计算机应用研究
Application Research Of Computers

基于辫群的代理盲签名方案

Proxy blind signature scheme based on braid group

中文关键词：辫群 盲签名 共轭搜索问题 量子算法 代理签名

英文关键词：braid group blind signature conjugacy search problem quantum algorithms proxy signature

基金项目：

作者	单位
李锋1， 郭艾侠2，赵秀凤3	（1. 广东工业大学， 应用数学学院， 广州 510006； 2. 华南农业大学 信息学院， 广州 510642； 3. 解放军信息工程大学 电子技术学院， 郑州 450004）

中文摘要：

由Shor等人构造的量子算法可以在多项式时间内解决传统三大难解问题而利用辫群构造的很多数学困难问题，在量子计算机条件下均无有效的解法，辫群是一种适合构造抵抗量子密码分析的计算平台。利用左右子群元素的可交换性，基于CSP问题、SCSP问题和p次方根问题的难解性，提出了一个新的代理盲签名方案，并通过方案分析验证了该方案的有效性和可行性。

英文摘要：

Three types of traditional hard problem could be resolved by Shor, Boneh and Lipton’s quantum algorithms in po-lynomial time. By the braid group constructed a lot of mathematics difficulties were not an effective solution under the conditions of the quantum computer. It seemed that braid group was a kind of considerable considerable cryptography platform in the future. This paper proposed a new proxy blind signature scheme based on conjugate search problem and the p-th root finding problem, and the exchangeable of the group operation between the elements in the left subgroup and the right subgroup of a braid group. Through program analysis shows that the new scheme is effective and feasible.