L-037

オーバーフロー発生の頻度を高めたカオス変調システムの特性評価に関する研究

The Chaotic Modulated System with A High Frequency of Overflow.

佐藤元樹[1]　寺田悠介[1]　田中博紀[1]　鎌田弘之[2]
Motoki SATO,[1]　Yusuke TERADA,[1]　Hiroki TANAKA[1]　and　Hiroyuki KAMATA.[2]

1　はじめに

カオス理論を用いたストリーム暗号は，暗号化・復号化に要する計算量が少ないことから，高速・大容量データを伴うディジタル回路網での秘密通信に有効な手段の一つである．筆者らはこれまで，Chaotic Neuron Type Nonlinearity を用いた秘密通信の変調システムを提案してきた [1][2][3].

カオス変調システムの信頼性を評価する方法として，リアプノフ指数を元にした係数感度に関する検証や，Diehard Test を用いたランダム性に関する検証を実施している [4]．さらに，一般の暗号方式評価の悪条件である，平文，暗号文のペアが明らかになった場合に加え，カオス暗号における内部状態変数をも既知となった場合を想定し，どの程度の時間，計算量で鍵となるパラメータを解析することが可能かを算出したところ，わずか数秒で解析されてしまう可能性があることを示した [5]．このカオス暗号を解析する方法は，固定小数点演算におけるオーバーフローの起きていない点を複数個集め，行列計算を解くものであり，非オーバーフロー点の発生頻度の高いカオス変調システムでは鍵となるパラメータを解析され易いことが明らかとなった.

本研究では，筆者らの提案した，非オーバーフロー点を突く解析アルゴリズムを想定したカオス変調システムの提案を行い，暗号強度，係数感度，ランダム性など複数の面から特性評価を行う.

2　カオス変調システム

本研究では Chaotic Neuron Type Nonlinearity に Volterra Filter を組み込むことにより構成された従来法と，オーバーフロー発生の頻度を高める為に計算方法を符号なし型へと変更したカオス変調システムの提案法との２つのカオス変調システムについて特性評価を行う．以下では単に「従来法」,「提案法」と呼ぶこととする.

[1]明治大学大学院理工学研究科電気工学専攻　博士前期課程
[2]明治大学理工学部電気電子生命学科　教授
〒 214-8571
神奈川県川崎市多摩区東三田 1-1-1

2.1　従来法

従来法の変復調は以下の式で行われる.

・変調式

$$\begin{aligned} x_1(n) &= s(n) + g\{x_1(n-1)\} \\ &\quad + \alpha x_3(n-1) + \theta \qquad (1) \\ x_2(n) &= h_0 + \sum_{i=1}^{3} h_i x_i(n-1) \\ &\quad + \sum_{i=1}^{3}\sum_{i=1}^{3} h_{ij} x_i(n-1) x_j(n-1) \\ &\quad + h_{123} \prod_{i=1}^{3} x_i(n-1) \qquad (2) \\ x_3(n) &= x_2(n-1) \qquad (3) \end{aligned}$$

・情報伝送式

$$x_4(n) = x_1(n) \qquad (4)$$

・復調式

$$\begin{aligned} r(n) &= x_4(n) + g\{x_4(n-1)\} \\ &\quad - \alpha x_6(n-1) - \theta \qquad (5) \\ x_5(n) &= h_0 + \sum_{i=4}^{6} h_i x_i(n-1) \\ &\quad + \sum_{i=4}^{6}\sum_{i=4}^{6} h_{ij} x_i(n-1) x_j(n-1) \\ &\quad + h_{456} \prod_{i=4}^{6} x_i(n-1) \qquad (6) \\ x_6(n) &= x_5(n-1) \qquad (7) \end{aligned}$$

但し，$h_1 = h_4$，$h_2 = h_5 \ldots h_{123} = h_{456}$

・非線形関数

$$g(x) = \begin{cases} \kappa x - \sigma & : x \geq \epsilon \\ \dfrac{\kappa\epsilon - \sigma}{\epsilon} x & : -\epsilon < x < \epsilon \\ \kappa x + \sigma & : x \leq -\epsilon \end{cases} \qquad (8)$$

$s(n)$ は入力信号，$r(n)$ は出力信号，$x_1(n)$ は暗号文，$x_1(n-1)$〜$x_6(n-1)$ はカオス変調システムにおける内部状態変数であり，$g(x)$ は式 (8) で表される非線形

関数である．鍵となるパラメータは h_0〜h_{123} の 11 個である．計算は下位 10 ビット目に小数点があると仮定する符号付き 16 ビット固定小数点演算で行う．

2.2 提案法

提案法の式自体は従来法と同じであり，計算は下位 10 ビット目に小数点があると仮定する符号なし 16 ビット固定小数点演算で行う．そのため入力信号は原信号を 0〜65535 に入るようにスケールを合わせる必要がある．

3 固定小数点演算

演算手法として一般的なのは，浮動小数点演算であるが，DSP（Digital Signal Processor）のような超高速演算機器のメリットを想定して，本研究では従来より，固定小数点演算を採用している．固定小数点演算は，演算途中でオーバーフローが発生し正確な演算の妨げになる場合があるが，本研究では，オーバーフローを非線形関数としてシステムに組み込むことを想定することにより，カオスに必要な有界性を実現している．もちろん，浮動小数点演算によってもオーバーフロー関数を変復調式に埋め込み実行することは可能だが，演算量が増加し実用的ではない．

固定小数点演算は，下位 n ビット目に小数点が有ると仮定する計算方式である．以下に従来法で使用する符号あり 16 ビット固定小数点演算と，提案法で使用する符号なし 16 ビット固定小数点演算について述べる．

3.1 符号あり 16 ビット固定小数点演算

下位 n ビット目に小数点が有ると仮定する 16 ビット固定小数点演算形式を符号あり Q_n フォーマットと呼ぶ．符号あり Q_n フォーマットと浮動小数点型との変換公式は $Q_nA = a * 2^n$ と書くことができる．符号あり Q_n フォーマットでの扱える実数の範囲は $-2^{15-n} \leq A < 2^{15-n}$ である．以下では浮動小数点型 x を符号あり Q_n フォーマットへと変換した記号として $Q_n(x)$ と表すこととする．

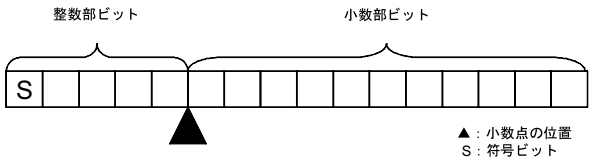

図 1: 符号あり Q_{10} フォーマット

表 1: NOP の存在確率

変調システム	NOP の存在確率 [%]
従来法	1.2982
提案法	0.00002

3.2 符号なし 16 ビット固定小数点演算

下位 n ビット目に小数点が有ると仮定する符号なし 16 ビット固定小数点演算形式を符号なし Q_n フォーマットと呼ぶ．符号なし Q_n フォーマットと浮動小数点型との変換公式は事前にスケールを合わせる必要があるものの，符号ありのそれと同じである．符号なし Q_n フォーマットでの扱える実数の範囲は $0 \leq A < 2^{16-n}$ である．

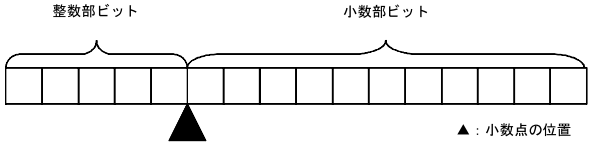

図 2: 符号なし Q_{10} フォーマット

4 非オーバーフロー点の存在確率

前章でも述べたとおり，筆者らの提案したパラメータ解析のアルゴリズムはオーバーフロー回数の少ない点を狙って解析していく手法である [5]．そこでカオス変調システムの新たな評価方法として，非オーバーフロー点 (non-Overflow Point:NOP) の存在確率を提案する．これは N サンプル中にオーバーフロー回数が 0 回となる点がどれだけあるのかを算出し，評価する方法である．いま，N サンプル中に n サンプル，オーバーフローが 0 回である点があったとすると非オーバーフロー点の存在確率 P を

$$P = \frac{n}{N} * 100[\%] \tag{9}$$

で定義する．

本研究では従来法，提案法の第 2 式のオーバーフロー回数が 0 である点を比較した．パラメータはランダムとし，計 $2GB$ 分のデータを暗号化した際の NOP の数から存在確率を算出した．表 1 より，提案法は従来法に比べて格段に NOP が減っていることがわかる．これは，計算方法を符号ありから符号なしへと変えたことにより，減算がなくなりオーバーフローが起きやすくなった為である．NOP を突く解析アルゴリズムにとって NOP が減少したことは提案法が従来法よりもパラメータ解析されにくいことを示している．

表 2: Diehard Test の結果

変調システム	Diehard Test の合格率 [%]
従来法	64.6
提案法	67.8
RC4	69.0

5 特性評価

5.1 Diehard Test

Diehard Test を用いてランダム性の検証を行った．Diehard Test では 18 種類の乱数テストを行い，これらのすべてに合格したものをランダム性があると見なす．従来法と提案法，比較対象として既存のストリーム暗号である RC4 の Diehard Test の結果を表 2 に示す．パラメータはすべてランダムとし，正弦波を入力した時の 1000 回の平均を結果とした．わずかではあるが提案法が従来法よりもランダム性が高いことがわかる．しかし，RC4 と比べるとやや劣っており，ランダム性の向上が今後の課題の 1 つとなる．

5.2 リアプノフ指数

Lyapunov 指数はカオスの定量的指標であり，最大 Lyapunov 指数が正の場合は系がカオス的であることを示す．カオス変調システムのヤコビ行列は式 (10) と表される．

$$\begin{pmatrix} \frac{\partial}{\partial x} g\left(x_1\left(n\right)\right) & 0 & \alpha \\ J_{21} & J_{22} & J_{23} \\ 0 & 1 & 0 \end{pmatrix} \tag{10}$$

ここで J_{21}, J_{22}, J_{23} はそれぞれ式 (11)〜式 (13) となる．

$$\begin{aligned} J_{21} &= h_1 + 2h_{11}x_1\left(n\right) + \left(h_{12}+h_{21}\right)x_2\left(n\right) \\ &+ \left(h_{13}+h_{31}\right)x_3\left(n\right) + h_{123}x_2\left(n\right)x_3\left(n\right) \qquad (11) \\ J_{22} &= h_2 + 2h_{22}x_2\left(n\right) + \left(h_{12}+h_{21}\right)x_1\left(n\right) \\ &+ \left(h_{23}+h_{32}\right)x_3\left(n\right) + h_{123}x_1\left(n\right)x_3\left(n\right) \qquad (12) \\ J_{23} &= h_3 + 2h_{33}x_3\left(n\right) + \left(h_{13}+h_{31}\right)x_1\left(n\right) \\ &+ \left(h_{23}+h_{32}\right)x_2\left(n\right) + h_{123}x_1\left(n\right)x_2\left(n\right) \qquad (13) \end{aligned}$$

図 3〜8 に従来法，提案法のヤコビ行列から求めた Lyapnov 指数を示す．従来法では h_2, h_3 を -32〜32 まで，提案法では h_2, h_3 を 0〜64 まで 1 ポイントずつ動かし，それ以外のパラメータは 1.0 で固定した．従来法，提案法共に，0 近傍では Lyapnov 指数が低くなる．しかし，パラメータの値が大きくなるにつれて提案法が従来法を上まっていくことがわかり，提案法は従来法よりもカオスの特徴である軌道不安定性が増加している．この特性は，パラメータや内部場やイ変数の微妙な差がすばやく拡大することを意味し，クラッキングに対する耐性が強いことを示している．

5.3 暗号鍵の有効ビット数

本研究でのカオス変調システムでは h_0 や h_1 などのパラメータを鍵として扱う．変調時とは異なるパラメータを用いて完全な復調ができてしまっては，暗号システムとしての役割を果たさなくなってしまう．そこで，パラメータが鍵としてどの程度有効かを判断する指標としてパラメータミスマッチングによる係数感度を導入し，以後では単に係数感度と呼ぶ．感度係数より変調式の鍵の総ビット数を算出し，評価する．

検証は，各パラメータを取り得る全ての値で復調し，入力信号との誤差を求めることにより行う．誤差を求めるには，次の式を使用する．

$$D = -\frac{1}{L}\sum_{t=0}^{L-1}\left|u\left(t\right) - s\left(t\right)\right| \tag{14}$$

ここで，$u\left(t\right)$ は復調信号，$s\left(t\right)$ は入力信号とする．L は検証に用いたサンプル数である．D が小さいほど正しく復調できてないことを，$D=0$ となる点で完全に復調できていることを表す．検証の条件として，全てのパラメータを 1.0 とし，1 つのパラメータを 1.1 として復号を行った．また，N は 1024 とした．図 9 より，

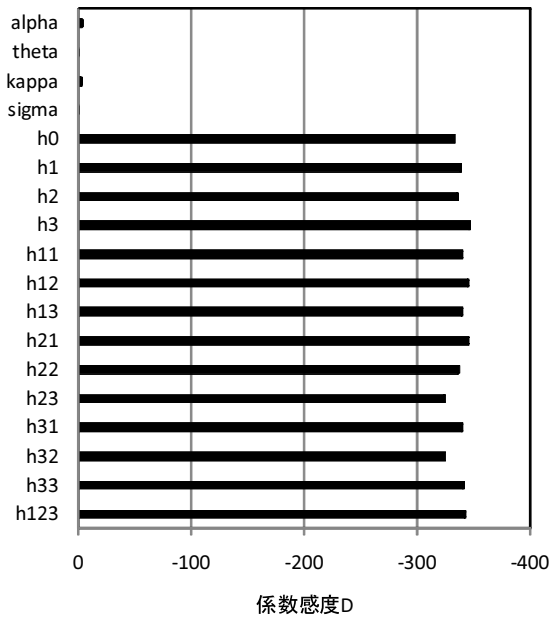

図 9: パラメータミスマッチング

α，θ，κ，σ は鍵として有効ではないことが分かる．鍵 1 つあたり 16 ビットであり，有効数が 11 であったので，提案法での鍵の有効ビット数は 176 ビットとなる．当然であるが，従来法と同値である．これは既存の暗号技術が 128〜256 ビットの暗号鍵長を有していること

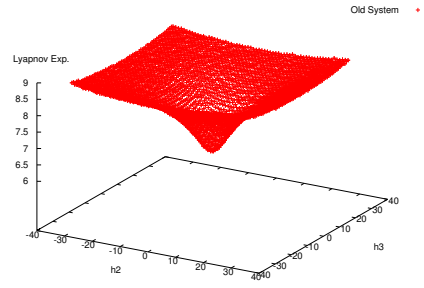

図 3: 第 1Lyapnov 指数 (従来法)

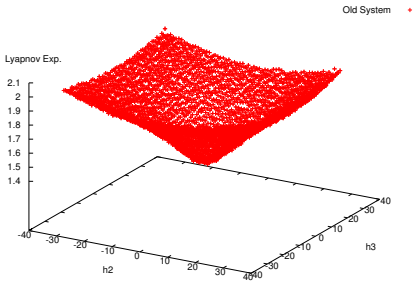

図 4: 第 2Lyapnov 指数 (従来法)

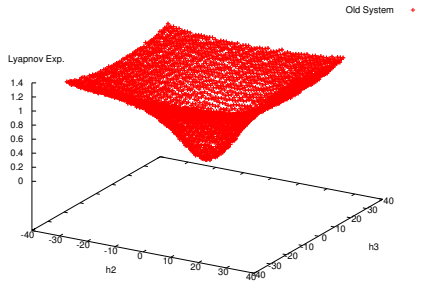

図 5: 第 3Lyapnov 指数 (従来法)

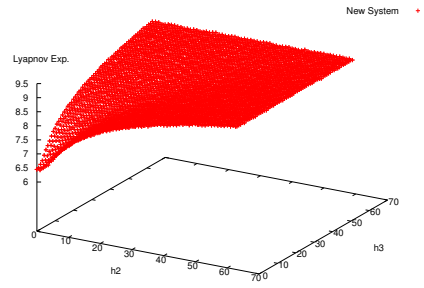

図 6: 第 1Lyapnov 指数 (提案法)

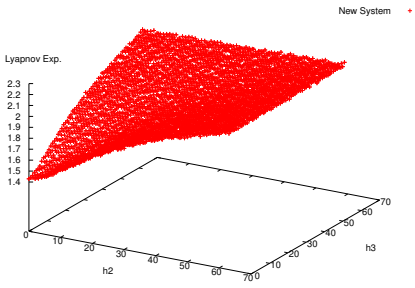

図 7: 第 2Lyapnov 指数 (提案法)

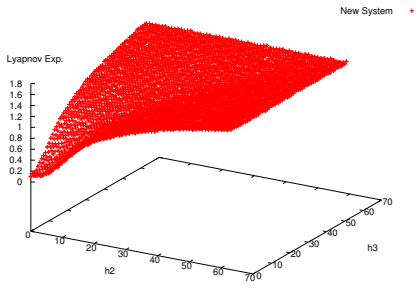

図 8: 第 3Lyapnov 指数 (提案法)

を考慮すると十分な値とは言い難い．しかし，カオス変調システムでは，カスケード接続が可能であり，鍵の有効ビット数は容易に増やすことができる．

6　まとめ

本研究では，符号なし型固定小数点演算によるカオス変調システムの提案を行った．Diehaed Test によるランダム性の評価において，提案法は従来法とそれほど変わらない結果となり，ランダム性が大きく向上したとは言い難かった．さらに既存技術である RC4 と比べてもやや劣る結果となり，ランダム性の向上が今後の課題のうちの 1 つとなる．Lyapnov 指数による評価より，最大 Lyapnov 指数は殆どの場所で従来法を上回り，軌道不安定性が向上している結果となった．NOP の存在確率による検証では，従来法に比べて極端に少なく，非オーバーフロー点を突くパラメータ解析アルゴリズムに対しては有効な変調システムであることが示された．

一方で，NOP の存在確率が低いだけであり，大量のデータが入手されてしまった場合にはその中から解析に必要な量の NOP を見つけ出し解析されてしまう可能性もある．つまり，解析しにくくなりはするが解析時間そのものが長くなるわけではない．

また，鍵の有効ビット数は従来法と提案法の共に 176 ビットであり，既存の暗号技術に比べるとやや劣ると言わざる得ないが，カオス変調システムではカスケード接続が可能であるので鍵のビット数を増やすことは容易である．

参考文献

[1] 中村剛 鎌田弘之，”カオティックニューロンによる２進カオス信号の生成とその応用について ”，電子情報通信学会，電子情報通信学会誌 A，Vol.J91-A No.2 pp.202-211，2008.

[2] 阿部幸政 堤清文 鎌田弘之 遠藤哲郎, “ カスケード構造を持った Chaotic Neurons による秘話通信符号化法について ”，電子情報通信学会，2002 年

[3] 入倉，鎌田，”ボルテラフィルタを用いた 2 次カオティックニューロンにより秘密通信について ”，電子情報通信学会ソサエティ大会 A-2-17，2002 年

[4] K. Iwata, T. Nakamura and H. Kamata, “ Chaotic Modulator with Volterra Filter for Cipher ”, IEICE, Proceedings of NOLTA 2007, pp. 216-219, 2007.

[5] 佐藤元樹 鎌田弘之，”カオス暗号の暗号強度検証に関する研究 ”，回路とシステム軽井沢ワークショップ A2-3-3，2009.