令和６（２０２４）年度　卒業研究報告書概要

課程，学籍番号，氏名	課程：電気・電子情報　工学課程，　学籍番号：B233286，氏名：TSOLMON ARIUNAA
工学分野名：情報通信システム	指導教員名：市川 周一

題　　目：

Staggered LFSR の回路設計と評価

（英　Staggered LFSR Circuit: Design and Evaluation　）

Abstract

The Pseudo-Random Number Generator (PRNG) generates sequences based on specific computational methods or algorithms, and thus its values are predictable from the output history and internal states. The Linear Feedback Shift Register (LFSR) is widely used as a PRNG due to its simplicity, and it has been implemented in both software and hardware.

LFSRs generate one bit per cycle, which might be insufficient for high-throughput applications. Parallelizing multiple LFSRs, generation speed can be enhanced. However, this approach introduces challenges, such as correlation between LFSRs and increased resource consumption.

To improve generation speed without compromising quality, Gu and Zhang (2009) introduced the Leap-ahead LFSR, which increases random bit generation rates by applying feedback polynomials multiple times per cycle.

Subsequently, Ichikawa (2023) proposed the Staggered LFSR, a new PRNG that samples LFSR values at variable cycles. The SLFSR employs two LFSRs: a main n-bit LFSR and a fluctuation control f-bit LFSR, with variability introduced by parameter m.

This study designs and evaluates SLFSRs in Verilog HDL, synthesized on Xilinx Vivado. Several designs were developed to assess performance, including a 64-bit LFSR, and a 32-bit SLFSR with a fluctuation width of 16 bits. A 16-bit fluctuation showed resource differences: a 32-bit SLFSR required 55 LUTs and 120 FFs, while a 64-bit SLFSR used 106 LUTs and 224 FFs.

概　　要

疑似乱数生成器（PRNG）は、アルゴリズムによって疑似乱数列を生成するため、出力履歴や内部状態から将来の値を予測可能である。線形帰還シフトレジスタ（LFSR）は PRNG の一例であり、その単純さからソフトウェアおよびハードウェアで広く採用されている。

LFSR は 1 サイクルに 1 ビットしか生成できず、高スループットを必要とするアプリケーションでは生成速度が不足する場合がある。この問題を解決するために、複数の LFSR を並列化することで生成速度を向上させる手法が考えられる。ただし、このアプローチは LFSR 間の相関問題や資源消費の増加といった課題を伴う。これを解決するために、Gu と Zhang（2009）は Leap-ahead LFSR を提案し、フィードバック多項式を 1 サイクル内で複数回適用することで乱数生成速度を向上させた。

その後、市川（2023）は、LFSR の値を可変周期でサンプリングする新しい PRNG「Staggered LFSR」を提案した。

本研究では、Staggered LFSR アーキテクチャに基づく PRNG の設計と評価を目的とする。設計には Verilog HDL を使用して、Xilinx Vivado 上で論理合成を行った。評価では、64 ビット LFSR、および揺らぎ幅 16 ビットの 32 ビット Staggered LFSR を含む複数の設計を比較した。

発表する際の課程を記入　　電気・電子情報工学　課程　　発表番号　101