trusted random source. The method includes: obtaining a trusted random number from the trusted random source; performing an operation on the held private data based on the obtained trusted random number to obtain an operation result; and transmitting at least the trusted random number as a computing parameter to other computing nodes participating in secure multi-party computation, so that the other computing nodes perform the secure multi-party computation based on collected computing parameters transmitted by the computing nodes participating in the secure multi-party computation.

Figure 1