平成３０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：B173237，氏名：武田　真明
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 のジッタを用いたメタスタビリティ型 TRNG の調査

（英 Experiments on metastability-type TRNG based on jitters of DCM ）

Abstract

True random numbers are widely used, for example, as a key in encryption. True Random Number Generator (TRNG) is required to generate true random number. This research presents the reproduced experiments on DCM-based invented by Johnson et al, and the quality of the derived random numbers. Random number quality survey was conducted with 100 combinations of frequencies in ascending order of the difference between the periods of the two DCMs. This type of TRNG passed all 18 items of the Diehard test with two combinations of frequencies. In these cases, the generation rates were 0.6266 Mbps and 1.2020 Mbps, respectively. From these result, it was found that it is necessary to raise the quality of random numbers in a wider frequency combination in order to raise TRNG's ideas invented by Johnson et al.

概　　要

暗号化の際の鍵として予測不可能性の高い真性乱数が用いられる．真性乱数を生成するためには真性乱数生成器（True Random Number Generator; TRNG）が必要になる．真性乱数生成器には出力する乱数の品質とともに生成速度も要求される．

熱雑音などのアナログな物理現象を用いた TRNG などがあるが，論理 LSI に集積することは容易ではない．論理素子を用いた TRNG としては，市川ら（2012）の考案した RS ラッチのメタスタビリティを用いたものや Johnson ら（2017）の考案した DCM を用いたものなどが挙げられる．

本研究では Johnson ら（2017）の考案した TRNG について再現実験を行い，乱数品質の評価と動作の確認を行った．Johnson ら（2017）の TRNG は Xilinx 社製の FPGA に搭載されている DCM（Digital Clock Manager）を 2 つ，DFF を 1 つ，カウンタを 1 つ用いる．2 つの DCM それぞれから周波数のわずかに異なる信号を発生させ，1 つは DFF の入力端子に，もう一方は DFF とカウンタのクロック端子に入力する．カウンタでは DFF が 0 を出力している期間を計測し，下位 3 ビットを出力する．カウンタからの出力は VNC（Von Neumann Corrector）と呼ばれる後処理を行い，乱数を得る．再現実験ではこの TRNG を Xilinx 社の ML501 評価ボード上の Virtex-5 FPGA に実装し，2 つの DCM の周期の差が小さい順に 100 パターンの周波数の組み合わせについて乱数品質を調査した．

調査の結果，100 パターンの組み合わせのうち，82.3529 MHz と 82.1429 MHz，96.6667 MHz と 96.2963 MHz の 2 組の周波数において，乱数試験である Diehard 試験の 18 項目すべてに合格した．このときの乱数の生成レートはそれぞれ 0.6266 Mbps，1.2020Mbps であった．また，平均 9.24 項目で不合格となった．さらに，下位ビットの方がより乱数品質が高いと考えられたため，出力の下位 1 ビットについても同様の調査を行った結果，平均 6.01 項目で不合格となり，下位 3 ビットの場合と比較して全体で乱数品質が向上したことが確認できた．しかし，18 項目すべてで合格した周波数の組み合わせはなかった．

この結果より，Johnson ら（2017）の考案した TRNG の有用性を高めるにはより幅広い周波数の組み合わせにおいて乱数品質を高める必要があるといえる．今後の課題として下位 2 ビットについても 100 パターンの周波数の組み合わせで実験を行う．

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　42

（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）