2024 年度 卒業研究発表 概要

電気学科

学籍番号 氏　名	V21061　苅谷　祥	指導教員	藤枝　直輝
題　目	FPGA 上の TERO 型真性乱数生成器の温度依存性の調査		

1　はじめに

現代社会では情報セキュリティの重要性が高まっており、暗号技術の基盤となる乱数生成器（RNG）が重要視されている。特に、物理現象を利用して乱数を生成する真性乱数生成器（TRNG）は、擬似乱数生成器（PRNG）よりも安全性が高い。TERO 型 TRNG を拡張し、パラメータ設定の柔軟性を加えたものが TC-TERO [1] である。先行研究 [2, 3] では、 TC-TERO の適切なパラメータとは何か、高速に見つけるにはどうすればいいかも研究されている。いずれの研究も、動作中の外部環境の変化により適切なパラメータが変動する可能性については言及していない。

本研究は、 TC-TERO 型 TRNG において、温度変化が乱数生成に与える影響を明らかにすることを目的とする。

2　TERO 型 TRNG

TERO 型 TRNG は、RS ラッチの一時的な発振現象を利用して乱数を生成する方式である。TERO 型 TRNG で重要なことは、発振回数のランダム性が乱数の品質を決定するということである。 TC-TERO は、TERO 型 TRNG を拡張し、パラメータにより発振回数を調整可能にしたものである。

3　評価システム

乱数の生成には、 PYNQ-Z1 ボードを使用する。FPGA 部分（PL: Programmable Logic）に TC-TERO 型 TRNG を実装し、プロセッサ部分を用いて、ソフトウェア制御やデータ収集を行う。ソフトウェアでは、乱数取得に必要な初期化処理行い、カスタム IP を起動して乱数の生成を開始する。乱数の生成が終了したら、TRNG を停止し、乱数出力ファイルを閉じるなどの後処理を行う。最後に、 TRNG に保存された統計情報を読みだして、ファイルに記録する。このプログラムを一定時間おきに繰り返し実行するように、プログラムを修正する。また、発振回数の統計情報をヒートマップで可視化できるようにし、 imshow 関数に 2 次元配列を与え、各要素の値が色と対応づけられて表示されるようにする。

4　評価

測定は以下の手順で行う。恒温器に PYNQ-Z1 ボードを収納する。恒温器の設定温度を初期温度に設定し、庫内の温度が初期温度になるまで待機する。パソコンから PYNQ-Z1 ボードへ、乱数生成のプログラムの実行を指示する。設定温度の初期温度は 10 ℃、最高温度は 60 ℃とする。乱数生成のプログラムの実行開始後、5 分おきに今の設定温度よりも 10 ℃高い温度に設定する。乱数生成は、5 秒ごとに行う。TC-TERO 型 TRNG のパラメータは 3 種類に設定する。

評価の結果、温度が 10 ℃から 60 ℃の間では温度依存性はあまり確認されず、乱数の質は大きく変化しないことが分かった。

5　おわりに

本研究では、TC-TERO 型 TRNG が動作中の環境変化によって受ける影響を調査するため、温度変化が乱数生成に与える影響を調査した。その結果、温度が 10 ℃から 60 ℃の間では温度依存性はあまり確認されず、乱数の質はそう変化しないことが分かった。

今後の課題として、今回の結論が別のボードやパラメータを使った場合でも成り立つのかどうか、より詳細に調査することが挙げられる。また、動作電圧などの他の動作環境も考慮して調査する必要がある。

参考文献

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

[2] 堀隼大, TC-TERO の乱数値評価, 卒業論文, 愛知工業大学, 2023.

[3] 小河優治, TC-TERO による乱数生成の改善案, 卒業論文, 愛知工業大学, 2024.