3C-7

統計的解析に基づいた秘匿通信系カオスモデルの設計

清水能理
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。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。カオス状態はその複雑さゆえ高い秘匿性をもつが、人工的にカオスを発振させる電子回路の実装において、システムパラメータの設定法が問題となる。そこで、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の評価を応用したモデル構築法を提案する[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）。カオスは高い秘匿性をもち秘匿通信に応用されるが、カオス発振回路の分岐パラメータ値の設定問題がある。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。カオス分岐はシステムパラメータの変化に従い軌道の位相的性質を変える現象であるが、分岐に基づくパラメータの設定においてカオス窓の問題がある。よって、周期軌道（窓）が発生していないかカオス性の評価が必然となる。

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．ポアンカレ写像

ポアンカレ写像は、あたかも相空間内の軌道をストロボで照射して次元を落として観察するものである。相空間内にポアンカレ切断面（ポアンカレセクション）を設けることによって得られる。ポアンカレセクションは相空間内に描かれたアトラクタの軌道が、相空間内にある切

Design of Chaos Model for Secure Communication System Based on Statistical Analysis
Y. Shimizu
Hachinohe Institute of Technology

断面を通過する時にできる点の集まりで描かれる。

６．提案手法

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分岐パラメータの設定手法について、以下にまとめる。

(1) 発振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。

サロゲート法を適用するには、データサンプリングをする必要がある。サンプリングしたデータは必ずしもカオス性を有していないので改良が必要である。上手くいかない原因としては、サンプリングした実験データの短さに問題があると考える。しかし、データを長くすると、負荷が大きくなり処理が難しくなる。そこで、連続データを離散化するのにポアンカレ写像を用いる。

７．シミュレーション

FT サロゲート法を用いた場合、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。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た。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。

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（分岐パラメータ 0.70）

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に切断結果のポアンカレ写像を示す。

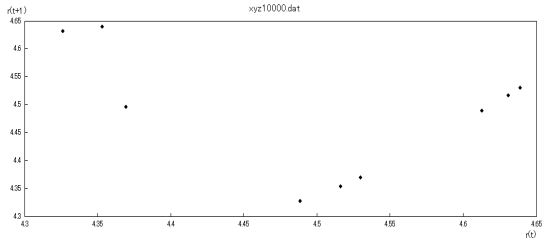

図１　ポアンカレ写像

ポアンカレ写像から得られた離散データを用いてカオス性の検証を行った。非線形統計量としてはリアプノフ指数を用いる。サロゲートデータの特徴量が正規分布すると仮定できる場合、以下の式で定義する検定統計量 S 用いて評価する。Q_H が正規分布するとき、S>1.96 であれば有意水準 α=0.05 で与えられた帰無仮説を棄却することで、カオス性を判定する。

$$S = \frac{|Q_0 - \mu Q_H|}{\sigma Q_H}$$

Q_0：オリジナルデータの非線形統計量

μQ_H：サロゲートデータの非線形統計量

σQ_H：サロゲートデータの非線形統計量標本標準偏差

各サロゲートデータ法における検定統計量 S と検定結果を表２に示す。

表２　検定統計量 S とカオス性の有無

RS	FS	FT	AAFT	IAAFT
0.6210	3.6884	0.2123	0.3350	5.8020
×	○	×	×	○

○：カオス性を示唆　×：カオス性の否定

８．まとめ

カオス分岐図を用いたパラメータ値の時系列信号にサロゲートデータ法を適用し、カオス性の検定を行った。特定値における出力がカオス的であることを示すことができた。サンプリング問題の解決には、ポアンカレの手法を用いた。今後、最適な切断面の設定法について検討する。

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