2023 年度 卒業研究発表 梗概

電気学科

学籍番号 氏　名	V20101　安達　雄基	指導教員	藤枝 直輝
題　目	MMCM を用いた真性乱数生成器の単一 IP 化に向けた検討		

1　はじめに

現代社会に用いられるセキュリティ技術において、乱数は重要な役割がある。乱数には真性乱数と疑似乱数がある。そのうちの真性乱数、すなわち物理現象をもとにした予測不可能な乱数を生成する回路や機器を True Random Number Generator (以下 TRNG) と呼ぶ。FPGA (Field Programmable Gate Array) に TRNG を組み込むことで幅広い応用が期待できる。先行研究として、AMD 社の 7 シリーズ以降の FPGA に搭載されているクロック生成回路である、MMCM (Mixed-Mode Clock Manager) を用いた手法が提案されている [1][2]。

本研究では、MMCM を用いた TRNG を、AMD 社の FPGA を搭載した SoC (Systems on Chip) である Zynq 上で扱いやすくすることを目的としている。先行研究では、2 個の MMCM のパラメータを動的に切り替えるため、dynclk (Dynamic Clock) とよばれる回路を 2 個使用している。これらを単一の回路にすることで、プロセッサ側とのインタフェース回路が 1 つで済むようにする。

2　MMCM を用いた TRNG の既存の実装

本研究で扱う TRNG は、コヒーレントサンプリングという手法に基づいている。コヒーレントサンプリングを実現するには、周波数が少し異なる 2 つのクロック信号が必要である。藤枝と高島は、適切なパラメータを設定した MMCM を 2 つのクロック信号の生成に使うことで、乱数生成の高速化と乱数の質の向上を可能にした [1]。

また、小谷は MMCM を用いた TRNG を Zynq 上で動作させるために、いくつかの改良を行った [2]。具体的には、従来ソフトウェアドライバで行われていた、MMCM に書き込むパラメータの計算処理をハードウェア化した。また、乱数の出力インタフェースを変更した。本研究は、小谷により作成されたシステムをベースに行う。

3　提案手法

本研究では、dynclk のインタフェース回路の統一化を行うことで、2 個の dynclk に相当する単一の IP コアを作成する。既存のインタフェース回路は、MMCM に書き込むパラメータや制御信号に対応するレジスタを 9 個持つ。このうち同一の値が入っている 1 個のレジスタを除いた、8 個のレジスタを複製し、メモリアドレスとの対応を変更する。提案するインタフェース回路では、レジスタは 17 個となる。また、MMCM やその周辺の回路と配線も複製し、名前の末尾に 0 と 1 をつけることで区別する。

4　評価

作成した dynclk が正しく動作するかを確認するために、シミュレーションと実機での動作確認を行う。また、ハードウェア使用量の比較を行う。動作確認の結果、シミュレーションでは正常な動作を確認したものの、実機ではパラメータによっては乱数の生成が正しく完了しない不具合が生じた。ハードウェア使用量の評価では、dynclk に使用された LUT とフリップフロップの個数は、それぞれ 478 個から 393 個、704 個から 660 個へと減少した。

5　終わりに

本研究では、MMCM を用いた TRNG を Zynq 上で扱いやすくするために、2 個の dynclk に相当する単一の IP コアを作成した。しかし、特定の場合で処理が途中で止まってしまい、乱数を取得することができないという不具合を解消することができなかった。この課題を解決することを今後の課題とする。

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] 小谷孟志, MMCM を用いた真性乱数生成器の PYNQ ボードにおける試作, 卒業論文, 愛知工業大学, 2023.