计算机工程 2008 34 (7): 17-18,22 ISSN: 1000-3428 CN: 31-1289/TP

博士论文

无需中央机构的电子投票协议分析

李云峰，何大可

（西南交通大学信息安全与国家计算网格实验室，成都 610031）

收稿日期 修回日期 网络版发布日期 2008-3-26 接受日期

摘要 针对无需中央机构的电子投票协议——Su-协议，分析指出投票者在给出其解密选票结果的参数时，协议无法确保投票人给出的参数是正确的，攻击者可以在投票的第5步给出经过设计的参数从而可以左右系统的计票结果。据此给出针对Su-协议的3种可行的攻击：公平性攻击，选票篡改攻击和秘密性攻击。

关键词 电子投票；公平性；秘密性；准确性

分类号 TP309.2

DOI:

通讯作者:

作者个人主页: 李云峰;何大可