平成２９年度　卒業研究報告書概要

課程，学籍番号，氏名	課程：電気・電子情報工学課程，学籍番号：B153237 ，氏名：竹原 翔也
工学分野名：情報通信システム	指導教員名：市川 周一，藤枝 直輝

題　　目：和　DCM と LUT ラッチのメタスタビリティを利用した真性乱数生成器の検討

（英　Preliminary design of metastability-based TRNG with DCMs and LUT latches　）

Abstract

A True Random Number Generator (TRNG) is essential for many security applications that depend on random numbers. Hata and Ichikawa (2008) implemented a TRNG using the metastability of RS latch. Johnson et al. (2017) proposed another TRNG utilizing the jitter with Digital Clock Managers (DCMs). The purpose of this research is to implement a new TRNG, which uses a pair of RS latches. R and S inputs of the both latches are connected to respective DCMs with slightly different clock frequencies. Timing difference in outputs of the latches is used as a source of randomness caused by metastability and jitter.

When the TRNGs were implemented in a Xilinx Virtex-5 FPGA, the proposed TRNG was 30% smaller in the number of slices than that proposed by Hata and Ichikawa. However, the generated random numbers passed only 173 items, out of 240, in the DIEHARD test. The removal of periodicity is left as future work.

概　　要

畑ら(2012)は, RS ラッチのメタスタビリティを利用した真性乱数生成回路 (TRNG; True Random Number Generator)を FPGA に実装した．また Johnson ら(2017)は，Xilinx FPGA の Digital Clock Manager (DCM) の分周および逓倍機能を利用して TRNG を実装した．畑らは NAND ゲートを用いた RS ラッチの R 入力と S 入力に同時にアサートする回路を作成し，RS ラッチのメタスタビリティを利用して乱数を取り出す手法を提案した．畑らはゲートの個体差などによる出力の偏りを補正するため，多数のラッチの出力を xor で集約した．Johnson らは 2 つの僅かに異なる周波数のクロックを DFF にアサートし，一方のクロックがもう一方のクロックに追いつくまでにかかったクロック数のジッタによるばらつきから乱数を取り出す手法を提案した．

本研究の目的は，これらの TRNG の利点を組み合わせ，より効率的に真性乱数を生成することである．本稿ではそのプロトタイプの FPGA への実装と評価について報告する．

本研究では，畑らおよび Johnson らの方法がラッチや FF の出力の不一致を検出していることに注目する．DCM によって周波数を変えた 2 種類のクロックを，2 個の RS ラッチの R 入力と S 入力にそれぞれアサートする．2 個の RS ラッチを xor することにより，配線遅延・ジッタ・メタスタビリティなどの理由によってラッチ間で出力に差異が生じたときのみ``1"が出力される．``1"が出力されたタイミングにおける 8 ビットカウンタの値を全ビット xor し，結果を乱数として取り出す．同じ論理を持つ複数の回路からは基本的に同じ出力が得られるはずだが，メタスタビリティやジッタの影響で出力に不一致が生じる．不一致が検出されている時間に一種の乱数性があると考え，その時間をもとに真性乱数を生成する方法を提案している．

評価には Xilinx 社の Virtex-5 FPGA (XC5VLX50)，論理合成・実装には Xilinx Design Suite 14.7 を使用した．乱数の品質評価は DIEHARD テストにておこなった．DIEHARD には明確な合格基準がないため，p-value が $0.025 < p < 0.975$ の範囲に入るものを合格とした．

実装結果から，回路規模は畑らの提案する TRNG と比較して 30 % 程度のスライスの減少が確認された．また，DIEHARD テストの結果，合格した項目は 240 項目中 173 項目となった．主にデータに規則性や偏りがないことをチェックする検定である OPSO テストや OQSO テストなどの項目で多く不合格になっている．

本研究で実装した回路を実応用するためには更なる検討が必要である.出力されるカウンタの値に規則性が生じているので，偏りを除去する補正回路を考案し実装する必要がある．

発表する際の課程を記入　電気・電子情報工学　課程　　発表番号　17

（学籍が他課程所属の学生も発表する課程を記入すること）