令和５（２０２３）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： B223284、 氏名： NURUL HIDAYAH BINTI AMRAN
工学分野名：情報通信システムコース	指導教員名：市川　周一

題　　目：FPGA Implementation of the Staggered LFSR

Abstract

Random numbers are widely used in various applications. In most cases, a pseudo-random number generator (PRNG) is used since true random number generators are slow and they essentially require the hardware implementation.

Gu and Zhang (2009) proposed a Leap-ahead Linear Feedback Shift Register (LFSR), which is a kind of PRNGs where the feedback polynomial is applied multiple times to derive a larger generation rate. Even though a Leap-ahead LFSR applies the feedback polynomial a fixed time, the quality of randomness might be improved by varying the times of application of feedback polynomial.

This study examines the hardware implementations of the Staggered LFSR.

概　　要

乱数には、真性乱数（TRN；True Random Number）と疑似乱数（PRN；Pseudo Random Number）がある。TRN を生成するための専用ハードウェアは真性乱数生成器（TRNG）と呼ばれる。高性能な TRNG においては実装コストが問題になる。一方、PRN を生成する計算方式やアルゴリズムを疑似乱数生成器（PRNG）と呼ぶ。出力履歴と内部状態から値が予測することができる。

線形帰還シフトレジスタ（LFSR）は疑似乱数生成器（PRNG）として普及しており、ソフトウェアで利用されるだけでなく、その単純さからハードウェア実装でも広く利用されている。LFSR は１サイクルに１つのビットを出力するが、多くの乱数を必要とする場合は生成速度が不足する。そこで、生成速度を上げるために、複数の LFSR を用いて並列に乱数を生成することが考えられる。しかし、LFSR 間の相関が新たな問題となり、LFSR の並列化にはより多くの資源量が必要となる。

Gu と Zhang(2009)は Leap-ahead LFSR アーキテクチャを提案し、乱数ビットの生成速度を向上させた。正岡・市川・藤枝(2021)は、128 ビットの LFSR をソフトプロセッサに実装して URNG を構成し、乱数品質を検証した.。鴨狩と市川(2023)は、LFSR の仕様や実装方法を詳細に検討した。市川(2023)は、LFSR の値を可変周期でサンプリングする Staggered LFSR と呼ばれる新しい PRNG を提案した。

本研究の目的は、Xilinx Virtex UltraScale+ FPGA 上で Staggered LFSR に基づく PRNG 論理回路の設計を構築することである。まず、揺らぎの値を変えた Staggered LFSR を設計した。検証プロセスは、設計され C 言語で記述された Staggered LFSR を使用して乱数を生成し、生成された乱数列を乱数テストに通して乱数の品質を検証するというものである。乱数テストに使用したテスト・スイートは DIEHARD である。テスト結果の合格基準は正岡らの先行研究に準拠して決定した。

システムのコストや性能を評価するためには，実装の評価が必要である。そこで、64-bit LFSRと44-bit Leap-Ahead LFSRと64-bit Leap-Ahead LFSRと f＝16 bit の32-bit Staggered LFSR を設計し、結果を評価した。VivadoとHLSで64-bit Leap Ahead LFSRと f＝16 bit の32-bit Staggered LFSR のLUTとFFのUtilizationはほぼ同じだが、最終タイミングはf＝16 bit の32-bit Staggered LFSR の方が大きい。

発表する際の課程を記入　　電気・電子情報工　課程　　発表番号　９８

（学籍が他課程所属の学生も発表する課程を記入すること）