2020 年度 卒業研究発表 梗概

電気学科

学籍番号 氏　名	V17111　平野　湧人	指導教員	藤枝 直輝
題　目	真性乱数生成器の動的再構成に関する研究		

1　序論

計算機システムで使われる乱数には，疑似乱数と真性乱数とがある．真性乱数は熱や雑音などの自然現象から生成され，次の値の予測が原理上不可能であるため，暗号鍵を作るときに利用される．真性乱数を出力する回路や機器を真性乱数生成器 (True Ramdom Number Generator, TRNG) と呼ぶ．先行研究では，FPGA に搭載されてある MMCM (Multi-mode Clock Manager) と呼ばれるクロッキング素子を用いた TRNG が提案されている [1]．先行研究では MMCM のパラメータを変更する際，回路自体の書き直しが必要であった．よって本研究の目的は，回路自体の書き直しをせずにパラメータを変更できるように，先行研究の TRNG を改良することである．dynclk と呼ばれる既存のコア [2] を改良し，MicroBlaze というソフトプロセッサを用いてソフトウェア制御し，FPGA ボードの実機を用いて動作検証する．

2　背景

先行研究の TRNG の動作原理は Coherent Sampling とよばれる．周波数が少しだけ異なる 2 つのクロック信号を D flip-flop (D-FF) のクロックとデータ入力に与える．このとき生じる信号のわずかなゆらぎ（ジッタ）を利用して，乱数を生成する．ここで，周波数が少しだけ異なるクロック信号の組を生成するために，MMCM を 2 つ使用する．MMCM とは，D，M，Q の 3 つのパラメータを選択し，入力周波数を逓倍・分周することで任意の周波数を生成することが出来る FPGA の機能である．

3　LED の点滅制御

MMCM の動的再構成を先行研究の TRNG に適用する前に，まずは LED の点滅回路に対して適用する．dynclk IP で生成したクロックを，点滅回路のクロック入力に接続する．クロック周波数をソフトウェアで正しく制御できれば， LED の点滅周期をソフトウェアから変更できるはずである．dynclk ドライバの関数に，任意の周波数を指定すると，その周波数になるように計算する関数がある．それを利用して，ソフトウェアから周波数を変更できるようなプログラムを作り Vitis 上で動作確認を行った．その結果，入力の周波数を 100 MHz から 80 MHz，160 MHz のに変更し出力できることが確認できた．また点滅周期をストップウォッチで計測したところ，80 MHz の時に比べ，160 MHz の時は，計測時間が約 1/2 であった．したがって，想定した周波数のクロックを dynclk で作成できていることを確認できた．

4　dynclk IP の改良

MMCM のパラメータ D は整数に限られるが，M，Q は 1/8 刻みの小数も使用可能で，先行研究の TRNG はこうしたパラメータも利用する．しかし，現行の dynclk のドライバは小数のパラメータに対応していないため，ドライバの改良に取り組んだ．dynclk ドライバ内の一部の関数を書き換え，小数のパラメータに対応するためのいくつかの変数の計算には成功したものの，ドライバそのものの修正までには至らなかった．dynclk ドライバの一部を更に改良することで，小数の分周比を扱うことが可能になると考えられる．

5　結論

本研究は dynclk IP を用いて Coherent Sampling を用いた TRNG の改良をすることを目的として行った．簡単な LED 点滅回路を題材に，入力クロックのソフトウェア制御に取り組み，dynclk IP に分数の分周比を与える方法について検討した．しかし，ドライバの修正や，修正後の実機検証には至らなかった．今後の課題は，これらの検討結果をもとに TRNG を改良し，動作確認することである．

参考文献

[1] N. Fujieda and S. Takashima: Enhanced use of mixed-mode clock manager for coherent sampling-based true random number generator, CANDAR 2020 Workshops, pp. 197–203, 2020.

[2] J. Tatsukawa: MMCM および PLL のダイナミックリコンフィギュレーション, アプリケーションノート XAPP888 (v1.6.1), Xilinx Inc., 2016.