統計的解析を用いたカオス通信系の構築

小向省吾・清水能理・小向大輝・木戸口孝人・髙橋潤
八戸工業大学

1．まえがき

現在ネットワーク上の電子情報を保護する暗号化プロトコルとしてSSL、TLS、S/MIMEなどが用いられている。公開鍵暗号方式は、素因数分解や離散対数問題などが用いられているが、昨今のコンピュータの処理速度の上昇により、今後さらに暗号鍵長の増加が必要とされ、コンピュータへの負担がより一層増加すると予想される。本研究では、単純規則に従うシンプル性を有しながらも複雑不規則な現象を生じるカオス現象を応用する。暗号化関数の利便性、暗号鍵の秘匿性、秘匿通信系モデルの秘匿性を解決するため、カオス同期およびカオス分岐に基づく搬送波生成および暗号方式を用いた秘匿通信系を設計する[1]。

2．秘匿通信系

対象とする秘匿通信系は、カオス発生回路のChua 回路を用いたカオス変調通信系である。サブシステム S1、S2 には、同期部、変調部、復調部を設計する。同期部はカオス同期化制御を行い、S1、S2 の状態を等しくする。同期化制御として用いる非線形フィードバック制御（NFC）は、線形状態フィードバック制御に、非線形フィードバック項を追加したものである。通信時の秘匿性を高めるため、変調部、復調部のカオス状態に対し、同期部の状態を暗号鍵として用いてカオス分岐を行う。カオス分岐を行うために用いるカオス同期部の状態、およびカオス分岐を行った変調部の状態は、カオス秘匿通信の特性上カオス性を保持していなければならない。変調部では、カオス分岐を発生させた変調部の状態を用いて、情報信号を暗号化関数により搬送波に変換し、送信する[2]。

3．問題の記述

秘匿通信系のカオス時系列は、変調部と復調部とも同様のカオス性が必要となる。カオスモデルは、分岐パラメータの値により軌道の位相的性質を変える現象が起こる（カオス分岐）。カオス挙動を示すとき、多くの不安定周期点を持っているが、パラメータのとる値によっては周期性を生じる（カオス窓）。カオス状態はその複雑さゆえ高い秘匿性をもち、秘匿通信システムに応用される。しかし、人工的にカオスを発振させる電子回路の実装において、分岐に基づきパラメータ値の設定するとき、カオス窓の問題がある。

4．サロゲート法

カオス応答を示す重要な要因は非線形性にある。サロゲートデータ法は、観測された時系列に対する線形確率過程の存在を帰無仮説として提示し、非線形統計量の推定を通じて検定する。そして、帰無仮説を棄却することで非線形の存在を示す。

基本アルゴリズムは、

(1)「観測された時系列信号は、時間的に全く無相関である」という帰無仮説に従うランダム・シャッフル(RS)

(2) 帰無仮説「観測された時系列信号は、時間的に線形相関を持つ確率的データである」に従うフーリエ・トランスフォーム(FT)

(3) 帰無仮説「観測された時系列信号は、非線形確率過程から作り出されたが、観測する際に性的な単調非線形変換を施されたことにより得られたデータである」に従うアンプリチュード・アジャステッド・フーリエ・トランスフォーム(AAFT)

である[3]。

5．提案手法

カオス発振回路のパラメータ値の推定にはカオス分岐図を用いることが考えられるが、周期軌道（窓）が発生していないかのカオス性評価が必然となる。よって、確率・統計論に基づいた時系列解析手法のサロゲートアルゴリズムに基づくカオス性検定と分岐図を応用したカオス分岐パラメータ値の範囲設定を行う。

分岐パラメータ設定手法について、以下にまとめる。

Chaotic Communication Systems Designed Applying Statistical Analysis
S. Komukai, Y. Shimizu, D. Komukai, T. Kidoguchi, J. Takahashi
Hachinohe Institute of Technology

(1) Chua 回路における分岐パラメータの値を変化させていき、各値のときの Chua 回路から出力される時系列信号を計算する。
(2) 横軸に分岐パラメータの値、縦軸に出力信号の状態を取る。各パラメータ値において、(1)で得られた信号の値を重ねてプロットし、カオス分岐図を作成する。
(3) (2)で作成した分岐図の形態をもとに、時系列がカオス的振舞いをする領域の分岐パラメータ値の範囲を推定する。
(4) 推定した領域において特定した分岐パラメータ値を用いたときの時系列データに対して、サロゲート法を適用し、カオス窓か否かの検定を行う。

秘匿通信システムの変調部でカオス分岐を行った状態は、カオス性を保持していなければならない。よって、分岐図を用いたカオス分岐パラメータ値の範囲で、サロゲート法によるカオス性の検定を行う。カオス同期化部のカオス状態を暗号鍵として用いてカオス分岐を発生させたカオス波形に基づいた暗号化関数を設計し、暗号化・復号を行う。従来の手法のように暗号化関数を複雑にする必要がなく、その逆関数を求める困難さが小さい。

6．シミュレーション

FT サロゲート法を用いた数値実験結果の例を以下に示す。

オリジナルデータとサロゲートデータの統計量を比較すると、表 1 のように平均、分散ともにサロゲートデータ作成過程において統計量が保存されていた。一方、FT アルゴリズムの性質上、頻度分布は保存されない。図 1 と図 2 の信号を比較すると、オリジナルデータ時系列信号の構造は全く壊されている。このことから、分岐パラメータが 0.70 値をとる場合、時系列信号は線形なダイナミクスで表現することが難しいことがわかる。

Chua 回路を用いたカオス同期秘匿通信系のシミュレーションを行った。サイン波の暗号化・復元を行った実験結果を図 3 と図 4 に示す。

表 1　FT サロゲートデータ作成過程において保存される統計量

平均	分散	頻度分布	自己相関
○	○	×	○

※保存される○　保存されない×

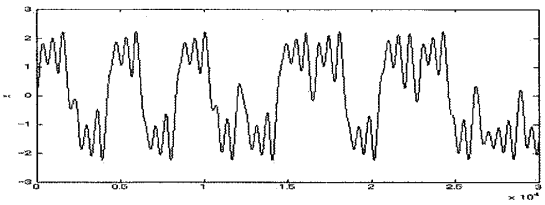

図 1　Chua 回路における時系列信号

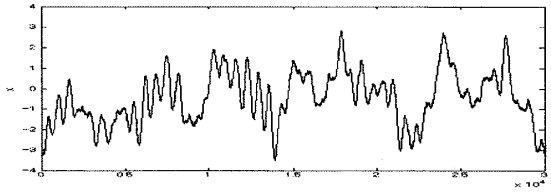

図 2　FT サロゲート変換信号

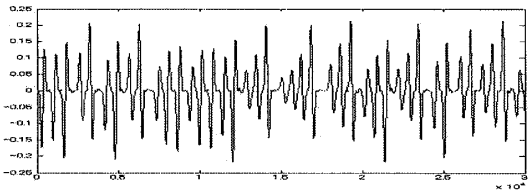

図 3　変調信号

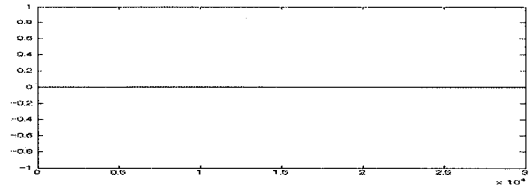

図 4　情報信号と復調信号の差

7．まとめ

カオス分岐図を用いて設定した分岐パラメータ値における Chua 回路からの時系列信号に対し、サロゲートデータ法を適用し、カオス性の検定を行った。特定パラメータ値における Chua 回路からの出力がカオス的であることを示すことができ、サロゲートデータ法を用いたカオス検定は有効であった。

カオス同期化部の状態を暗号鍵として用い、変調部、復調部にカオス分岐を発生させる Chua 回路を用いた秘匿通信システムにおける分岐パラメータの探索にサロゲートデータ法が有効であることが、暗号化・復号の数値実験から確認できた。

参考文献

[1] 合原一幸:カオスセミナー, 海文堂出版, 1994
[2] 潮 俊光:カオス制御, カオス全書 4, 朝倉書店, 1996
[3] 合原一幸, 池口徹, 山田泰司, 小室元政：カオス時系列解析の基礎と応用, 産業図書, 2000