

研究简报

## 密码体制中的正形置换的构造与记数

亢保元

中南大学铁道校区数力系,长沙,410075

收稿日期 2001-2-11 修回日期 2001-7-11 网络版发布日期 2008-7-30 接受日期

摘要

正形置换在密码体制中有重要应用,该文在前人工作的基础上,利用有限群的理论对正形置换的构造和记数问题进行了讨论,特别在正形置换的记数方面得到了有价值的结果。

关键词 [密码体制](#) [置换](#) [有限群](#)

分类号 [TN918.1](#)

## Constructions and enumerations of orthomorphic permutations in cryptosystems

Kang Baoyuan

Central Southern University of China Changsha 410075 China

Abstract

Orthomorphic permutations have good characteristic in cryptosystems. In this paper, by using of knowledge about finite group to investigate the constructions and enumerations of orthomorphic permutations, several results are obtained.

Key words [Cryptosystems](#) [Permutations](#) [Finite group](#)

DOI:

通讯作者

作者个人主页 [亢保元](#)

### 扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF\(477KB\)](#)

▶ [\[HTML全文\]\(OKB\)](#)

▶ [参考文献\[PDF\]](#)

▶ [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](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中包含“密码体制”的相关文章](#)

▶ 本文作者相关文章

• [亢保元](#)