2021 年度 卒業研究発表 梗概

電気学科

学籍番号 氏　名	V18087　辻 周造	指導教員	藤枝 直輝
題　目	MMCM を用いた真性乱数生成器のシステム化		

1　序論

真性乱数はセキュリティシステムの用途で重要である。乱数を生成する機器や回路は、TRNG(真性乱数生成器) と PRNG(疑似乱数生成器) に大別される。PRNG は次の出力を計算で求めるので、内部の状態が知られた際、次の出力が予想できてしまう可能性がある。それに対して、TRNG は物理現象の挙動の不確実性を抽出し、それをビット列として出力するため、次の出力の予想ができないという利点がある。

fujieda らは最近の Xilinx 社の FPGA(Field Programmable Gate Array) に搭載されている、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]。fujieda らはまた、MMCM に動的な周波数変更のインターフェイスを追加する dynclk を用いて、TRNG のプロトタイプを作成した。しかし、既存の dynclk のドライバはパラメータに整数の値しか用いることができない。そのため、先行研究で挙げられたうちの一部の周波数の組しか利用することができなかった。本研究の目的は Dynclk を用いたプロトタイプを改良し、先行研究のすべての周波数の組を利用できるようにすることである。

2　背景

kohlbrenner ら [2] は、coherent sampling と呼ばれる動作原理に基づく FPGA 向けの TRNG を提案している。周波数が少しだけ異なる 2 つの信号を D flip-flop のクロックとデータ入力に与える。このときに生じる信号のゆらぎ (ジッタ) を利用し、ある周期内で'1' をサンプリングした回数をカウントすることで、乱数生成する。MMCM を用いて coherent sampling を行うには、2 つの MMCM に対して逓倍・分周のパラメータである D、M、Q をそれぞれ適切に設定する [1]。M と Q には 1/8 刻みの分数も設定可能である。

3　dynclk IP コアの改良

dynclk は Digilent 社で開発された IP コアであり、MMCM に動的な周波数変更のインターフェイスを与えるものである。dynclk は clk0L レジスタ、clkFBL レジスタ、clkFBH_clk0H レジスタ、divclk レジスタ、lockL レジスタ、fltr_lockH レジスタの 6 つのレジスタをもち、これらに適切な値を書き込むと MMCM の周波数が変更できる。先行研究のプロトタイプ [1] に含まれる dynclk のドライバでは、M、D、Q の整数のパラメータをもとに書き込むべき値を計算する。

本研究では、パラメータ M と Q に分数の値を指定できるように dynclk のドライバを改良した。dynclk のレジスタのうち分数のパラメータを扱う場合のみ使用する部分が存在する。そのため本研究では M と Q に対応している clk0L レジスタ、clkFBL レジスタ、clkFBH_clk0H レジスタをビットシフトなどを用いて書き換えることで分数のパラメータに対応する。

4　評価

評価には Digilent 社の Arty A7 FPGA ボードを使用した。dynclk を用いて 10 秒ごとに MMCM に異なるパラメータを書き込んだ。coherent sampling により得られたカウンタ値を取得し、それをもとにカウンタ値の分布のヒートマップを作成した。評価の結果、想定した期待値を中心に、ある程度の分散をもってカウンタ値が現れた。これにより、改良に成功したことと、出力を真性乱数として取り出せる見込みがあることが確認できた。

5　結論

本研究では dynclk のドライバの改良を通じて、先行研究の TRNG のプロトタイプの改良を行った。その結果、先行研究で挙げられたすべての周波数の組を利用できるようになった。今後の課題として dynlk に書き込む値の事前計算や、カウンタ値ではなく乱数を出力することなどがあげられる。

参考文献

[1] N. Fujieda and S. Takashima, An MMCM-based high-speed true random number generator for Xilinx FPGA, Intl. J. Networking and Computing, vol. 11, no. 2, pp. 154-171, 2021.

[2] P. Kohmbrenner and K. Gaj, An embedded true random number generator for FPGAs,12th international symposium of Field programmable gate arrays, pp. 71-78, 2004