論文の内容の要旨

論文題目：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）

氏　名：　サリー　エルギュン

本論文では、連続時間カオスシステムによる新しい乱数生成手法を提案する。これは、もっとも良い統計的特性と高い乱数生成速度を持ち、外部からの雑音等の妨害や回路パラメータのバラツキ、悪意の攻撃に対して高いロバスト性を有している。さらに、この手法に基づく集積回路向きの真正乱数生成器を提案する。カオス・トラジェクトリ手法を用いて雑音の影響を解析し、提案するカオスによる乱数生成器が真の乱数源として利用できることを証明する。

また、ブーストストラップ手法を用いて乱数生成器を設計するための数学モデルを提案する。これによりカオス信号の中の統計的特性を推定できることを示す。さらに新しいカオス発振器から派生する設計手法についても提案する。設計例として、カオス特性においてよりロバス性を有する交差結合非自律型カオス発振器とそれらを利用した乱数生成への応用についても説明する。

まず、リングオシレータによる乱数生成器の ASIC 設計とその実現例を紹介する。この設計のプロトタイプは HHNEC の“0.25μm eFlash プロセス”を用いて設計され、2.5V の電圧電源で動作する。実現例では毎秒数百メガビット程度の高い乱数生成速度が得られた。

次に、提案する乱数生成器が FIPS-140-2 と NIST-800-22 の評価認定テストを発生数列の後処理なしでパスしたことを数値実験結果を用いて実証する。

本論文で説明する連続時間カオス発振器とリングオシレータによる乱数生成手法は知られる限り世界初のものであり、数学的手法と実験結果を併用して提案回路の正しい動作を証明している。本提案が集積回路向き高性能・高速の真正乱数生成器として、実用に寄与することを期待している。