審査の結果の要旨

論文提出者氏名　サリー　エルギュン

本論文は「Chaotic Oscillator and Ring Oscillator Based Approaches for Random Number Generation (カオスオシレータとリングオシレータによる乱数生成方法)」と題し、暗号等の主としてセキュリティシステム応用に向けた真正乱数を発生するためのハードウェア回路を提案し、その乱数特性を解析的および実験的に検証したものであり、英文で記述され七章より構成されている.

第一章は「INTRODUCTION(序論)」であり研究の背景として過去の乱数生成手法を紹介し、本研究の目的と位置づけを述べている。

第二章は「CHAOTIC OSCILLATOR BASED APPROACH FOR RANDOM NUMBER GENERATION（カオスオシレータによる乱数生成)」と題し、カオスオシレータの出力を通常のオシレータ出力でサンプリングする方法、カオスオシレータの出力を別のカオスオシレータの出力でサンプリングする方法、さらに通常のオシレータの出力をカオスオシレータでサンプリングする方法を理論的に解析し、また実験データを用いて検証している。これによりカオスオシレータを基にした手法の分類と特徴、位置づけを明らかにしている。

第三章は「RING OSCILLATOR BASED APPROACH FOR RANDOM NUMBER GENERATION（リングオシレータによる乱数生成)」と題し、本論文で研究しているもうひとつのカテゴリーであるリングオシレータと雑音源を利用した乱数生成方法について解析している。ここでも雑音源をリングオシレータ出力でサンプリングする方法とリングオシレータ出力を雑音源でサンプリングする方法を理論と実験データ用いて比較検討している。

第四章は「PROPOSED CHAOTIC OSCILLATORS AND APPLICATION TO RANDOM NUMBER GENERATION（カオスオシレータの提案と乱数生成への応用)」と題し、“バイポーラトランジスタ差動対とキャパシターおよび抵抗を用いた非オートノマス・カオスオシレータ”と、“バイポーラトランジスタ差動対とキャパシター、抵抗およびインダクターを用いた非オートノマス・カオスオシレータ”の２種類を提案し、シミュレーションによりその特性を解析するとともに乱数生成への具体的応用例を示している。さらに後者を CMOS 向けに設計した非オートノマス・カオスオシレータを個別素子による回路として試作測定し、実験的にその有効性を検証している。

第五章は「FPGA BASED STATISTICAL TEST AND DATA ACQUISITION SYSTEM（フィールドプログラム可能なゲートアレイを用いた統計的検定とデータ収集システム)」と題し、FPGA により乱数の統計的検定を高速化する手法を提案している。このシステムは乱数の統計的検定に用いるだけでなく、擬似乱数生成器に代わる真正乱数生成器としても利用できるよう設計されている。第二章で述べたカオスオシレータベースの乱数生成器のひとつであるカオス信号で変調された電圧制御発信器出力を乱数信号源として用いており、５種の検定項目をハードウェアで実施できる。結果は PCI インターフェースを通じて外部に出力する機構となっている。また PCI を通じて、将来の新たなソフトウェアで生成された乱数系列の検定も短時間で可能な構成となっている。

第六章は「USING PROPOSED RNG FOR APPLICATIONS IN CRYPTOGRAHY（提案した乱数生成器の暗号技術への応用)」と題し、論文で提案した乱数生成器を“生物学的特長を利用した安全な認証”と“組み込み型指紋認証”システムに用いる例を紹介している。

第七章は「CONCLUSIONS AND FUTURE WORK(結論と今後の課題)」であり本論文の研究成果をまとめ、本研究の将来の発展方向を議論している.

以上、本論文はカオスオシレータやリングオシレータを用いてハードウェアにより真正乱数を効率的に生成する手法を網羅的に分析し、生成される乱数の特性を解析的および実験的に検証するとともに、新たなカオスオシレータおよび乱数高速検定ハードウェアを考案しその有効性を示したもので、電子工学の発展に寄与する点が少なくない.

よって本論文は博士（工学）の学位請求論文として合格したものと認められる.