令和元（２０１９）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：B121814，氏名：奥田　純基
工学分野名：情報通信システムコース	指導教員名：市川　周一

題　　目：和　Xilinx 製 FPGA を用いた NIST 乱数検定回路の軽量実装

（英　Lightweight Implementation of Statistical Tests for Random Number Generators by NIST for Xilinx FPGA　　）

Abstract

This study presents the implementation of four type of NIST SP 800-22, that are Frequency (Monobits) Test, Test For Frequency Within A Block, Runs Test, and Test For The Longest Runs of Ones In A Block, on Xilinx FPGA.

The evaluation environment includes Artix-7 FPGA board, SystemVerilog as Hardware Description Language, Vivado (2018.1) Web Pack as behavioral simulation, logic synthesis and implementation. For simple hardware design, only integer arithmetics were implemented. Although these tests include Error function and Gamma function, these functions are not suitable for hardware. Thus, the test results are judged by the thresholds that satisfies the significance level.

In the derived implementation, the check circuit occupies 486 Look Up Tables, 191 Flip-Flops, and 2 Digital Signal Processors.

概　　要

暗号技術に必要な乱数の生成を行う真性乱数生成器（TRNG）の出力は，経年劣化や電圧等の動作環境の変化，あるいは外部からの意図的な攻撃によってその出力に偏りが生じる．乱数品質を判定する乱数検定は，ソフトウェアとハードウェアのいずれにも実装可能であり，TRNG の出力をオンラインで検定することにより，出力の異常をリアルタイムで検出可能となる．オンラインで乱数検定を行う場合，ソフトウェアとして実行すればプロセッサ時間を消費し，ハードウェアとして実装すれば論理規模・実装コストの増大を招く．

Suresh ら (2013) は，ハードウェアに米国標準技術研究所 (NIST) が開発した乱数検定 NIST SP 800-22 のうち 6 種(Frequency (Monobits) Test, Test For Frequency Within A Block, Runs Test, Test For The Longest Runs of Ones In A Block，Non Overlapping Templete Matching Test，Binary Matrix Rank Test) をハードウェアとして実装した．Yang ら(2015)は，ソフトウェアとハードウェアの両方を用いて，NIST SP 800-22 に含まれる 15 種全てのオンライン検定回路を実装した．

本研究の目的は，　NIST SP 800-22 のうち 4 種(Frequency (Monobits) Test, Test For Frequency Within A Block, Runs Test, Test For The Longest Runs of Ones In A Block) を，Xilinx 社製の FPGA である Artix-7 XC7A35TICSG324-1L に実装し，乱数品質をリアルタイムで検定することである．計算が簡易な検定のみをハードウェアに実装することでハードウェアのコストを軽減する．検定回路による簡易検定で乱数品質低下が発見された場合，ソフトウェアで正確な乱数品質を調べる．

本研究では，　SystemVerilog で記述し，Xilinx 社の Vivado (2018.1) Web Pack を用いて機能のシミュレーション・論理合成・実装を行った．SystemVerilog ファイルについては，NIST SP 800-22 (2010)を参考に記述した．正確な検定には小数演算を必要とするが，小規模化のために整数演算で実装した．Xilinx 社の FPGA には除算器がない為，除算が必要となる場合は論理シフトを用いて計算している．誤差関数やガンマ関数といった複雑な計算はハードウェアでの処理に向かないため，本来の検定で誤差関数やガンマ関数に代入する観測値を有意水準に対応した閾値と比較を行う設計とした．NIST は有意水準 0.001～0.01 を推奨しており，実装した検定回路では，0.001，0.004，0.007，0.01 を選択可能である．

実装した上述の 4 種の検定を含む検定回路の規模について，ルックアップテーブル使用数は 486 個，フリップフロップ使用数は 191 個，デジタルシグナルプロセッサ使用数は 2 個となった．

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　1

（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）