2020 年度 卒業研究発表 梗概

電気学科

学籍番号 氏 名	V16097 芳賀拓途	指導教員	藤枝直輝
題 目	真性乱数生成器の環境依存性の評価システム		

1 はじめに

情報通信のセキュリティ、たとえば暗号キーの作成において真性乱数が重要視されている。真性乱数とは、物理現象を利用した不確定性のあるビット列である。真性乱数を生成する回路のことを真性乱数生成器と呼ぶ。ディジタルシステムの実装には FPGA (Field Programmable Gate Array) がよく使われている。FPGA とは、製造した後でも内部の論理を変更できる PLD (Programmable Logic Device) の一種である

本研究は、既存の FPGA 向けの TRNG である TC-TERO [2]をもとに、その挙動の温度依存性を評価するシステムを構築することを目的として行う。

2 関連研究

FPGA 上に実装できる TRNG がいくつか提案されている。そうした TRNG の多くはリングオシレータを基礎とする [1]。遷移効果リングオシレータ (TERO) は、SR ラッチの 2 つの入力に同一の信号を接続した回路と等価である。回路がうまく調整されていると、このとき出力はしばらく振動する。その回数をカウンタで数え、その偶奇を乱数として用いる。TC-TERO [2] では、この回路の調整をパラメータによって行える。

3 測定手法の概要

TC-TERO では、カウンタの値が大きすぎても小さすぎても、うまく乱数を生成できない。そのため適切なパラメータを見つける必要がある。適切なパラメータは、先行研究 [2] の手順に従って求める。先行研究の手法で得た値をカウンタの平均値として取得するスクリプトを本研究では Python スクリプトとして作成し、Jupyter Notebook とよばれる環境で実行した。同時に温度の測定をするため Arty というボードに搭載されている XADC で温度を測定した。

4 測定結果

本研究では、カウンタの平均値を取得するスクリプトと温度を測定するスクリプトを同時に動作させることで、これらの同時測定に成功した。しかし、温度変化の幅が小さく、TC-TERO の挙動に温度依存性があるかどうかを調べることはできなかった。ダミー負荷を加えた場合などの評価と温度測定の自動化などが今後の課題となっている。

参考文献

[1] O. Petura, U. Mureddu, N. Bochard, V. Fischer, and L. Bossuet, A survey of AIS-20/31 compliant TRNG cores suitable for FPGA devices, 26th International Conference on Field Programmable Logic and Applications, pp. 1–10, 2016.

[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.