



北京理工大学

数学与统计学院学术报告

Some results on functions with low c -differential uniformity

报告人: 查正邦 新疆大学数学与系统科学学院

时间: 2024.9.24 (周二) 14:30-15:30

地点: 线上腾讯会议: 会议号 935584989

摘要: Functions with low c -differential uniformity have optimal resistance to some types of differential cryptanalysis. In this talk, we show some classes of power functions with low c -differential uniformity over finite fields. Based on some known permutation polynomials, we present several classes of perfect c -nonlinear or almost perfect c -nonlinear polynomials by using the Akbary-Ghioca-Wang criterion.

简介: 查正邦, 新疆大学数学与系统科学学院教授, 硕士生导师。2008年博士毕业于湖南大学应用数学专业, 2012年至2014年在中科院信息工程研究所从事博士后研究工作。主要研究领域为密码函数、有限域及其应用, 在 *IEEE Transactions on Information Theory*, [Journal of Algebra](#), *Finite Fields and Their Applications*, *Designs Codes and Cryptography*, *中国科学 (数学)* 等杂志发表学术论文四十余篇, 主持国家自然科学基金4项。