

SECURE MULTI-PARTY COMPUTATION

ABSTRACT

Some embodiments of this specification provide a secure multi-party computation method and apparatus. According to the method in these embodiments, first, a TEE node cluster including K TEE nodes is joined based on a quantity N of data owners; then, a trusted execution environment is created in the TEE nodes, and a basic algorithm for secure K-party computation is loaded into the trusted execution environment; next, at least one data fragment is obtained from the trusted execution environment; and finally, secure K-party computation is performed by using the basic algorithm for secure K-party computation and the obtained data fragment.

FIG. 2