カオスを用いた乱数生成方法（特願２００７－３２５２５３）

本願の発明はロジスティック写像 $x_{t+1} = 4x_t(1-x_t)$　　$(0 < x_t < 1,\ \ t = 0,1,2,...)$ に対し、整数演算による固定小数点演算で計算する手法を開発した。また、整数演算による計算過程に存在する計算精度と同じビット数の（一般的な計算方法では出力する際に切り捨てられている）下位ビットを利用した撹拌方法を開発した。そのため、計算精度を 128 ビットに拡張するときも擬似乱数の出力速度を 500Mbps (Genuine Intel(R) 1.50GHz)以上に維持できた。

本発明は乱数の生成において、整数を用いた計算（加算、乗算、ビットシフト、論理演算）だけで実行されるため、整数の分割計算が容易であるから、異なるシステム（汎用計算機（各種のＯＳ）、専用ハードウェア、マイクロコンピュータなど）であっても、最も基本的な整数演算（加算、乗算、ビットシフト、ビットごとの論理演算）ができるのであれば、同じ入力による同じ出力が得られる。そして、集積回路化も容易に実現でき、更なる高速化も容易である。

本発明はセキュリティー用に不向きな伝統的乱数生成法である線形合同法と違い、カオスの振る舞いをする時系列を生成する非線形写像を計算することにより、乱数を生成する上、撹拌方法に一方向性を有する排他的論理和の演算を施したことで、出力された乱数から内部状態 x_t を予測することができない。また、出力された一部の乱数から他の乱数を推測することもできない。

従って、本発明の乱数生成装置は様々なニーズに対応できる「性能―コスト」の組合せを持ち、拡張性も富み、科学研究、セキュリティー分野を含む幅広い産業の分野での応用が可能である。