摘要

Bent 函数是非线性度和相关免疫性均最佳的布尔函数，用于流密码体制的加密系统中，以抵抗线性攻击和相关攻击方式。本报告介绍一种 bent 函数构造方式，它们具有最佳的代数次数（变量个数的一半），并且有较大的自同构群。