辫群上的不经意传输协议

http://www.firstlight.cn 2010-08-01

量子计算的快速发展给基于整数分解或离散对数问题的密码协议带来严重威胁。为了研究抵抗量子分析的密码协议，基于非交换的辫群提出了一个2取1不经意传输协议，并将其扩展为N取1不经意传输协议。在共轭搜索问题和多重共轭搜索问题难解的前提下协议能同时保证发送方和接收方的隐私性。

存档文本