

基于反交换拟群的消息认证码

李伟强, 徐允庆

宁波大学理学院, 宁波 315211

收稿日期 修回日期 网络版发布日期 2008-11-16 接受日期

摘要 (Q, \circ) 是一个拟群。如果对 (Q, \circ) 中任何两个不同元素 x, y 皆有 $x \circ y \neq y \circ x$, 则称 (Q, \circ) 是反交换的。本文给出一种基于反交换拟群的消息认证码, 并讨论反交换拟群的构造方法。

关键词 [拟群](#) [拉丁方](#) [消息认证码](#)

分类号 [05B15](#) [94A62](#)

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF\(299KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [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](#)

▶ [复制索引](#)

▶ [Email Alert](#)

相关信息

▶ [本刊中 包含“拟群”的 相关文章](#)

▶ 本文作者相关文章

· [李伟强](#)

· [徐允庆](#)

Abstract

Key words

DOI:

通讯作者 李伟强, 徐允庆 xuyunqing@nbu.edu.cn