应用数学学报 2008 31 (31卷5): 877-883 ISSN: 1439-8516 CN: 11-2039/O1

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

Abstract

Key words

DOI:

通讯作者 李伟强, 徐允庆 xuyunqing@nbu.edu.cn