2023 年度 卒業研究発表 梗概

電気学科

学籍番号 氏 名	V20160 八代 航輔	指導教員	藤枝 直輝
題 目	FPGA を用いた TRNG の可視化システムの改良		

1. はじめに

TRNG（真性乱数生成器）とは，物理的現象を元に規則性のないビット列を出力する回路である．対して，アルゴリズムを元に規則性のないビット列を出力する回路を PRNG（疑似乱数生成器）と呼ぶ．TRNG は，PRNG と異なり原理的に出力を予測することが不可能であるため，セキュリティ用途で用いられる．TRNG からの出力が十分な不確定性を持たないとき出力に偏りが生じる可能性がある．若林[1]は，このとき起こりうる問題点を可視化するシステムを作成した．このシステムでは，TRNG からの出力をもとに定めた座標に繰り返し点を打つ様子を，映像で出力する．

本研究では，若林の先行研究の可視化システムの問題点を改善することが目的である．特に，先行研究の可視化システムに文字表示の機能を追加する．また，打った点の統計情報を画面上に数値で表示するプログラムを作成する．これにより，可視化された画面を見た人が，数値的判断を行えるようにする．

2. 研究背景

本研究では，TERO という回路に基づいた TRNG を扱う．RS ラッチを禁止状態から保持状態へと一気に切り替えると，回路はしばらくの間発振する．その発振の回数が偶数か奇数かを数えて，乱数を取り出すのが，TERO 型 TRNG の動作原理である．今回システムに組み込んでいるのは，TERO の改良版の TC-TERO[7]である．

先行研究の可視化システムは（1）真性乱数生成器の評価システムと（2）グラフィックパターン生成システムをベースに設計されている．(1)は TC-TERO を用いて乱数を生成し，ファイルに保存するシステムである．(2)はグラフィックパターン生成回路から出力された信号を，HDMI 信号に変換し，出力するシステムである．システムは PYNQ というプラットフォーム上に実装されている．PYNQ は，FPGA を搭載した AMD のシステムオンチップのためのプラットフォームである．これにより，FPGA を Python のプログラムで制御できる．

先行研究のシステムには，2 つの問題点がある．1 つは，出力される映像が左右に数ピクセルずれたり，異なる色で表示される不具合があることである．もう 1 つは，出力結果を数値的に比較すると方法を持たないことである．これら 2 つの問題点についてアプローチする．

3. 不具合の原因調査

本章では ILA 機能を用いて，不具合の調査を行う,AMD の FPGA には，FPGA 内部にロジックアナライザの機能を搭載することが可能である．グラフィックパターン生成回路の周辺にILAを挿入し，関連のありそうな信号確認のキャプチャを行った．この調査によって，Jupyter Notebook 上でプログラムを書き換えた際に不具合が生じる場合があるということが確認出来た．しかし，再現性があることは判明したが，その条件には至らなかった．

4. 動作結果の数値化

数値的な比較を行うために,円周率の推定値を表示する機能を追加する.ソフトウェア上でフレームバッファに文字のパターンを書き込むためのクラスを追加する.ハードウェア上で打った点の数を出力できるように,グラフィックパターン生成回路を修正する.このシステムによって,文字を表示すること,円周率と推定値をそれぞれ表示することが可能になった.

5. おわりに

本研究では,乱数の挙動を可視化するシステムの改良として，不具合の原因調査と，文字表示の機能追加を行った．本研究で特定出来なかった不具合の原因を究明し，取り除くことが今後の課題である．

参考文献

［1］ 若林岳流, FPGA を用いた TRNG の可視化システムの構築，卒業論文，愛知工業大学, 2023.

［2］ N. Fujieda, On the feasibility of TERO-based true random number generator on Xilinx FPGAs, 30th International Conference on Field-Programmable Logic and Applications, pp. 103-108, 2020.