TOYOCRYPT-HR1 評価書要旨

日本語版

本稿では、CRYPTREC に応募された擬似乱数生成器 TOYOCRYPT-HR1 の安全性について評価を行ったものである。その結果、周期、線形複雑度、および 0/1 等頻度性に関する提案者の解析は妥当なものであることが検証された。また、統計的な性質として、4 ビットの等頻度性、連、自己相関性に関する数値的な検証を行ったが、特に問題は見つからなかった。

英語版

In this report, the security of the pseudorandom number generator TOYOCRYPT-HR1 submitted for CRYPTREC is discussed. The desiner's self-evaluation about the theoritical analysis including period, linear complexity, and 0/1 frequency are confirmed. In addition, other statistical properties, 4-bit freqency, and auto-correlation are numerically examined. As a result, any statistical flaw is not found.