様 式 第 9 号（学位論文公表様式）

称号及び氏名	博士（ 理学 ） 青木 一弘
学位授与の日付	平成１９年１２月３１日
論 文 名	「カオスを用いたスペクトル拡散符号の構成と通信への応用」
論文審査委員	主査 馬野 元秀 副査 佐藤 優子 副査 佐々木 逸雄

論文要旨

近年，スペクトル拡散(Spread Spectrum：SS)方式が，携帯電話や無線 LAN など多くの無線通信システムに利用されている。SS 方式とは，情報信号の周波数帯域を拡散符号と呼ばれる情報信号と独立な符号によって広い帯域に広げて伝送する通信方式である。SS 方式は，秘話性や秘匿性，雑音や干渉に強いなどの通信システムとして優れた特徴を持っている。また，複数の異なる拡散符号を用いることにより多重通信が可能で，限られた周波数帯域の中で多数のユーザを収容するとともに高速なデータ伝送が実現できる。しかし，通信できるユーザ数を増加するためには，互いに相関がない拡散符号が多数必要になる。代表的な SS 方式には，直接拡散(Direct Sequence：DS)/SS 方式と周波数ホッピング(Frequency Hopping：FH)/SS 方式がある。DS/SS 方式では，拡散符号として広帯域なスペクトルを有する 2 値系列を必要とするのに対し，FH/SS 方式では，多値系列の拡散符号が必要となる。どちらの方式においても，拡散符号が通信システム全体の性能を決定する大きな役割を果たす。

このようなスペクトル拡散符号の生成手法として，カオスを応用しようとする研究が行われている。カオスは，非線形システムにおいて発生する不規則で複雑な現象で，カオスから発生する信号は広帯域なスペクトルを持つ。カオスは，その発生式が持っている一つのパラメータを調整するだけで様々なパターンを持った系列を生成できる。また，同じパラメータであっても初期値を変えれば発生する系列は大きく異なり，理論上は無限個の系列を生成できる。カオスが持つこれらの特徴を利用することにより，カオスから擬似乱数を生成し，それを暗号通信に応用できる。また，相関特性に優れた 2 値の系列が多数生成できれば，DS/SS 方式の拡散符号への応用が可能となる。

SS 通信や暗号通信にカオスを応用する場合，送信側と受信側で同一のカオス信号を生成する必要がある。従来，カオスが持つ初期値鋭敏性や軌道不安定性により，初期値の異なる複数のカオスシステムが，カオス状態で同期することは困難であると考えられてきた。しかし，1990 年に Pecora と Carroll によってカオス同期現象を利用した通信方式が提案されて以来，数多くのカオス同期通信システムが提案されている。カオス同期通信では，送信側と受信側にある二つのカオスシステムをカオス状態で同期させることで情報信号の変復調を行い，カオス信号のランダム性

により通信の暗号化が可能となる。しかし，従来のカオス同期通信システムでは，通信路雑音によりカオス同期が完全に達成されず，通信品質の劣化を引き起こすという問題がある。

このような背景のもとに，本論文では，カオスを応用した通信に関する次の 3 点について検討する。

(1) 2 値の擬似乱数の構成と DS/SS 方式用拡散符号への応用
(2) FH/SS 方式用拡散符号の構成
(3)カオス同期通信システムにおける耐雑音性の改善

(1) 2 値の擬似乱数の構成と DS/SS 方式用拡散符号への応用では，カオスから 2 値の擬似乱数を生成する方法を提案し，統計的検定法により生成した系列が十分に乱雑であることを示す。また，提案法による 2 値の擬似乱数が DS/SS 方式用の拡散符号に応用できることを示す。

(2) FH/SS 方式用拡散符号の構成では，カオス写像から FH/SS 方式用の拡散符号を生成する方法を提案し，良好な特性を持った符号が生成できることを示す。

(3)カオス同期通信システムにおける耐雑音性の改善では，カオス同期通信に対して M-ary/SS 方式の導入を検討する。M-ary/SS 方式とは，一つの送信局に対して複数の 2 値符号を用意し，送信する情報に基づいて複数の符号の中から一つを選択して送信する方式であり，DS/SS 方式と比較して周波数利用効率が高く,耐雑音性に優れたスペクトル拡散通信方式として知られている。

本論文は 8 章で構成されており，以下に，各章の概要を述べる。

第 1 章では，本論文の序論を述べ，本研究の背景と目的を説明している。

第 2 章では，従来のカオスを用いた符号の構成とその問題点について整理している。

第 3 章では，カオスを用いた 2 値の擬似乱数の生成法を提案している。カオスから 2 値の擬似乱数を得るには，カオス発生式から不規則な実数値系列を生成し，それを設定したしきい値によって 2 値系列に変換すればカオスから 2 値の擬似乱数（カオス 2 値系列）が生成できる。しかし，この方法によって生成した擬似乱数は，乱雑な 2 値系列の典型例であるベルヌイ試行との近似を考えた場合には,従来の擬似乱数と比較して性質のよい乱数とはいえないことが報告されている。また，電子計算機によってカオスを発生させるため，生成される擬似乱数は計算機の有限精度に応じた周期性を持つという難点がある。そこで本研究では，カオス 2 値系列にフィードバックを加えて新しい 2 値系列に変換し直す手法を提案する。本論文では，本手法により生成された系列をカオスフィードバック変換系列と呼ぶ。本提案により，乱数に適さないカオスから良好な性質の 2 値の擬似乱数が生成でき，更には系列の長周期化も可能となることを示す。

第 4 章では，2 値の擬似乱数に対する新たな乱数検定法として，Ahmed らが提案した拡張型ウォルシュパワースペクトルを用いた方法を提案している。擬似乱数の周期性に関する検定を行う場合，フーリエ変換が用いられるが，2 値の擬似乱数を検定する場合には，三角関数を基底に持つフーリエ変換よりウォルシュ変換の方が適していると考えられる。しかしながら，ウォルシュパワースペクトルはフーリエパワースペクトルのように巡回シフトに関して不変ではない。本研究では，巡回シフトに関して不変である拡張型ウォルシュパワースペクトルを 2 値の擬似乱数の検定に適用し，統計的な検定法との比較により，擬似乱数の検定に適していることを示す。

第 5 章では,カオス発生式から DS/SS 方式用の拡散符号を生成する方法を提案している。DS/SS 方式では，従来，M 系列や Gold 系列等が用いられていたが，符号の種類数に制限があるという難点があった。それに対し，ランダムな系列を多数生成できるカオスを拡散符号に利用する提案がなされているが，符号の発生効率に問題があった。本研究では，発生効率を損なわない符号生成法を二つ提案する。一つ目は，第 3 章で述べたフィードバック変換を用いた方法で，カオスフィードバック変換系列が，乱数としてだけではなく，拡散符号としても有効であることを示す。二つ目は，2 種類のカオス発生式を用いて，各々の式から得られるカオス 2 値系列を一致演算により合成しランダムな 2 値系列を生成する方法である。本論文では，この系列を結合カオス系列と呼ぶ。どちらの方法も簡単なシステムで拡散符号を生成できる。また，複数あるパラメータを

変化させることで多種類の符号を生成できることも示す。

第 6 章では，カオス写像から FH/SS 方式用の拡散符号を構成する方法を提案している。これまで，カオスを FH/SS 方式用の拡散符号の生成に応用しようとする研究は，ほとんど行われていない。本研究では，デシメーションと呼ばれる手法を使って，カオス写像から FH/SS 方式用の拡散符号を生成する方法を提案する。提案法により生成された系列のハミング相関特性，ホッピング距離を調べ，FH/SS 方式用拡散符号としての有効性を確認した。

第 7 章では，カオス同期通信システムの耐雑音性の改善を目的に，カオス同期通信に M-ary/SS 方式の原理を適用した通信システムを提案している。M-ary/SS 方式では，伝送される符号系列が情報信号に応じて変化するため,受信機において符号系列の先頭と最後の位置を検出すること，すなわち，フレーム同期タイミングの獲得が難しいという問題があるが，カオス同期現象を利用することによりこの問題を解決できることを示す。また，提案したシステムの雑音に対する性能を評価している。

最後に，第 8 章において本研究によって得られた結果を総括し，今後の課題について述べる。

学位論文審査結果要旨

近年、携帯電話、無線 LAN 等の利用者増に伴い、情報通信分野において高速、大容量通信が可能なスペクトル拡散通信（SS 通信）方式が注目されている。SS 通信は、擬似乱数系列（SS 符号）を用いてスペクトルを拡散して通信を行う方式であり、SS 符号の特性により通信品質が左右される。SS 符号には十分な乱数性と良好な相関特性が必要であり、符号系列を数多く生成可能という条件も要求される。現行通信システムの SS 符号には、ゴールド符号系列等が用いられているが、多種類の系列を生成できないために今後のユーザ数の増加に対応し難いことやセキュリティ対策に難があること等の問題点がある。これらを解決するために、本論文ではカオスを用いた SS 符号の構成法を示し、これを SS 通信へ応用したカオス SS 通信の実現を目指している。本論文の主要な成果は次の通りである。

（１） カオスを用いて 2 値の擬似乱数系列を生成する方法（カオスフィードバック変換法）を提案し、生成した擬似乱数系列が十分な乱数性を有することを統計的検定法により示している。

（２） 拡張型ウォルシュ変換を用いた乱数検定法を新たに提案し、これが巡回シフト型の 2 値の擬似乱数系列の検定に有効であることを示している。

（３） 直接スペクトル拡散通信に適した SS 符号生成法として新たに結合カオスを提案し、この方法が符号生成効率に優れていることおよび SS 通信に有効であることを示している。

（４） 周波数ホッピングスペクトル拡散通信に適した SS 符号として３区分 N 型カオス写像の値をデシメーションすることにより得られる符号系列がよい結果を得ることを示している。

（５） カオス同期通信に M-ary／SS（M 元 SS 通信）の方式を用いることにより、耐雑音性に優れたカオス通信システムが構築できる事を示している。

本研究は、カオスの乱雑性を利用することにより擬似乱数系列を生成し、これを SS 通信の SS 符号に適用して、その有効性を計算機シミュレーションにより確認している。カオスを用いて良好な相関特性を有する多種類の SS 符号系列を生成可能にしたことは大きな成果である。カオスの通信への応用を考えた本研究は、カオス SS 通信の可能性を示唆するものとして有効であり、特にカオスの予測不可能性を利用した秘密通信への応用が大いに期待される。

本研究の成果は、カオスを用いたスペクトル拡散通信の新しい手法を提案し、計算機シミュレーションによる良好な結果を与えており、理論および実践面で今後の情報通信分野、特にスペク

トル拡散通信の発展に大きく貢献するものである。