2021 年度 卒業研究発表 梗概

電気学科

学籍番号 氏　名	V16069　鈴木 涼太	指導教員	藤枝 直輝
題　目	TC-TERO 型真性乱数生成器のためのパラメータ選出手法		

1　はじめに

暗号キーなどの情報通信のセキュリティでは真性乱数が重要視されている。真性乱数は、物理現象が持つ予測不可能性を利用し生成される乱数であり、乱数としての安全性が高い。この真性乱数を生成する回路を真性乱数生成器 (TRNG) 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。FPGA の論理素子を使って TRNG が構成できれば、実用上のメリットが大きい。本研究では、既存の FPGA 向けの TRNG である TC-TERO を用いる。TC-TERO [1] はパラメータにより構成を変更できるが、適切なパラメータを見つける方法はこれまで検討されてなかった。本研究の目的は、自動的に質の良い乱数が得られるパラメータを見つけるシステムを構築することである。

2　関連研究

FPGA 上に TRNG を実装するにあたり、リングオシレータと呼ばれる回路が基礎となる場合が多い [2]。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ときの回路と等価な回路である。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発振する。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 [1] では、この回路の調整をパラメータによって行える。先行研究 [1] で平均の発振回数が 100 付近の場合、質の良い乱数が生成されやすいことわかっている。

3　選出方法の概要

予備実験として、TC-TERO のパラメータのうち 2^{19} 個に対してそれぞれ 4,096 回の発振を行い、発振回数の平均を求めて、パラメータ番号と発振回数の関係を取得した。これをグラフにまとめることで、類似するパラメータでは発振回数が近くなるという特徴が確認された。

この特徴に注目して、選出方法を以下のように定める。あるパラメータで発振回数を測定する。平均発振回数がしきい値未満の場合が一定回数続いた場合、次のパラメータをランダムに選出する。そうでなければ、次のパラメータは今のパラメータに 1 を加えた値とする。この手順を、平均発振回数が 100 前後のパラメータが見つかるまで繰り返す。

4　評価

評価はシミュレーションと実機のそれぞれで行った。シミュレーションでは、パラメータに対する発振回数は、予備実験の結果を参照する。プログラムは C 言語で作成した。実機実験では、実際に TC-TERO で発振を行い、発振回数を求める。プログラムは Python で作成し、Jupyter Notebook と呼ばれる環境で実行した。

シミュレーションによる実験の結果，発振回数のしきい値を 30 に設定し，そのしきい値よりも発振回数が小さい場合は必ずランダムにパラメータを変更する方法が最も適していることがわかった．このとき，常にランダムにパラメータを変更する場合よりもより早く適切なパラメータを見つけることができた。同様の結果は実機実験でも得られた。

5　おわりに

本研究では、提案した選出手法により一部のケースでランダムにパラメータを変更するより早く適切なパラメータを見つけることができた。特にある発振回数がある値を下回ったらすぐにランダムにパラメータを変更した方がより速く適切なパラメータを見つけることができた。

より早く適切なパラメータを見つける方法を提案することや、パラメータと乱数の質との関係を定量的に評価することが、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] 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 FPL , pp. 1–10, 2016.