2022 年度 卒業研究発表 梗概

電気学科

学籍番号 氏　名	V17123　堀　隼大	指導教員	藤枝 直輝
題　目	TC-TERO の乱数値評価		

1　序論

情報通信のセキュリティでは乱数が多く用いられている。乱数には擬似乱数と真性乱数が存在し、暗号キーなどの生成に疑似乱数を使用すると、次の値が予測できてしまう危険性がある。そのため、原理的に次の値が予測不可能な真性乱数が用いられる。ディジタルシステムの実装では実装後でも内部の論理の書き換えが可能な FPGA (Field Programmable Gate Array) がよく使われている。FPGA に真性乱数生成器 (TRNG) を実装することにより部品の数が減るなどのメリットがある。本論文では FPGA 上で論理素子を用いて遷移効果リングオシレータ (TERO) を用いた TRNG を作成し、先行研究 [1] では明らかになっていなかった TERO における発振回数と乱数の質の関係を調査する。

2　TC-TERO

FPGA 上に実装できる TRNG には複数の種類が存在する。今回は使用する論理素子が少なく済む TERO 型を用いる。TERO は SR ラッチと等価な回路であり，SR ラッチは禁止状態から保持状態に遷移させたとき発振する．TERO 型 TRNG はこの発振の回数を記録するという方法で乱数を生成している。この発振がどのように起きるかは回路の配置や FPGA の個体によって異なる。今回用いる TC-TERO とよばれる回路では回路の調整をパラメータで行う事が出来る。先行研究では発振回数が 100 付近の場合、質のいい乱数が生成されやすいとされている。

本研究では、出力された乱数に規則性があるかどうかを、count the ones とよばれるアルゴリズムを用いて判定する。このアルゴリズムの出力が、平均 2500 、標準偏差 $\sqrt{5000}$ の正規分布に従う値である場合、出力された乱数に規則性が無いものとされている [2]。

3　乱数評価

本研究ではまず、 TC-TERO のパラメータごとに一定数の乱数生成を行いながら、発振回数の分布と乱数検定の結果を収集する。実験には PYNQ-Z1 ボードを用いて、FPGA 上に乱数生成回路 [1] 、 DMA 回路、乱数検定回路 [2] を搭載する。Python で作成したプログラムにより、プロセッサで発振回数の集計を行う。実験の結果、発振回数の平均が 50 でも検定に成功する場合もあれば、発振回数の平均が 110 で検定に失敗した場合もあった。すなわち、発振回数の平均が 100 付近であるとよいという先行研究の基準は、あくまで目安であることがわかった。そのため、発振回数によってどれくらい偏りのない乱数が得られやすいか、定量的な評価が必要である。

収集したデータを集計して、 TC-TERO のパラメータを発振回数の平均値と乱数検定の成否の 2 種類の判断基準で分類する。発振回数の平均値は、 Python のプログラムにより計算する。乱数検定の成否は、先行研究 [2] をもとに、検定回路の出力が 2200 以上 2800 未満かどうかで判断する。評価の結果、発振回数の平均値が 50 〜 150 の範囲にある場合は、 80% 以上のパラメータが検定に合格し、合格するパラメータの割合はそう大きく変化しないことがわかった。

4　結論

本研究では、 TC-TERO 型の TRNG を用いて、発振回数と乱数の質の関係を定量的に評価した。その結果、発振回数の平均が 100 付近であるとよいとされてきたことはあくまで目安にすぎず、発振回数の平均が 50 〜 150 の範囲にある場合、乱数の質はそう大きく変化しないことがわかった。

今後の課題として、発振回数の平均や乱数園庭の結果以外に乱数の質を調べる方法がないか調べ、失敗している 20% のパラメータをすぐに見分けられる方法を探すことが挙げられる。

参考文献

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

[2] R. Oya, N. Fujieda, S. Ichikawa, An HLS implementation of on-the-fly randomness test for TRNGs, 10th CANDAR, pp. 151–157, 2022.