2020 年度 卒業研究発表 梗概

電気学科

学籍番号 氏　名	V17021　内野　開文	指導教員	藤枝 直輝
題　目	FPGA システムに向けた真性乱数生成器の利用		

1　はじめに

システムセキュリティにおける安全性を確保するために真性乱数が利用されている。真性乱数とは、物理現象をもとに生成される乱数のことである。物理現象自体が原理的に予測不可能であることから、乱数としての安全性が高い。真性乱数を生成するための回路や機器のことを真性乱数生成器 (TRNG) という。内部の論理回路を書き換え可能なディジタル LSI である FPGA (Field Programmable Gate Array) を用いた TRNG も提案されている [1] [2]。先行研究 [3] では、遷移効果リングオシレータの改良の一種 TC-TERO を用いた TRNG を提案し、その実装を FPGA 上の回路として行った。しかし、必要なパラメータを手動で設定する必要があることが、この TRNG を FPGA システムで利用するための課題であった。そこで本研究では、先行研究 [3] における回路をプロセッサから利用可能な IP コアと呼ばれる形にパッケージ化し、これを用いて、パラメータの自動検出を行うことを目標とする。

2　システムの設計

TC-TERO を用いた TRNG には、適切なパラメータを求めるために以下の機能が必要とされる: (1) カウンタ値の生成、(2) 一定期間のカウンタ値の合計・二乗和の集計、(3) カウンタ値の分布が好ましいものであるかのチェック、(4) カウンタ値の最下位ビットの列を乱数として出力。先行研究 [3] では、ハードウェア側が (1) (2) (4) の機能をもっていた。そのため、(2) で得られたデータを PC に送信し、その情報をもとに適切なパラメータを PC で計算することで (3) の機能を PC 側で実行していた。

それに対し、本研究では、これらの回路をプロセッサから利用可能な IP コアへとパッケージ化し、(3) の処理を FPGA 向けのソフトプロセッサである MicroBlaze 上のソフトウェアで実現する。これにより、適切なパラメータが FPGA システム内で自動検出できるようになる。また、パッケージ化された IP コアでは、パラメータをプロセッサから読み出し、命令信号をプロセッサから書き込めるように設計されている。具体的には、パッケージ化された IP コアでは、動作開始信号をソフトウェアから受け取るごとに 4096 回のカウンタ値の生成を行い、その間のカウンタ値の合計・二乗和を集計する。IP コアが動作中であるかはソフトウェアから読み取れるようになっている。ソフトウェアは動作の終了を検知したら、合計・二乗和を読み取り、平均・分散を計算する。もしそれがあらかじめ指定した値に最も近いものであれば、ソフトウェアはその時のパラメータを記録し、PC に表示する。最後に、表示されたパラメータをもとに乱数生成を延々と行い、生成された乱数列を PC に保存し、乱数検定をする。

3　実験方法及び結果

Vivado 2019.1 (Xilinx 社) を使用して、ARTY A7 (xc7a35ticsg324-1L) を対象の FPGA として論理合成と配置配線を行う。MicroBlaze 上のソフトウェアを実行した結果、問題なくすべて機能していることを確認した。 先行研究でのパラメータ検出時と同じく、はじめは得られた平均・分散は指定した値と離れているが、終わりに近づくにつれて近しい値となっていた。また、乱数検定 (AIS-31 のテスト B) を行った結果、乱数列としての基準を満たした。以上により、本研究の目的である TRNG 回路のパッケージ化とパラメータの自動検出に成功した。

参考文献

[1] P. Kohlbrenner and K. Gaj: “An Embedded True Random Number Generator for FPGAs,” in FPGA ’04, pp. 71-78, 2004.

[2] A. Peetermans et al.: “A Highly-Portable True Random Number Generator based on Coherent Sampling,” in FPL ’19, pp. 218-224, 2019.

[3] N. Fujieda: “On the feasibility of TERO-based true random number generator on Xilinx FPGAs,” in FPL ’20, pp. 103–108, 2020.