

METHODS, DEVICES, AND APPARATUSES FOR DYNAMICALLY CONFIGURING SECURE MEMORY, AND STORAGE MEDIA

ABSTRACT

5 This specification discloses methods, devices, and apparatuses for dynamically configuring a secure memory, and storage media. A client application in a rich execution environment sends a registration instruction of a secure memory to a trusted application in a trusted execution environment, where the registration instruction carries a memory address. Based on the registration instruction, a trusted application calls a registration interface of an operating system in a trusted execution environment, and sends a registration request of the secure memory to a processor
10 trusted framework unit, so that the processor trusted framework unit updates, based on the registration request, an attribute of memory space corresponding to the memory address to a secure attribute. In this method, through dynamically configuring the secure memory, a security requirement in privacy protection is satisfied, and memory resource waste is reduced.

15 FIG. 1