计算机工程与应用 2008 44 (3): 136-138 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

基于ECDLP的高效承诺方案

赖 欣, 喻秀英, 何大可

西南交通大学 信息安全与国家网格计算实验室，成都 610031

收稿日期 修回日期 网络版发布日期 2008-1-11 接受日期

摘要 承诺方案不仅是许多密码协议中的核心部分，同时也被直接使用于远程电子投票、电子选举、电子拍卖等场合。提出一个基于椭圆曲线离散对数困难问题的承诺方案，该方案不需要在参与方之间进行信息交互，并通过执行一轮承诺阶段和公开承诺阶段就可以实现发送方对某一消息的承诺。对该方案进行详尽地分析，指出基于椭圆曲线离散对数困难问题该方案具有消息隐藏性和消息绑定性，且在执行效率和通信带宽上具有优势。

关键词 密码协议 承诺方案 椭圆曲线离散对数问题 隐藏性 绑定性

分类号

Efficient commitment scheme based on ECDLP

LAI Xin,YU Xiu-ying,HE Da-ke

Information Security and National Computing Grid Laboratory（IS&NC），Southwest Jiaotong University，Chengdu 610031，China

Abstract

Commitment scheme is not only the fundamental primitive in cryptographic protocols but also be used directly in the remote electronic voting，electronic voting，and electronic auction occasions.In this paper，based on the elliptic curve discrete logarithm problem a commitment scheme is proposed.In this scheme the information exchange among participants is not needed.Through the implementation of commitments phase and a decommitment phase a commitment of message can be achieved from the sender.A detailed security analysis of the scheme is given.Based on elliptic curve discrete logarithm problem the scheme is hiding and binding，also has the advantage in efficiency and communication bandwidth.

Key words cryptographic protocols commitment scheme ECDLP hiding property binding property

DOI:

通讯作者 赖 欣 lxswjtu@163.cm