2022 年度 卒業研究発表 梗概

電気学科

学籍番号 氏　名	V19069　小谷 孟志	指導教員	藤枝 直輝
題　目	MMCM を用いた真性乱数生成器の PYNQ ボードにおける試作		

1　はじめに

乱数は現代のセキュリティ技術において重要な役割がある。乱数には一定の計算式と内部の状態をもとに作られる疑似乱数と、物理現象の観測結果をもとに作られる真性乱数がある。内部状態が分かると予測が可能になる疑似乱数に比べ、物理現象をもとにしている真性乱数は予測ができないという利点がある。

近年、組み込みシステムに FPGA (Field-Programmable Gate Array) が採用されることが増えており、真性乱数生成器 (TRNG) を FPGA 内に実装するという需要がある。藤枝と高島は Xilinx 社の FPGA に搭載される MMCM (Mixed-Mode Clock Manager) というクロッキング素子を用いた TRNG を提案した [1]。また、辻は MMCM のドライバプログラムの改良を提案した [2]。これによって整数のみ使用可能だったパラメータに 1/8 刻みの分数値が与えられるようになり、MMCM から出力される周波数を細かく調整できるようになった。

しかし、先行研究でのシステム構成には複雑で扱いづらく、データ収集に手間がかかるという問題があった。本研究ではこれらの問題を解決した、移植性の高い FPGA 向け TRNG の試作を行うことを目的とする。

2　提案システムの設計

先行研究の TRNG からの変更点は 3 つある。第 1 に、使用するボードを Arty A7 から PYNQ-Z1 (以下、PYNQ ボードと呼ぶ) とする。PYNQ ボードでは作成した回路に対し、Python からハードウェア制御が行える。第 2 に MMCM のソフトウェアドライバのハードウェア化を行い、回路部品として扱えるようにする。第 3 に TRNG の出力方式をシリアルポートから、DMA (Direct Memory Access) 方式に変更する。これにより、FPGA 単体でのデータ収集が可能になる。

3　提案システムの実装

ドライバのハードウェア化について述べる。MMCM のドライバは C 言語で記述されており、高位合成をすることで IP コアにする。元のソースコードは先行研究の環境に合わせた形となっているため、これを高位合成可能なプログラムに変更する。その後、先行研究 [2] の成果をもとに 1/8 刻みのパラメータが使用できるよう改良をする。ドライバでは M, D, Q の 3 つのパラメータから MMCM が持つ 6 つのレジスタに書き込む値を計算している。分数値を扱えるようドライバの計算処理を修正または追加する。

出力方式の変更について述べる。DMA はプロセッサを介さずにプロセッサのメモリからデータを読みだしたり、書き込んだりすることができるデータ転送方式である。先行研究で使用されていた TRNG と DMA 制御回路は信号のプロトコルが違うのでそのまま接続できない。そのため、DMA が採用された汎用乱数評価回路の TRNG 部分を MMCM を用いたものに変更する。また、MMCM の信号を受け取る入力ポートを追加する。

4　評価

PYNQ ボード上での動作検証とシステムのリソース使用量の調査を行う。動作検証では Python でスクリプトを作成、乱数の出力を確認できた。システムのリソース使用量調査では、ハードウェア化したドライバ回路が 1571 個の LUT と 2079 個のフリップフロップを使用しており、使用量が多いことが分かった。

5　終わりに

本研究を通して先行研究の TRNG を改良し、PYNQ ボード上に実装することができた。ドライバのハードウェア化と出力方式の変更によって、移植性の高い FPGA 向け TRNG に近づけることができた。必要な回路をパッケージングすることや、ハードウェアの使用量を少なくすることが今後の課題となる。

参考文献

[1] N.Fujieda,S.Takashima, An MMCM-based high-speed true random number generator for Xilinx FPGA, International Journal of Networking and Computing, Vol. 11, No. 2, pp.154-171, 2021.

[2] 辻 周造, MMCM を用いた真性乱数生成器のシステム化, 卒業論文, 愛知工業大学, 2022.