

摘要

APN 函数是一类重要的非线性密码函数, 是特征 2 的有限域上抵抗差分密码攻击能力最强的函数。本报告介绍了密码函数的三类安全性指标、密码函数的 EA 等价与 CCZ 等价、特征 2 有限域上 APN 函数的构造、特征 2 有限域上 APN 函数的等价性, 在此基础上, 我们证明了目前已有的 10 类多项式 APN 函数跟 APN 幂函数是 CCZ 不等价的。