一种不可否认协议额外增益的公平性分析

郭煦
上海电机学院电子信息学院，中国上海市，201306

摘要：由于区块链技术的发展，许多传统应用程序得以改进。其中一项服务是不可否认性，在这种服务中，通信过程中的参与者不能否认他们的参与。由于不可否认协议的脆弱性，通信中的一方当事人往往可以规避不可否认规则，获取预期信息，从而损害另一方当事人利益，造成不良影响。本文利用概率模型检测技术对该协议的公平性保证进行定量研究。利用概率时间自动机对协议建模，并验证概率计算树逻辑中指定的属性，来衡量协议的公平性。此外，提出为协议相关参数选择合适值的建议，以获取一定程度的公平，从而回答了另一个问题：对于一定程度的公平性度量ε，如何指定协议参数以确保公平性？

关键词：不可否认协议；公平性分析；概率模型检测；PRISM
https://doi.org/10.1631/FITEE.2100413