2019 年度卒業研究発表梗概

電気学科

学籍番号・氏　名	V16072　高島壮剛	指導教員	藤枝 直輝
題　目	MMCM を用いた FPGA 向け真性乱数生成手法の提案		

1　はじめに

近年、通信の暗号化およびセキュリティ分野におけるパスワードの作成などでは、真性乱数が大量に必要とされている。真性乱数とは物理的なランダム要因から生成された、出現する値に規則性、再現性のないビット列である。用いられている真性乱数の実用性、安全性はシステムの安全性に強く影響する。

真性乱数を発生させる回路を TRNG (True Random Number Generator）という。TRNG を FPGA(field-programmable gate array) に作り込むことで、安価かつ外部から盗み取ることが困難な真性乱数を生成できる。FPGA とは回路の動作や構成をユーザ側が設定・構築することができる書き換え可能なハードウェア集積回路である。

2　関連研究

FPGA を用いた TRNG に関連した研究は、Johnson ら [1] によって行われた。彼らの提案した TRNG は、Xilinx 社の古い世代の FPGA に搭載されたクロック生成機能 DCM (Digital Clock Manager) を用いたものであった。DCM を 2 つ用い、それぞれわずかに異なったクロック信号を生成し、一方の信号をもう一方の信号でサンプリングし、その結果をカウントし出力する。この時わずかに異なった 2 つの DCM の信号には、ジッタ (時間的に非常に短い波形の揺らぎ)・メタスタビリティ（DFF のタイミング制約によって発生する出力が不安定になってしまう状態）の影響が発生する。これらの現象を利用し、出力されるカウントの下位ビットを分散させることで真性乱数の生成が行われた。

3　研究の概要

Johnson ら [1] の手法を土台に、新しい世代の FPGA で高速かつ高品質な真性乱数を生成する手法を提案する。本研究では、新しい世代の FPGA である Xilinx 社の Artix-7 FPGA Board に搭載された MMCM (Mixed Mode Clock Manager) [2] を用い、真性乱数の生成を試みる。MMCM とは入力クロックを逓倍・分周することで任意の周波数クロックを得ることのできる FPGA の機能であり、DCM よりも詳細にパラメータを設定することが可能である。MMCM は D、M、Q の 3 つのパラメータを用いることで、生成する周波数を設定する。さらに、DRP(Dynamic Reconfiguration Port) をもち、回路全体の再構成なしに出力周波数を変更することが可能である。この MMCM を用い、高速かつ高品質な真性乱数を生成するため、2 種類の手法を提案する。また、乱数の評価システムは Diehard 試験 (乱数の質を評価するための 18 項目の乱数検定試験) を用いる。

1 つ目の手法として、乱数の生成レートの高速化を提案する。乱数の生成レートの高速化を実現するため、サンプリングされる MMCM の周波数を 4 倍にする。理論上、通常の 1 周期分のカウント時間内に 4 周期分のカウント時間の確保が可能になり、乱数の生成時間は 1/4 になる。この手法を評価した結果、全体の周波数組を通して平均 71.57% の生成時間の短縮が実現できることが示された。

2 つ目の手法として、ジッタ（揺らぎ）の増加による良質な乱数の取得を提案する。各周波数のジッタ増加のため、各 MMCM のパラメータ M,D の値を 7 倍する。それにより、ジッタが増加し、カウントする値の分散が大きくなることで良質な乱数の生成が期待される。この手法を評価した結果、Diehard 試験の結果は大きく変化はなかったが、カウントする値の分散が大きくなることが確認できた。

4　おわりに

本研究では、Johnson ら [1] の手法をもとに、Artix-7 FPGA Board 上に TRNG を実装した。Artix-7 FPGA Board に搭載された MMCM を利用し、高速かつ高品質な真性乱数の生成を行える手法を 2 種類提案した。これらの手法を用いることで、高速性、大きく分散した乱数性、高い確率での真性乱数の実現性などが可能となり、MMCM を用いた TRNG の実用性を高めることが可能となった。

参考文献

[1]A. P. Johnson et al., An Improved DCM-Based Tunable Ture Random Number Generator for Xilinx FPGA, IEEE Trans. Circ. Syst. II : Express Briefs, vol.64, no.4, pp. 454-456, 2017

[2] 小林 優，FPGA プログラム大全 Xilinx 編，株式会社秀和システム，東京，2017