2021 年 1 月 8 日

電気・電子情報工学専攻	学籍番号	M163221
申請者氏名	岸部 仁美	

指導教員氏名	市川 周一

論　文　要　旨（修士）

論文題目	ラッチ型 TRNG の軽量実装と乱数品質保持手法の検討

乱数は多くのセキュリティ応用で必須の要素となっており，高品質な乱数が求められている．乱数には疑似乱数と真性乱数がある．疑似乱数はアルゴリズムに基づいて生成されるため，内部状態が推測されれば将来の値が予測できる．真性乱数は物理現象に基づいて生成されるため，ハードウェア支援が必須であるが，予測と再現が不可能である．本研究では真性乱数生成を扱い，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）を検討する．

畑と市川（2012）は，ラッチ型 TRNG を Xilinx Virtex-4 FXFPGA 上に実装した．乱数品質向上のためハードマクロで実装した結果，FPGA の機種に依存した実装となった．藤枝と市川（2018）は，HDL を使用したソフトマクロでラッチ型 TRNG を実現した．設計のポータビリティと保守性が向上したが，ソフトマクロ実装はハードマクロ実装よりハードウェアコスト（ラッチ数）が大きくなるという問題点があった．

TRNG は物理現象に基づいて動作するため，得られる乱数品質は電源電圧・動作温度などの影響を受ける．動作条件が悪い場合や外部からの攻撃により，乱数品質が低下する可能性がある．動作不良や攻撃を検出するため，TRNG 動作時にオンラインで出力を検査し，品質低下時に警告を出す必要がある．本研究では，乱数品質をオンラインで検査する方法を調査する．

本研究の目的は，ソフトマクロ実装のハードウェアコストを低減しつつ，乱数品質を維持することである．実装コストを削減するためにはラッチ数を減らさなければならないが，ラッチ数を減らすと生成されるエントロピーが減少して乱数品質が低下する．そこで TRNG の出力を XOR で複数サイクル集約することにより，乱数品質の向上を図る．実装評価の結果，ラッチ個数を削減しても乱数検定に合格し，時間的に連続したビットを XOR で集積するより時間的に離れたビットを XOR で集積する方が，乱数品質が高いことが示された．本研究では，乱数品質に応じて集約サイクル数を増減して乱数品質を維持する方法についても検討する．

評価システムには FPGA ボード Avnet ZedBoard を用いて実装した．ZedBoard は Xilinx Zynq-7000 XC7Z020-CLG484-1 を搭載しており，Zynq-7000 は OS として Linux の一種である Xillinux が動作している．評価システムでは Xillinux の周辺回路に TRNG を実装した．乱数を統計的検定にかけることで乱数品質の評価を行う．今回は Diehard テストを利用した．Diehard テストの結果を分析することにより，乱数品質をオンラインで検査する方法を考察する．