面向网络编码的无证书多重签名方法

俞惠芳，亓哲伟
西安邮电大学网络空间安全学院，中国西安市，710121

摘要：比起具有转储功能的传统路由技术，网络编码能节省网络资源且速度快。但在实际应用场景中，网络编码容易受到污染攻击和伪造攻击。本文针对这些问题提出面向网络编码的无证书广播多重签名（NC-CLBMS）方法，每个源节点用户生成对消息向量的多重签名，中间节点将接收到的数据线性组合。NC-CLBMS 是一种多源的多重签名方法，具有抗污染和防止伪造攻击的功能；此外，它还具有固定的签名长度和较高的计算效率。本文设计的 NC-CLBMS 在无人机通信网络、5G 无线网络、无线传感器网络、移动无线网络和车联网等方面具有广泛应用前景。

关键词：网络编码；无证书多重签名；线性组合；同态哈希函数
https://doi.org/10.1631/FITEE.2200271