摘　要

真随机数生成器的校正器是一个后处理函数，用来减少或消除物理随机数生成器的统计弱点，以提高输出序列的随机性和统计独立性。如何设计在校正能力、处理效率和非线性性质之间实现优化折中的校正器是真随机数生成器设计中的核心难题。针对这一难题，我们从密码函数的角度研究了校正器的设计，利用等距线性码构造出一大类多输出、高校正阶、高非线性度、高代数次数的非线性校正器，首次使校正器的校正阶大于其弹性阶，实现了校正器的输出维数、校正阶、非线性度、代数次数等多种参数指标之间的优化折中。