

SECURE MULTI-PARTY COMPUTATION METHODS AND APPARATUSES

ABSTRACT

Embodiments of this specification provide secure multi-party computation
5 methods and systems. According to the method, a first party performs a first mapping
operation and homomorphic encryption on first plaintext data to obtain a first converted
ciphertext in a Montgomery state, where the first mapping operation is used to convert
data from an integer ring to the Montgomery state; and then the first party sends the
first converted ciphertext to a second party. Then, the second party performs a first
10 homomorphic operation in the Montgomery state based on the first converted ciphertext
to obtain a first result ciphertext in the Montgomery state, where the first homomorphic
operation includes a modular multiplication operation. As such, computation
performance of a ciphertext computation stage can be calculated.

15

FIG. 3