2022 年度 卒業研究発表 梗概

電気学科

学籍番号 氏　名	V19171　若林 岳琉	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構築		

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) とよぶ．TRNG は，PRNG と異なり原理的に次の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よく用いられる．TRNG が偏りのないビット列を出力しているかどうかは，乱数検定によって調べられる．しかし，乱数検定によっては TRNG の合否が出てくるのみで，実際に偏りやパターンのある乱数が表示された場合に生じる問題を，直感的に理解することが難しい．そこで，出力された乱数を用いて映像により可視化するシステムを構築することで，より直感的に TRNG に生じる問題を感じ取れるようになる．

本研究は，FPGA を用いた TRNG の可視化システムを構築することを目標とする．動作環境として，プロセッサと FPGA がワンチップ化された Zynq とよばれるシステムオンチップを搭載した評価ボードである，PYNQ-Z1 を用いる．映像生成のための回路は，C 言語のプログラムを元に Vitis HLS を用いて高位合成を行い作成する．可視化の題材としてモンテカルロ法の円周率近似を用いる．システムの論理合成および配置配線は，Vivado 2021.2 を用いる．

2　システムの設計

本研究で構築したシステムは，(i) 真性乱数生成器の評価システム [1] と，(ii) グラフィックパターン生成システム [2] をベースに設計を行う．(i) は遷移効果リングオシレータ (TERO) と呼ばれる回路からなる TRNG を用いた，乱数を生成し保存するシステムである．乱数の挙動は，ソフトウェアから異なるパラメータを与えることにより，変更可能である．(ii) 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．

構築したシステムは，2 つのシステムから必要な回路を取り出して結合し，グラフィックパターン生成回路を変更したものである．すなわち，(i) のシステムからは TRNG を，(ii) のシステムからは HDMI 信号への変換・出力部分を取り出す．構築したグラフィックパターン表示回路は，TRNG の出力を入力とし，それを 2 つに分け X 座標 Y 座標とし，原点からの距離が一定値以下の場合は赤色，そうでない場合は青色で描画する回路である．このシステムが正常に動作する場合，乱数に偏りがない場合は映像全体がうっすら赤色と青色に染まると予測され，偏りがある場合は映像に不自然な縞模様が観測されると予想される．

3　評価

このシステムの評価に，動作検証とハードウェア量の測定を行う．動作検証は，PYNQ-Z1 を用いて FPGA 上の回路を動作させる Python スクリプトを作成し，実行することにより行う．TRNG に与えるパラメータは，5 秒ごとに変更する．ハードウェア量の測定は Vivado での論理合成および配置配線終了後に，ハードウェア量に関するレポートを確認することにより行う．

PYNQ-Z1 ボード上でスクリプトを実行したところ，HDMI 出力からモニターに映像が出力され，5 秒おきに色の濃さや縞模様の有無などが切り替わる様子が確認できた．このシステムに使用した回路素子は，LUT が 4723 個，レジスタが 6870 個であった．そのうち，本研究で新たに構築したグラフィックパターン表示回路は LUT を 317 個，レジスタを 375 個を使用した．

4　おわりに

本研究では，FPGA を用いた TRNG の可視化システムの構築に成功した．本研究のシステムは，映像信号のみの出力となっているので，これに加えて計算により求めた円周率を表示するといった，よりわかりやすい可視化の実現が今後の課題である．

参考文献

[1] N. Fujieda, On the feasibility of TERO-based true random number generator on Xilinx FPGAs, 30th FPL, pp. 103-108, 2020.

[2] 中村 光希，PYNQ プラットフォームを用いた可視化システムのプロトタイプ，卒業論文，愛知工業大学，2022.