(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115189887 A
(43)申请公布日 2022.10.14

(21)申请号 202210753890.8

(22)申请日 2022.06.29

(71)申请人 南京大学
地址 210023 江苏省南京市栖霞区仙林大道163号

(72)发明人 李京悦 李杉杉 张贺 周鑫 汉瑞克·库得森 雅克布·斯万维克·瑙特兰得 彼得·浩兰得·哈荣 特鲁斯·巴克优德·袁得

(74)专利代理机构 南京众联专利代理有限公司 32206
专利代理师 顾进

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)
H04L 67/10(2022.01)

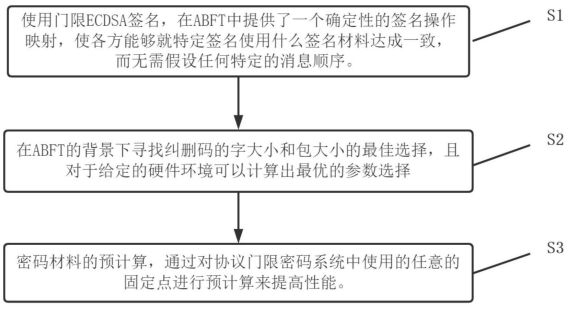
权利要求书1页 说明书8页 附图1页

(54)发明名称

一种优化的异步拜占庭容错(ABFT)共识方法

(57)摘要

本发明涉及一种优化的异步拜占庭容错(ABFT)共识方法,包括:使用门限ECDSA签名,在ABFT中提供了一个确定性的签名操作映射,使各方能够就特定签名使用什么签名材料达成一致,而无需假设任何特定的消息顺序;在ABFT的背景下寻找纠删码的字大小和包大小的最佳选择,且对于给定的硬件环境可以计算出最优的参数选择;密码材料的预计算,通过对协议门限密码系统中使用的任意的固定点进行预计算来提高性能。本发明原有的协议提供了更高的性能,显著降低的计算开销,和更高的可扩展性。此外,结果表明,ABFT在非对称网络退化的故障阈值内不受影响。



CN 115189887 A