

论文

基于安全E-mail协议的电子选举研究

牛项须<sup>1</sup>, 崔喆<sup>2</sup>, 代翔<sup>2</sup>

- 1. 中国科学院成都计算机应用研究所
- 2. 中科院成都计算机应用研究所

摘要:

在安全邮件协议PGP中引入公正机构(CA), 设计了一个适合大规模选举的电子选举方案。该方案不仅能满足电子选举的安全要求, 而且不要求选民在固定地点投票; 此外, 新方案在一定程度上解决了电子选举中权威机构权力过大及绝对匿名性引发问题, 可以在不泄露选票内容的情况下使选举的结果具有可验证性。

关键词: 电子选举 安全E-mail协议 安全邮件协议 electronic elections secure E-mail protocol Pretty Good Privacy (PGP) protocol

Electronic elections based on secure E-mail protocol

Abstract:

By introducing the Certificate Authority (CA) into secure E-mail protocol Pretty Good Privacy (PGP), the author designed a vote scheme for large-scale electronic elections. It fulfills the security demands of electronic elections, but does not require constituencies to the settled polling booth. Moreover, the proposed scheme resolves the problems, which result from exceeding authority of authoritative organization and absolute anonymity, in electronic elections to a certain extent. And it can provide public verifiability without disclosing the vote messages.

Keywords:

收稿日期 2008-11-11 修回日期 2009-01-05 网络版发布日期 2009-06-09

DOI:

基金项目:

无

通讯作者: 牛项须

作者简介:

参考文献:

本刊中的类似文章

- 1. 郭栋梁 秦静 李鹏程. 一个基于OT协议的电子选举方案[J]. 计算机应用, 2008,28(5): 1335-1337

文章评论 (请注意: 本站实行文责自负, 请不要发表与学术无关的内容! 评论内容不代表本站观点.)

扩展功能

本文信息

- Supporting info
- PDF (674KB)
- [HTML全文]
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 引用本文
- Email Alert
- 文章反馈
- 浏览反馈信息

本文关键词相关文章

- 电子选举
- 安全E-mail协议
- 安全邮件协议
- electronic elections
- secure E-mail protocol
- Pretty Good Privacy (PGP) protocol

本文作者相关文章

- 牛项须
- 崔喆
- 代翔

PubMed

- Article by Niu,X.X
- Article by Cui,z
- Article by Dai,x

反馈人	<input type="text"/>	邮箱地址	<input type="text"/>
反馈标题	<input type="text"/>	验证码	<input type="text" value="7265"/>