計測自動制御学会東北支部第 273 回研究集会(2012. 6. 29)
資料番号 273-4

量子化カオスデータに基づく暗号化・復号および同期通信

Encryption, Decryption and Synchronization Communication Based on Quantized Chaos Data

○清水能理
○Yoshimasa Shimizu

八戸工業大学
Hachinohe Institute of Technology

キーワード: カオス(chaos), 同期化制御(synchronization control), 秘匿通信(secure communication), 量子化(quantization), 暗号(encryption)

連絡先: 〒031-8501 八戸市大字妙字大開 88-1 八戸工業大学工学部システム情報工学科
Tel.: (0178)25- 8135, Fax.: (0178)25-1691, E-mail: shimizu@hi-tech.ac.jp

１．はじめに

近年では、インターネットなどを通じて多種多様な情報がオープンな状態でやり取りされており、これらの情報を保護するための暗号化技術が重要になっている。暗号通信手法の一つとして、カオス同期を用いた秘匿通信法が研究されている。カオス同期を用いた通信では各サブシステムの出力が鍵の役割を果たすが、サブシステムのパラメータが盗まれると暗号を解読される恐れがある。そこで本研究では、カオス同期化制御により各サブシステムで同じカオス乱数を生成し暗号化・復号を行ない、カオス乱数を生成する際のパラメータを逐次的に変化させることで秘匿性を高める手法について提案する。

２．同相変換量子化

カオスデータの中には様々な秘匿性が隠されている。また、あらゆる組合せの多値を内包しており、鍵とコード表のバランスも非常に良い。しかし、カオスは本来、無理数であるからコンピュータの丸め誤差などの影響を受け、真の数を求めることはできない。

そのため、カオスデータに量子化変換を施し、線形データとなるようにする。デジタル変換には式（1）の同相変換量子化を用い、カオスの内部状態をデジタルデータへ変換する。

$$y_{t,n} = \frac{2}{\pi}\arcsin \sqrt{x_t}\cdot 2^n$$
$$Y_{t,n} = \left[\frac{2}{\pi}\arcsin \sqrt{x_t}\cdot 2^n \right] \quad (1)$$

カオスの内部状態は無理数であるが、同相変換量子化して観測すると、有理数で表される時系列としてカオスが観測できる。カオスデータに同相変換量子化を行い、有理数あるいは整数で表される時系列の振る舞いとしてカオスが観測できる。一般にカオスを生成す

る非線形写像に、結果として線形となるような変換が約束されているわけではない。ロジスティック写像に対する同相変換は、特別に都合のいい例である。

$$X_{t,n} = [x_t \cdot 2^n] \qquad (2)$$

無理数である内部状態 x_t を式（2）でそのまま量子化を行ったものと、式（1）で変換してから量子化を行った分布を比較する。量子化分解能n=8とする。

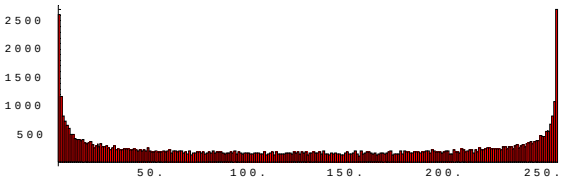

Fig. 1　内部状態 $X_{t,8}=[x_t 2^8]$ の度数分布

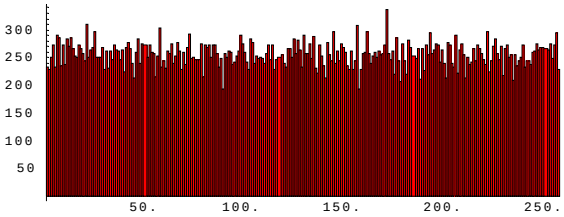

Fig. 2　式（1）を用いて同相変換量子化をした $Y_{t,8}$ の度数分布

Fig. 1 のは両端にデータが鋭く片寄っている。一方、図2はほぼ均一な分布となっており、どの量子もほとんど片寄のない埋まり方をしている。すなわち、式（2）の量子化観測は公平とはいえないのに対し、式（1）の同相変量子化は公平であることを示す。グラフの先端のギザギザはカオスの初期値鋭敏性を示しており、初期値の異なるグラフは決して重なり合うことはない。

３．カオス乱数

ある期間で使い捨てられる秘密鍵を生成する際、その都度、全くの無作為に決定することは難しい。このため、乱数を用いて秘密鍵の種とする手法が用いられる。しかし、乱数が規則性を有するとこれを利用し鍵を特定される恐れがあるため、等頻度性・非線形性を持った乱数を使用する必要がある。真の乱数には確率的一様性、不規則性などが求められるが、暗号に用いる乱数は、あるアルゴリズムから生成される擬似乱数が一般的である。しかしこのような擬似乱数はアルゴリズムによる規則性が生じ暗号の安全性を損なう恐れがある。このためより質の高い乱数が必要となり、これを実現するひとつの手段としてカオス理論を用いたカオス乱数が挙げられる。ロジスティック写像 $L(x_n)$ を

$$L(x_m) = ax_m(1-x_m) \qquad (3)$$

とすると、ある時刻において極めて近い初期値をそれぞれ与えても、十分に時間がたてばこれらは全く無関係な振る舞いを見せる。この性質はカオスの特徴である初期値鋭敏性の表れである。

４．カオス同期化制御

カオス的な振る舞いをする複数のシステムが結合した時に、各時刻でのそれぞれのシステムの状態が等しくなる現象をカオス同期という。結合した個々のシステムの状態の差を抑制させるような条件の下でこのカオス同期化現象は観測される。また，互いのシステムの状態が一致しない非同期状態のカオスに制御を施し、カオス同期を実現させることをカオス同期化制御といい、秘匿通信などへの様々な応用が検討されている。しかし、カオス同期化制御で扱われているのは離散時間系に対してのものがほとんどである。一方、カオス力学系は自然系、人工系を問わず偏在するが、その多くが連続時間系であり離散時間系のものは限られている。そのため連

続時間系に対するカオス同期化制御の確立が必要となる。

平文を暗号化しデータをやり取りする際、送信されたデータを受信側で復号するために付加したカオス乱数を暗号文より取り去る手法がある。このためには、受信側（復号側）にも送信側（暗号化側）と同じ乱数列が必要となる。非線形フィードバック制御の対象として以下のシステムを考える。

$$x(k+1) = f(x(k)) + bu(k) \qquad (4)$$

$$y(k+1) = g(x(k)) \qquad (5)$$

$x(k)$: 制御対象の状態

$u(k)$: 入力

$y(k)$: 出力

このシステムにカオスが存在し、そのアトラクタに埋め込まれたτ周期の周期軌道を $x_p(k)$とおくと、次式を満足する。

$$\begin{aligned} x_p(k+1) &= f\left(x_p(k)\right) \\ x_p(k+\tau) &= x_p(k) \end{aligned} \qquad (6)$$

この周期軌道の安定化を目指すと、式(4)に対して次の非線形状態フィードバック制御を考え、

$$u(k) = h(x(k) - h(x_p(k))) \qquad (7)$$

(h : 非線形関数)

とすれば、このときの閉ループシステムは、

$$x(k+1) = f(x(k)) + B(h(x)) - h(x_p(k))) \qquad (8)$$

となる。簡単のため、

$$(f + Bh)(x) = f(x) + Bh(x) \qquad (9)$$

とする。関数（$f + Bh$）は縮小写像であり、

$$\left\|(f + Bh)(x_1) - (f + Bh)(x_2)\right\| < \beta \left\|x_1 - x_2\right\| \qquad (10)$$

を満たすβが存在すると仮定する。このとき

$$\begin{aligned} \left\|x(k+1) - x_p(k+1)\right\| &= \left\|(f + Bh)(x(k)) - (f + Bh)(x_p(k))\right\| \\ &< \beta \left\|x(k) - x_p(k)\right\| \end{aligned}$$

(11)

となり、0≦β＜1なので、

$$\lim_{k\to\infty} \left\|x(k) - x_p(k)\right\| = 0 \qquad (12)$$

すなわち、$x(k)$ は周期軌道に収束する。式(10)を満たすようなβが存在すれば式（7）の非線形フィードバックによって任意の周期軌道を安定化でき、カオス同期が達成できる。

５．秘匿通信への応用

情報信号をカオス信号に変調して送り、受信側でカオス同期を用いて情報信号を取り出す通信方法はカオス通信と呼ばれる。カオス的に変調された信号から、直接もとの信号を読み取ることは出来ず、システムのパラメータが変わるとカオス同期が達成できなくなるため、送信側と受信側で同じシステムが必要になる。これはつまりカオスシステムのパラメータをKeyとした秘匿通信とみなすことが出来る。

非線形フィードバックによる同期化制御を用いた秘匿通信システムについて述べる。同期化部、変調部、復調部は次式で表される。

同期化部

$$x_i(k+1) = f(x_i(k)) + bu_i(k) \qquad (13)$$

変調部

$$w_i(k+1) = p(x_i(k)), w_i(k), s_i(k+1) \qquad (14)$$

復調部

$$t_i(k+1) = p^{-1}(x_i(k-1), v_i(k-1), v_i(k)) \qquad (15)$$

ただし、$x_i(k)$、$w_i(k)$、$t_i(k)$ はそれぞれ同期化部、変調部、復調部の状態、$u_i(k)$、$v_i(k)$ は、同期化部、復調部への入力信号、$s_i(k)$ は

送信した情報信号 b は、定数ベクトルを表す。

S_1 から S_2 に $C_{12}(k)$、S_1 から S_2 に $C_{21}(k)$ なる信号がやり取りされているとき、送信信号から、直接情報信号 $s_i(k)$ が復元できないようにする必要がある。そのため、$w_i(k), x_i(k)$ が異なる振る舞いをするように写像 p を選ぶ必要がある。制御入力および送信信号としてどのような信号をセットするかは、情報信号を送信する方向に依存する。S_1 から S_2 に情報信号を送ることを考え、以下のように信号をセットする。

$$\begin{aligned} &C_{12}(k) = m_{12}(w_1(k)) \\ &C_{21}(k) = m_{21}(x_2(k)) \\ &u_1(k) = h(m_{21}(x_1(k)) - h(C_{21}(k)) \\ &u_2(k) = 0 \\ &v_1(k) = 0 \\ &v_2(k) = m_{12}{}^{-1}(C_{12}(k)) \end{aligned} \quad (16)$$

このとき、

$$\lim_{k\to\infty}\|x_1(k) - x_2(k)\| = 0 \quad (17)$$

であり、

$$s_1(k+1) = p^{-1}(x_1(k), w_1(k), w_i(k+1)) \quad (18)$$

であることから、

$$\lim_{k\to\infty}|t_2(k+1) - s_1(k)| = 0 \quad (19)$$

となり、情報信号 $s_1(k)$ が $t_2(k+1)$ として、復調されることがわかる。

6．提案

2つのカオス・サブシステムを含む通信システムにおいて、同期化部を式 (20) で表す。

$$x_i(t+1) = f(x_i(t)) + u_i(t) \quad (20)$$

ここで i はシステム 1 ならば 1、システム 2 ならば 2 となる。また、$u_i(t)$ は制御入力で、式（21）を満足するような β $(0 \leqq \beta < 1)$ が存在するように決定する。

$$\|x_1(t+1) - x_2(t+2)\| < \beta\|x_1(t) - x_2(t)\| \quad (21)$$

制御入力 $u_i(t) = 0$ であり、非同期であれば、2 つのサブシステムの差は収束しない。

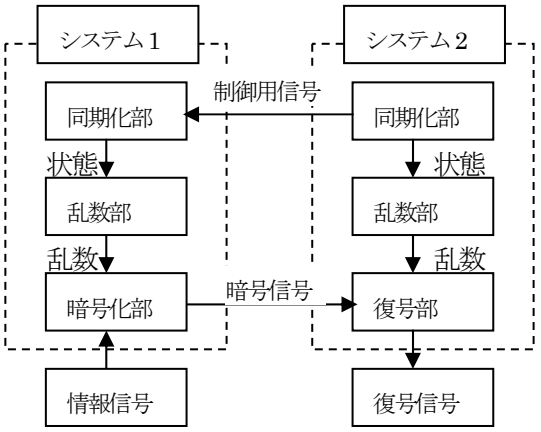

Fig. 3　カオス通信システム

送信側システムＳ１では同期化部・乱数部・暗号化部から成り、受信側システムＳ２では同期化部・乱数部・復号部から成る。各サブシステムの同期化部は同じ動特性を持ち、同期化制御入力がない状態では初期値の違いにより非同期とする。図 3 の S2 の同期化部より、S1 の同期化部に制御用信号を送り、これにより制御入力を決定し、S1 の同期化部に印加する。受信側に送信された暗号信号は復号部にておなじ乱数列を用いて復号される。しかし、システムのパラメータが盗まれると、暗号を解読される恐れがある。これを改善するため、同期化部の状態を用いて乱数部のパラメータおよび初期値を変化させ、秘匿性を高める方法を考えた。これにより、ある瞬間のシステムのパラメータが知られても、次の時刻にはパラメータが変化し、暗号信号を解読される可能性が低くなると考

えられる。

7．シミュレーション

同期化部、乱数部は、以下の式(22)、(24)のように設定し、情報信号として2値の時系列を与えシミュレーションを行った。

同期化部

$$\left.\begin{aligned} x_{1,i}(n+1) &= 1.4 - x_{1,i}^2(n) + 0.3x_{2,i}(n) + u_i(n) \\ x_{2,i}(n+1) &= x_{1,i}(n) \end{aligned}\right\} \quad (22)$$

初期値を次のように与えた。

システム1の初期値

$$x_{11}(0) = 0.1$$
$$x_{21}(0) = 0.1$$

システム2の初期値

$$x_{12}(0) = -0.6$$
$$x_{22}(0) = 0.5$$

制御入力は式（23）を用いた。

$$u_1(n) = x_{11}{}^2(n) - 0.3x_{21} - (x_{12}{}^2 - 0.3x_{22}) \quad (23)$$
$$u_2(n) = 0$$

乱数部

$$\begin{aligned} x_{4,i}(n) &= a(n)x_{3,i}(n)(1 - x_{3,i}(n)) \\ a(n) &= 3.6 + \left|\frac{x_{1,i}(n)}{6}\right| \\ x_{3,i}(n) &= \left|\frac{x_{1,i}(n)}{1.8}\right| \end{aligned} \quad (24)$$

式（24）がカオス的振る舞いをするために、パラメータ $a(n)$ は4.0で設定した。生成されたカオス乱数を、式(1)より分解能 n=1 として量子化し、情報信号との EXOR を用いて暗号化した。

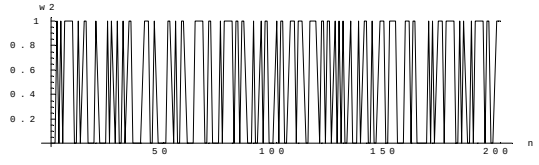

Fig.4　暗号化された信号

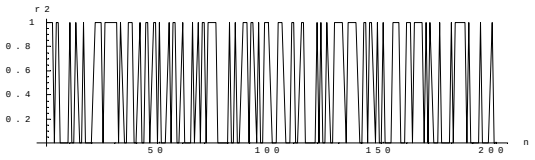

Fig. 5　復号信号

8．おわりに

同相変換量子化を用いて量子化したカオスデータをデジタル通信システムに応用した。量子化データは均一な分布となっており、片寄りは見られなかった。時系列の異なる場所の分布も異なっていることから、同相変換量子化を行った後もカオス性を失っていないことが分かった。非線形フィードバックを同期化制御に用いた秘匿通信システムを提案し、シミュレーションを行った。乱数部より生成されたカオス乱数を量子化し、暗号化・復号に用いた。

参考文献

1) 庄野 克房：カオスエンジニアリング，シュプリンガー・フェラアーク東京 (2002)
2) 鈴木 昱雄：カオス入門，コロナ社 (2000)
3) 合原 一幸：カオスセミナー，海文堂出版 (1994)
4) 潮 俊光：カオス同期化制御とその秘匿通信への応用，情報処理学会論文誌，36-3，525/530 (1995)