通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

胡斌,金晨辉,邵增玉.密码学中3类具有特殊Walsh谱值布尔函数的关系[J].通信学报,2010,(7):104~109

密码学中3类具有特殊Walsh谱值布尔函数的关系

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
胡斌	
金晨辉	
邵增玉	

中文摘要：

从函数结构角度对Bent函数与Plateaued函数、部分Bent函数与Plateaued函数的关系进行了研究，指出了任意一个Bent函数都可拆分成2个Plateaued函数的链接，而Plateaued函数在满足一定条件下也可拆分成Bent函数的链接。给出了n-1阶Plateaued函数具有非零线性结构时与Bent函数的特殊关系，讨论了部分Bent函数可表示成2个Plateaued函数链接时的条件。研究结果进一步说明了这3类具有特殊Walsh谱值密码函数之间有着紧密的内在联系，为密码设计中使用此类函数提供了重要依据。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭