2023 年度 卒業研究発表 梗概

電気学科

学籍番号 氏　名	V20040　小河　優治	指導教員	藤枝 直輝
題　目	TC-TERO による乱数生成の改善案		

1　はじめに

現代社会において，真性乱数生成器（True Random Number Generator, TRNG）はセキュリティ用途で重要な役割を果たしている．FPGA を使ったシステム上では，FPGA 上の回路として TRNG を実装することにより，別途 TRNG のハードウェアを外付けする場合と比べて，部品点数が減ることによるコストの削減が期待できる．FPGA 上で実装できる TRNG の一種に TERO (Transition Effect Ring Oscillator) 型 TRNG があり，そのうちパラメータにより回路の設定を変更できるものに，TC-TERO [1] がある．TC-TERO には，パラメータ値によっては偏りのある乱数を生成するといった課題が存在する．

本研究では，TC-TERO において，質の良い乱数が生成されるパラメータを見つけるより良い方法を提案する．偏りのある乱数が発生するパラメータでの挙動の傾向を分析し，複雑な乱数検定を行うことなしに，適切なパラメータを先行研究 [2] よりも確実に見つける方法を提案する．

2　TC-TERO

TERO 型 TRNG は SR ラッチと等価な回路である．SR ラッチには，禁止状態から一気に保持状態に移行させた場合，一時的に発振が発生するという特性があり，発振が安定するまでにかかる回数には不確実性がある．TERO 型 TRNG はこの不確実性を利用している．TC-TERO の適切なパラメータを見つける方法の先行研究において，発振回数の平均値が 50〜150 の範囲にある場合，約 8 割のパラメータが検定に合格することが確認されている．

3　提案手法

まずは TC-TERO 型の乱数生成器を使用し，発振回数の分布と乱数検定の結果を収集する．乱数の生成は，Digilent 社の PYNQ-Z1 ボード上に実装された，先行研究 [2] と同じシステムを用いて行う．10,000 個のパラメータのそれぞれで，乱数を生成しながら，SR ラッチの発振回数の分布の収集と乱数検定回路の合否の判定を同時に行う．測定の結果，10,000 個のパラメータのうち乱数検定に合格したものは 569 個であった．先行研究の方法で選別を行った場合，672 個のパラメータが選択され，そのうち合格したものは 382 個（56.8%）であった．

得られた発振回数の分布をプロットしたところ，先行研究の方法で選別されかつ乱数検定に合格しなかったパラメータ値のグラフは明らかに歪んでいることがわかった．これを踏まえ，先行研究の条件に加えて，発振回数の分布の二階微分の正負が入れ替わった回数が閾値 t 以下であるという条件で，パラメータを選別する方法を提案する．

提案手法を適用し，t を 10〜100 の範囲で変化させてパラメータの選別を行った．その結果，t が 10 のときに，268 個のパラメータが選択され，そのうち乱数検定に合格したものは 214 個（79.9%）であった．

4　まとめ

本研究では，TC-TERO 乱数生成において，質の良い乱数が生成されるパラメータを，複雑な乱数検定を行うことなしに見つける手法の改善案を提案した．その結果，発振回数の二階微分の正負が入れ替わった回数という条件を加えることにより，合格するパラメータの割合は 56.8% から 79.9% に上昇した．

今後の課題として，今回の分析結果がメモリ数を減らして乱数生成した場合にも適用されるかどうかの確認や，偏りのない乱数が生成されるパラメータをさらに絞り込む方法の確立が挙げられる．

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.