

METHOD AND APPARATUS FOR SECURELY ENTERING TRUSTED EXECUTION ENVIRONMENT IN HYPER-THREADING SCENARIO

ABSTRACT OF THE DISCLOSURE

One or more implementations of the present specification provide a method and apparatus for securely entering a trusted execution environment in a hyper-threading scenario. The method can include: in response to that a logical processor running on a physical processor core generates a trusted execution environment entry event through an approach provided by a virtual machine monitor, labeling the logical processor with a state of expecting to enter a trusted execution environment; and in response to determining that all logical processors corresponding to the physical processor core are labeled with the state of expecting to enter a trusted execution environment, separately controlling each one of the logical processors to enter a trusted execution environment built on the physical processor core. In either a privacy blockchain scenario or other privacy protection scenarios, the solution above can allow the hyper-threading technology to be enabled to improve computing efficiency while ensuring that a trusted application exclusively occupies a physical processor core to avoid a risk of privacy leakage.

Fig. 1