

PROGRAM EXECUTION AND DATA PROOF SCHEME USING MULTIPLE KEY PAIR SIGNATURES

Abstract

Methods, systems, and apparatus, including computer programs encoded on computer storage media for program execution and data proof scheme to prove that sub-logic code that was expected to be executed within a TEE was indeed executed, and that the resulting data is trustworthy. In some implementations, each sub-logic code of a plurality of sub-logic code is registered, and stored within the TEE, and a key pair (private key, public key) corresponding to the sub-logic code is generated. The client receives and stores the public key, sends requests to the TEE with an identifier of the sub-logic that is to be executed. The sub-logic code corresponding to the identifier is executed within the TEE, which signs the result using a digital signature that is generated using the private key of the sub-logic code. The client verifies the result based on the digital signature and the public key of the sub-logic code.

FIG. 3