カオス暗号方式／認証方式

Encryption/Decryption Method and Cirtification Method Using Chaos

奥富　秀俊

Hidetoshi OKUTOMI

東芝情報システム株式会社　技術企画部（〒210-8540 神奈川県川崎市川崎区日進町７番地１
川崎日進町ビル　E-mail : okutomi@tjsys.co.jp（会社），okutoma@okutoma.ne.jp（自宅））

ABSTRUCT. A proposal of application of Chaos pseudo random number generation technique and stream cipher and certification method performed only by integer arithmetic and bit calculation, which integer arithmetic extended design is adopted in Chaotic Return Maps. Since FPU is not used when Chaos generates, arithmetic compatibility is completed without special process. These give fast, light and long cycle by periodic parameter variation and parameter variation pattern uses infinite time development direction as enormous long key.

１．背　景

安全な電子社会，電子政府の運用において情報セキュリティは不可欠な基盤技術である．中でも機密情報の「守秘」，個人や端末の「識別／認証」といった要素は暗号化技術より支えられる．また，一般的に「守秘」と「認証」はそれぞれ異なる数論を根拠とする背景より異なる方式として提供されている．

昨今のコンピュータの目覚しい進歩を背景に，暗号化技術は一層の複雑強固性が求められている．一方，ブロードバンド時代には高速性が必要であり，また，ユビキタス環境の重要インフラである携帯端末，情報家電，ＩＣカード等への実装には軽量性が欠かせない．複雑性と高速軽量性といった相反する要素の解決が課題である．

一般的に「認証」機能を提供する公開鍵暗号方式は，今後さらに鍵長増加が必要とされており剰余算用特殊コプロセッサ類が必要と言われている．ユビキタスな小規模システムへの展開にはコスト面を始めいくつかの難点が挙げられる．

２．目　的

本研究の目的は，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利用し，高速軽量性と複雑性を実現する暗号方式／認証方式の設計と試作である．また，本研究の最大の特徴ともいえる目的は以下である．

（１）汎用性の追求

カオスを用いたアプローチは既にいくつか提案，実用化がされているが，いずれもカオス算出として常識的な高精度浮動小数点演算が前提であると思える．この場合，カオスは異なるプロセッサ機種間の僅かな演算特性差にまで敏感に反応するためアルゴリズム内で演算互換性が完結できない．そこで異機種エミュレーション，その他の外的対策が必要となる．また，数値演算コプロセッサを持たないシステムへの応用ができないなど根本的に汎用性に関する問題があった．写像系カオスの幾何学構造は整数演算範囲拡大体を考えた場合でも原理的に保たれる点に着目し，全処理過程を整数演算，ビット演算のみで構成する方向性を与え，プロセッサ非依存～将来的に容易な電子回路化など高い汎用性の実現が目的である．

（２）識別／認証応用

カオス暗号方式に共通する点は，カオスを擬似乱数生成手法として利用し，擬似乱数式ストリーム暗号（「守秘」）を構成する点である．本研究では新たにカオス乱波形を鍵固有の「識別信号」と解釈し，正しい鍵の所有者を識別／認証する手法としての利用を考えた．そこで「守秘」と「認証」機能を同時提供する方式の構築が目的である．

３．整数演算型カオス擬似乱数生成部

（１）整数演算に適した写像関数の設計

代表的なロジスティック写像のカオスは，

$$x = a\ x\ (1 - x) \qquad (1)$$

として与えられ x の単純反復構造（図１）である．また，写像範囲は[0, 1]である．ここでパラメータ a の僅かな違いによる軌道差を見てみると図２であり，倍精度浮動小数点演算で表現し得る仮数部最小桁にまで及ぶ．ただし，a の取り方は x が周期解とならない値を選ぶ必要があり，視覚的に見ると図３で示す範囲に制限される．図３は分岐図と呼ばれ，横軸パラメータ a に対し，縦軸方向に複数点プロットされている領域がカオスを示す．

一方，ロジスティック写像を単純拡大し（横軸方向に 2^16 倍），かつ整数演算，小数点以下切捨てを行った場合

の分岐図は図４である．図３，図４を比較し，整数演算化でも「カオス性」は確認できることがわかる．

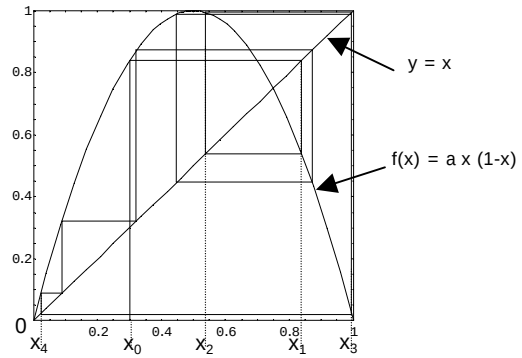

図１　ロジスティック写像のカオス発生構造

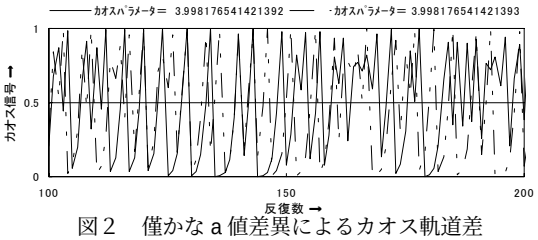

図２　僅かなａ値差異によるカオス軌道差

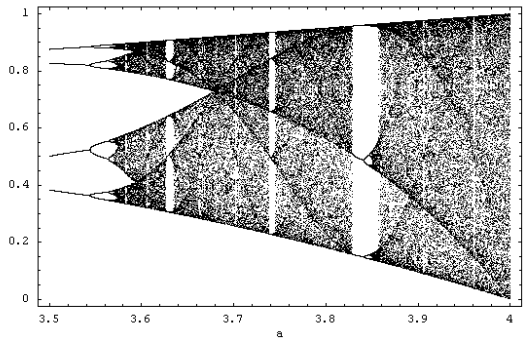

図３　ﾛｼﾞｽﾃｨｯｸ写像分岐図

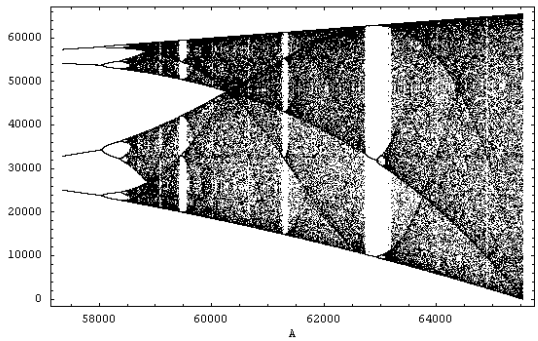

図４　ﾛｼﾞｽﾃｨｯｸ写像（整数演算化）分岐図

このような整数演算化では，扱える状態総数が非常に小さく，また，小数点以下切捨てによる軌道縮退などから短周期性を招く．ここでは定期的にパラメータａを変化させる方向性による対策を与えるが，図３，図４のようにロジスティック写像では多数の周期領域（窓）が存在するため，あらかじめａの有効範囲をテーブルとして持たせておく必要がある．また，パラメータ変動方式はシンプルにしたいため，なるべく連続した広いカオス領域が望ましい．　そこで，ロジスティック写像から方程式の傾きの絶対値が１以下となるなる部分を取り除き，写像の中心で張り合わせた関数形　（図５）を選ぶことで連続したカオス領域が確認できる（図６）．

次に具体的な関数形を示す．まず，２次の関数基本形を(2)とおくことにする．

f(x) = a x^2 + b x + c　　(2)

ここで，写像範囲を 0＜x＜2M（M は整数値）とし，特に右側関数（M＜x＜2M）は，x=2M－x の変換後左側関数（0＜x＜M）と同様に扱えるので左側関数のみを考える．また，上に凸の２次関数を選ぶこととし，極値を(3)～(5)と表すと，関数条件は(6)～(8)である．

f(M) = H （最大値）　(3)
f(0) = 0 （最小値）　(4)
f'(M) = r（最大値での傾き）　(5)
H ＜ 2M （写像の上限条件）　(6)
1 ＜ r ＜ 2（傾き r の条件）　(7)
a ＜ 0（上に凸の条件）　(8)

特に r = R / M（R は整数値）として，これらを a，b，c について整理すると以下となる．

a = -(H - R) / M^2　(9)
b = (2H - R) / M　(10)
c = 0　(11)
M ＜ R ＜ H ＜ 2M　(12)

ここで，R，H の２変数が(12)を満たす範囲で選択できる，さらに左右の関数形を独立して考える場合は４変数として扱える．尚，計算過程で(2)，(9)より M の３乗のオーダを扱う部分があるため，32-bit プロセッサで直接演算可能な範囲は M＜210 に限られる，本件などではより多くの関数形が欲しいので M～215 程度を考えるなどでは分割計算が必要となる．特に M=2^K（2 のべき乗）とした場合，(9)，(10)の除算は K ビット右シフトで代用できる．以上より分割整理した関数処理は(13)となる．

```
x = 2M - x　（x＞M のとき）
b1 = (x^2) >> K
b2 = (x^2) & (M-1)
d1 = ((H - R) b2) >> K
sss = (2H - R) x - (H - R) b1 - d1
x = sss >> K　　(13)
```
（& はビットごとの AND，>>は右ビットシフト）

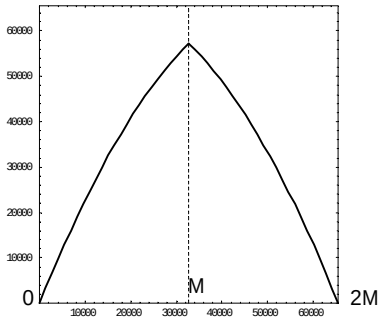

図５　２次の整数演算化設計写像

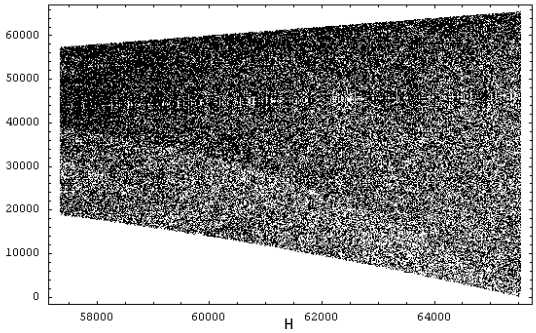

図６　２次の整数演算化設計写像　分岐図

これまではロジスティック写像を変形した２次関数について考えたが，１次関数であるテント写像を考えた場合，M～215 程度ならば 32-bit プロセッサで直接演算可能である．パラメータ数の増加を考慮し図７のような変形を考える．特に傾きを A/M（＜2）として，ここでも右側関数は x=2M－x の変換後左側関数（0＜x＜M）と同様に扱えるので左側関数のみを考えると，(14)，および A,B の条件(15)を得る．

$$f(x) = A/M\ x + B \quad (14)$$
$$f(M) = A + B < 2M \quad (15)$$

また，M=2^K（２のべき乗）としてビット演算を考慮し整理すると，関数処理は(16)となる．(16)は，(13)と比較し非常にシンプルである．

$$x = 2M - x \quad (x>M \text{ のとき})$$
$$x = (A\ x) >> K + B \quad (16)$$

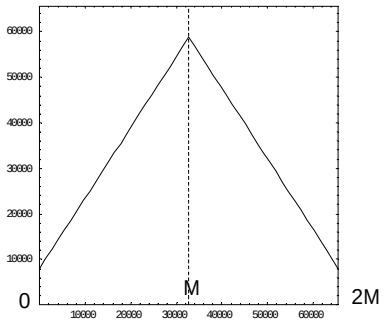

図７　１次の整数演算化設計写像

（２）パラメータ可変関数

パラメータ可変関数は（１）節で示した整数演算化設計写像でのカオス生成を補助し，全体として長周期化を狙うものである．尚，カオス初期条件敏感性を考えると比較的単純な方式でよいと考えている．以下(α)～(γ)に設計方針を挙げた．

（α）初期パラメータ列は鍵から求める
（β）初期パラメータ列（鍵）のユニーク性を保ちながらパラメータ列に変化を加える
（γ）シンプルであることが望ましい

今回は，PK[]：鍵より与えられる初期パラメータ列，P[]：パラメータ列（逐次変化），MaxP：パラメータの最大値として，PK[]の要素数を N とすると，初期の N-1 番目まで(0≦i＜N)のカオス算出に使われるパラメータ列は(17)とし，N 番目以降，N･j＋i 番目は(18)変動処理後の値を使うことを考えた．沿え字 j は i について j 回目の可変処理（j≧1）という意味である． 尚，ここでいうパラメータ P とは，(9)～(13)での H，R，(14)～(16)での A，B に相当する．

$$P[i] = PK[i] \quad (17)$$
$$P[N\cdot j+i] = \mathrm{fmod}(P[N\cdot(j-1)+i] + PK[i],\ MaxP) \quad (18)$$
$$0 < PK[i] < MaxP \quad (19)$$
MaxP は素数 (20)

(18)は，PK[]（鍵）の固有性を保ちつつ P[]に変化を与える仕組みであり，P[]は PK[]に固有の変化パターンとなる．特にカオスは僅かな微小差異によって軌道差は広がっていくので，(18)は，カオス初期条件敏感性をさらに補助する効果を与える．そして，間接的にカオス軌道は鍵固有の軌道となることを示唆する．

また，本件での整数演算化設計写像は２or４パラメータを考えているので，それぞれ互いに素で同程度の大きさの MaxP を与えれば，だいたい N×MaxP^2 or N×MaxP^4 のパラメータ組が生成できる．これはパラメータの可変周期長であり，本カオスの周期でもある．例えば，MaxP を 2^12 以上の素数とすると，２パラメータ使用では N×2^24 以上，４パラメータでは N×2^48 以上の周期となる．(N＝鍵長／PK[]のビット数／パラメータ数)．

このように，カオス写像とパラメータ可変関数の併用では，鍵長の増加は初期パラメータ列要素数 N の増加として容易に扱うことができる．また，カオス算出の１サイクル毎に１回のパラメータ変動を与えているので，鍵長を増加させても１サイクル当たりの処理量は不変で，処理速度を落とすことはない．

（３）パラメータ範囲

M=2^15 の場合，(13)式２次の設計写像でのパラメータ H,R の範囲は以下を与えた．

$$61436 \leqq H \leqq 65534 \text{（MaxH=4099）} \quad (21)$$
$$57325 \leqq R \leqq 61435 \text{（MaxR=4111）} \quad (22)$$

MaxH, MaxR は素数である．尚，鍵より与えられる初期パラメータ列 HK[], RK[]は 8-bit とした．２パラメータ使用時では,鍵長 128-bit のとき,HK[],RK[]の要素数 N = 128/8/2 = 8 なので，周期は 8×4099×4111（＞2^27)である．鍵長 4096-bit では周期長 2^32 に到達する．また，４パラメータ使用時は，鍵長 128-bit の場合 N = 128/8/4 = 4 なので周期長は 2^50 である．

次に，(16)式１次の設計写像のパラメータ A,B の範囲は以下とした．

$$57308 \leqq A \leqq 61408 \quad (\mathrm{MaxA}=4099) \tag{23}$$

$$17 \leqq B \leqq 4127 \quad (\mathrm{MaxB}=4111) \tag{24}$$

MaxA, MaxB は素数である．ここでも鍵より与えられる初期パラメータ列 AK[], BK[]は 8-bit とした．周期に関しては先と同様である．

４．暗号方式／認証方式

（1）暗号方式

２章で述べたカオス擬似乱数生成手法を用い，図８のように擬似乱数式ストリーム暗号を構成する．尚，暗号鍵に相当する部分は２章（２）節で述べたパラメータ可変関数にて処理される．パラメータ可変関数は鍵固有のパラメータ変動パターンを与える．

（2）認証方式

本認証方式の根本的な概念は，カオス算出上の初期値とパラメータ（＝認証鍵）固有のカオス乱軌道（＝認証子）を，正しい初期値とパラメータ（＝認証鍵）の所有者を識別する手段としての利用を考えるものである．認証子生成構造は図９に示した．

従って認証鍵を共通鍵とする共通鍵方式の認証を構成するが，認証サーバ（認証側）が認証毎に異なる乱数鍵を供与し，端末（被認証側）が乱数鍵と，あらかじめ端末に組みこまれている端末固有鍵を組み合わせ認証鍵とすることで，認証毎に全く異なるカオス乱軌道（＝認証子）を交換するチャレンジレスポンス型ワンタイム認証を構成する．基本認証手続きは図１０に示した．

特徴として，２章（２）節後半に記したように，本カオス生成コア部の処理速度は鍵長に依存しないため，考え得る多大鍵長を扱える点である．また，図８，図９のように，暗号方式と認証方式ではカオス生成コア部が共有できることより全体的な軽量化が望める．

また，公開鍵型暗号を用いた認証との相違点は，認証毎に端末⇔認証サーバ間で異なるカオス乱軌道（＝認証子）を交換するワンタイム認証を提供する点である．公開鍵暗号での認証は，認証時に認証サーバは関与せず，一定期間同一の証明書を用いる点と異なる性格を持つ．

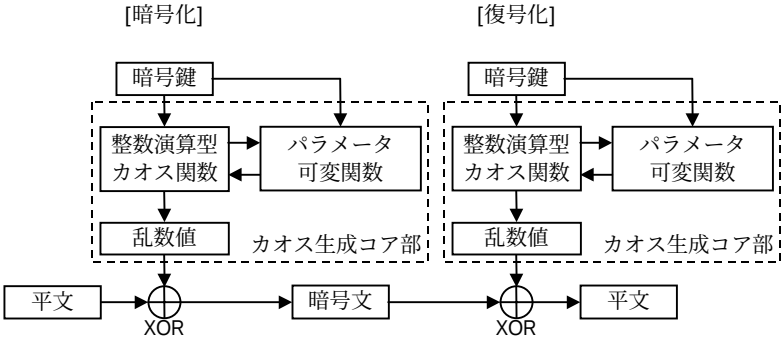

図８　暗号化構造

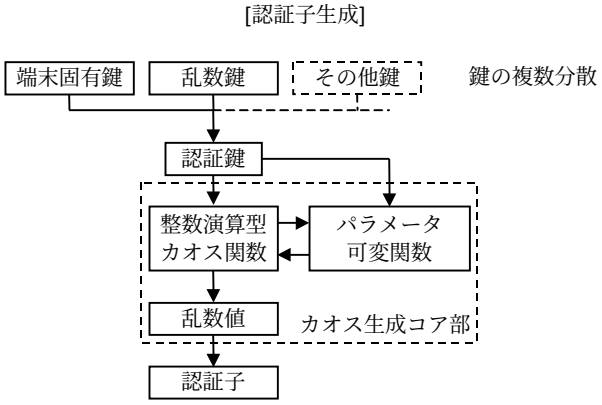

図９　認証子生成構造

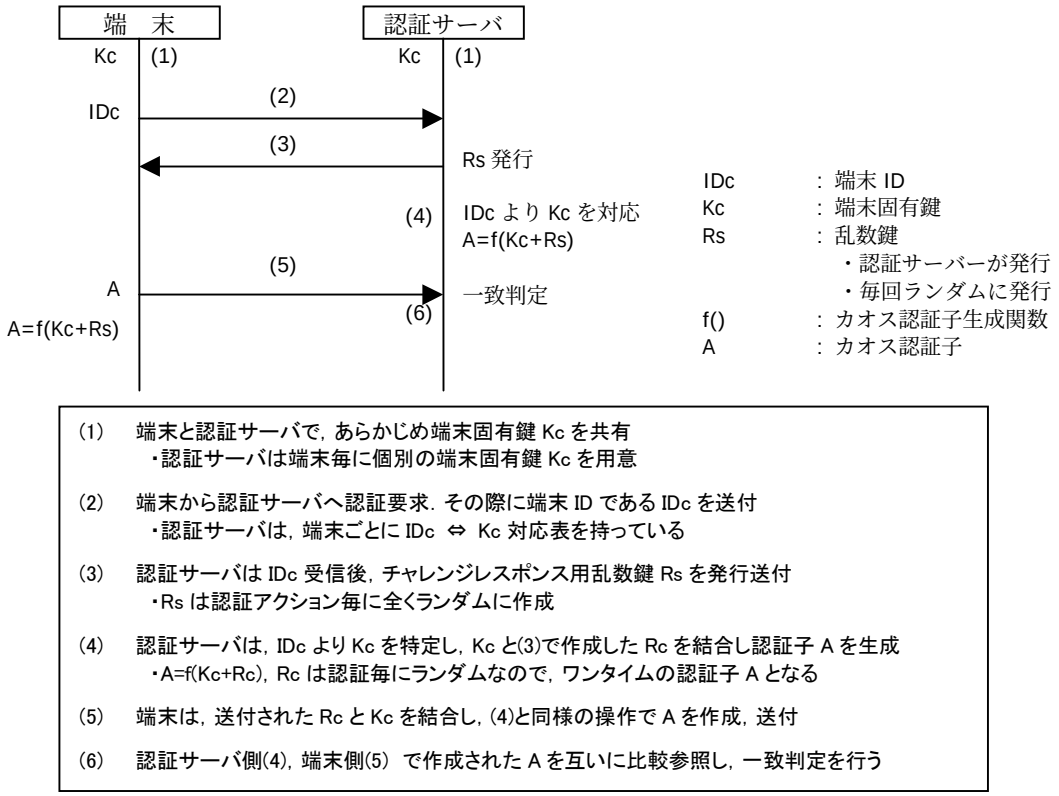

図１０　基本認証手続き

５．検　証

（1）統計的乱数検定

暗号方式および認証方式で共有するカオス擬似乱数生成部の乱数検定を行った．尚，ここでは特にシンプルで高速性が期待できる１次関数系（変形テント写像系，(14)～(16)式，(23),(24)式）についてのみ掲載する．比較的複雑な２次関数系（変形ロジスティック写像系，(9)～(13)式，(21)，(22)式）については文献[13][15]を参照されたい．

今回は検定手法として以下８手法について行った．

(A) 等頻度検定
(B) 等頻度検定（Kolmogolov-Smirnov 検定）
(C) ポーカー検定
(D) 上昇連下降連検定
(E) 間隔検定
(F) 順列検定
(G) 最大値検定（Kolmogolov-Smirnov 検定）
(H) 札集め検定

これら詳細については参考文献[1][2][3]に委ねるが，(A)，(C)～(F)，(H)については観測データと各検定手法の理論分布に対するχ２乗検定である．また，(B)，(G)は Kolmogolov-Smirnov 検定（以下 KS 検定）である．

χ２乗検定は離散化されたクラスを用いて各クラスの度数を見るという離散データに対する手法であるが，KS 検定は連続データ，もしくは意図する確率分布が連続分布と考えたほうが有効な場合に適用する．しかし観測データのソーティングが必要なため，あまり大きすぎる母数（観測データ量）については効率的でない．

また，(A)～(H)の全てについて，統計的検定手法の慣例である 5%ポイント点，1%ポイント点を対象とした．

その他条件として，

試行鍵長　　：512-bit，2048-bit，8192-bit　３通り
観測データ数：2^12，2^16，2^20　　３通り
試行鍵数　　：2^10，2^12　　２通り

とした．

検定結果は表１～表３に示した．各表内の数値は，それぞれ各検定手法，検定条件で棄却された鍵数の全試行鍵数に対する割合（%表示）を示している．これら総合的に見ると，全検定手法，検定条件についても，それぞれが属する棄却率にて棄却された鍵の割合（表内の数値）は，それぞれの棄却率にほぼ等しいと判断できる．つまり，本カオス擬似乱数生成部は，ほぼ理論分布通りの擬似乱数性を有すると言える．

表１　鍵長 512-bit の乱数検定

データ長			2^12		2^16		2^20	
試行鍵数			2^10	2^12	2^10	2^12	2^10	2^12
(A) 等頻度検定		棄却率5%	4.69	4.69	5.66	5.03	4.00	5.27
		棄却率1%	1.07	1.12	0.68	0.93	0.98	1.22
(B) 等頻度検定（ＫＳ）	K+	5%	4.00	5.35	4.98	5.37	5.08	5.27
		1%	0.98	1.39	0.98	1.03	1.56	1.32
	K-	5%	4.30	4.54	4.98	4.57	4.88	4.79
		1%	0.88	1.03	1.07	0.85	0.78	0.76
(C) ポーカー検定		5%	6.05	5.22	4.49	5.00	4.69	5.18
		1%	1.46	1.20	0.98	1.25	0.98	1.15
(D) 上昇連・下降連検定	上昇	5%	5.18	5.32	4.10	4.88	4.49	4.79
		1%	1.76	1.64	1.07	1.22	0.59	1.03
	下降	5%	6.64	6.13	5.57	5.32	4.49	4.83
		1%	1.95	2.32	1.27	1.22	0.98	1.03
(E) 間隔検定		5%	5.18	5.18	4.39	4.86	6.15	4.64
		1%	1.17	1.03	0.59	0.98	0.88	0.66
(F) 順列検定		5%	3.81	4.42	4.49	4.54	6.74	5.18
		1%	1.07	1.25	0.98	0.83	1.37	1.22
(G) 最大値検定	K+	5%	6.15	5.03	4.30	5.35	4.88	4.71
		1%	1.17	1.10	1.07	1.05	0.98	1.03
	K-	5%	4.30	4.27	4.00	4.27	5.37	4.74
		1%	0.78	1.00	1.46	0.83	1.07	0.76
(H) 札集め検定		5%	7.13	6.10	4.30	4.39	4.59	4.83
		1%	2.15	1.95	1.46	1.29	1.17	0.85

表２　鍵長 2048-bit の乱数検定

データ長			2^12		2^16		2^20	
試行鍵数			2^10	2^12	2^10	2^12	2^10	2^12
(A) 等頻度検定		棄却率5%	4.49	4.30	4.69	4.88	4.98	4.93
		棄却率1%	0.88	0.88	0.68	0.78	1.07	1.05
(B) 等頻度検定（ＫＳ）	K+	5%	5.08	4.98	4.79	4.91	3.91	4.44
		1%	1.17	1.00	1.17	0.76	1.07	0.85
	K-	5%	4.88	5.13	5.47	5.42	5.57	5.30
		1%	1.07	1.00	1.17	1.05	0.98	0.98
(C) ポーカー検定		5%	5.18	5.52	4.79	4.86	3.71	4.30
		1%	0.98	1.29	0.88	0.93	0.78	0.76
(D) 上昇連・下降連検定	上昇	5%	6.84	6.27	4.00	5.00	5.18	4.96
		1%	1.76	2.00	1.27	1.00	1.27	1.10
	下降	5%	6.25	6.54	3.81	5.25	5.18	4.83
		1%	1.86	1.90	0.78	1.00	1.86	1.17
(E) 間隔検定１		5%	4.39	5.05	4.98	4.98	4.10	4.98
		1%	1.17	1.34	0.98	0.95	0.88	1.20
(F) 順列検定		5%	5.66	4.52	4.20	5.20	4.39	4.96
		1%	1.07	0.81	0.68	1.00	0.59	0.98
(G) 最大値検定	K+	5%	6.25	5.18	4.69	5.20	4.20	4.59
		1%	1.27	1.00	1.17	1.00	0.59	0.76
	K-	5%	4.69	4.39	4.49	4.98	4.98	5.35
		1%	1.07	0.66	1.17	0.85	1.27	1.49
(H) 札集め検定		5%	7.71	6.52	5.47	4.91	4.10	3.91
		1%	3.13	2.78	1.66	1.39	0.49	0.85

表３　鍵長 819-bit の乱数検定

データ長			2^12		2^16		2^20	
試行鍵数			2^10	2^12	2^10	2^12	2^10	2^12
(A) 等頻度検定		棄却率5%	4.98	4.32	4.88	4.98	5.57	4.71
		棄却率1%	1.17	0.95	0.68	0.85	1.95	1.27
(B) 等頻度検定（ＫＳ）	K+	5%	5.86	5.22	4.88	5.10	4.88	5.47
		1%	1.46	1.20	0.68	0.73	1.07	1.05
	K-	5%	4.39	4.10	5.27	5.03	5.18	5.25
		1%	0.98	0.90	1.46	1.12	0.78	0.88
(C) ポーカー検定		5%	4.79	4.59	6.45	5.66	5.08	5.40
		1%	0.78	0.98	1.46	1.17	1.07	1.10
(D) 上昇連・下降連検定	上昇	5%	5.08	5.74	5.57	4.86	5.27	5.27
		1%	1.27	1.68	1.17	1.03	0.98	0.93
	下降	5%	6.35	6.25	4.59	4.96	4.88	4.86
		1%	2.05	2.22	1.27	1.07	1.37	1.03
(E) 間隔検定		5%	5.57	5.66	4.69	4.91	4.49	4.74
		1%	0.78	0.95	0.68	1.17	1.27	0.90
(F) 順列検定		5%	4.10	4.91	4.30	4.59	5.08	4.91
		1%	0.68	0.93	0.49	0.81	1.27	1.22
(G) 最大値検定	K+	5%	6.25	6.10	4.10	5.03	5.57	5.76
		1%	0.98	0.98	0.78	0.88	1.07	1.07
	K-	5%	5.57	4.59	5.96	5.42	5.08	4.88
		1%	1.46	0.83	0.98	1.07	1.27	1.10
(H) 札集め検定		5%	6.74	6.03	4.88	4.96	5.57	4.44
		1%	2.83	2.66	1.66	1.61	0.78	0.81

（２）理論的検証 ～ 軌道拡散

a)-1 リアプノフ指数（Lyapunov exponent）

カオス軌道を特徴付ける統計量的指標の１つとしてリアプノフ指数（Lyapunov expnent）がある．リアプノ指数は隣接軌道の拡散を裏付けるカオスの重要な指標値である．

ある軌道初期値 x_0 と，これに隣接する $x_0+\Delta x$ を出発した軌道は，１回の写像変換後,

$$\left|f(x_0+\Delta x)-f(x_0)\right| = \left|\Delta x\right| e^{\lambda} \tag{a-1}$$

$$e^{\lambda} = \left|\frac{f(x_0+\Delta x)-f(x_0)}{\Delta x}\right| \tag{a-2}$$

$$\lambda = \ln\left|\frac{f(x_0+\Delta x)-f(x_0)}{\Delta x}\right| \tag{a-3}$$

の割合で広がっていく．ここでλ値が Lyapunov 指数である．また(a-3)よりλと軌道拡散の関係は(a-4)である．

$$\begin{aligned} &\lambda > 0 \quad \text{（拡散）} \\ &\lambda = 0 \quad \text{（変化無し）} \\ &\lambda < 0 \quad \text{（収束）} \end{aligned} \tag{a-4}$$

系がカオスならば隣接軌道は拡散される必要があるため，λ＞0 がカオスの条件となる．

実際には，十分大きい反復回数に渡って(a-3)を算出し平均値をλとするので，x_0 の m 回写像を $f^m(x_0)$とすると，

$$\begin{aligned} \lambda &= \lim_{m\to\infty}\frac{1}{m}\lim_{\Delta x\to 0}\ln\left|\frac{f^m(x_0+\Delta x)-f^m(x_0)}{\Delta x}\right| \\ &= \lim_{m\to\infty}\frac{1}{m}\ln\left|\frac{d f^m(x)}{d x}\right|_{x=x_0} \end{aligned} \tag{a-5}$$

となる．
ここで，$x_m = f^m(x_0)$に対する連鎖則(a-6)より，(a-7)なので，(a-5)は(a-8)に整理される．

$$\left.\frac{d f^m(x)}{d x}\right|_{x=x_0} = f'(x_{m-1})\cdot f'(x_{m-2})\cdots f'(x_0) \tag{a-6}$$

$$\begin{aligned} \ln\left|\frac{d f^m(x)}{d x}\right|_{x=x_0} &= \ln\left|f'(x_{m-1})\cdot f'(x_{m-2})\cdots f'(x_0)\right| \\ &= \ln\left|f'(x_{m-1})\right| + \ln\left|f'(x_{m-2})\right| + \cdots \ln\left|f'(x_0)\right| \\ &= \sum_{i=0}^{m-1}\ln\left|f'(x_i)\right| \end{aligned} \tag{a-7}$$

$$\therefore \quad \lambda = \lim_{m\to\infty} \frac{1}{m}\sum_{i=0}^{m-1} \ln\left|f'(x_i)\right| \tag{a-8}$$

(a-8)より，λ値は x_i における写像関数 f の１階微分値 f'（写像の傾き）の連鎖的総和より求められることがわかる．一般的にカオス信号 x_i は分布上偏りが生じるため，１階微分値 f'が x の変数となる場合，つまり，ロジスティック写像のような２次関数以上の場合，x_i の分布を考慮する必要がある．

ここで，x_i の分布関数をρ(x)とすると，(a-8)は(a-9)となる．

$$\lambda = \int \ln\left|f'(x)\right| \rho(x)\, dx \tag{a-9}$$

（ただし，$\int \rho(x)\, dx = 1.0$ ）　（以上，参考文献[5][6]）

a)-2 本暗号化関数のリアプノフ指数

１次写像関数型の関数系は，写像範囲 0＜x＜2M とし，以下である．

$$\text{if}\,(x > M) \quad x = 2M - x \tag{b-1}$$

$$f(x) = \frac{A}{M}x + B \tag{b-2}$$

M = 2^15 = 32768,　57310≦A≦61408 (b-3)

(b-2)は１次関数なので，１次導関数には x の変数を含まないため，(a-8)定義に従う Lyapunov 指数は(b-4)である．

$$\lambda = \ln\left|\frac{A}{M}\right| \tag{b-4}$$

また，本暗号方式では，A はパラメータスケジューリング関数より変動が加わるため，i 番目の A を A[i]と表すと(b-5)である．

$$\lambda = \frac{1}{m}\sum_{i=0}^{m-1} \ln\left|\frac{A[i]}{M}\right| \tag{b-5}$$

A[i]はパラメータスケジューリング関数より与えられ鍵固有の変化パターンとなる．ただし，A[i]変化は，A[i]の全状態値を効率良く巡回する仕組みとしているため，少なくとも A[i]の状態総数，および十分な m 値を考慮した場合では，鍵（鍵により制御されるカオス軌道）に依存せず一定値に収束する．

上記に従い，m=4099（パラメータ A のスケジューリング１周期）とし，(b-3)条件式を考慮し，特に整数演算化を無視した場合について(b-5)を算出すると，

$$\begin{aligned}\lambda &= \frac{1}{m}\sum_{i=0}^{m-1} \ln\left|\frac{A[i]}{M}\right| \\ &= \frac{1}{m}\left\{\ln\frac{A[0]}{M} + \ln\frac{A[1]}{M} + \cdots + \frac{A[m-1]}{M}\right\} \\ &= 0.59395 \quad (>0)\end{aligned} \tag{b-6}$$

となり，(a-4)式カオス拡散条件を満たす．

これより，設計関数の系はカオス拡散条件を満たしており，初期の僅かな軌道差は，写像反復を増加させる毎に指数関数的に広がっていく様子がわかる．尚，(b-6)は，<u>如何なる鍵を用いても拡散の度合いは一定であることを意味する</u>．

次に，パラメータ A を固定した場合での，本設計関数が実際に生成する軌道についてリアプノフ指数の算出を試み理論値(b-4)との比較を行う．ここでは，実軌道に沿ったリアプノフ指数λ_1の計算として以下(b-7)を定義する．

$$\begin{aligned}\lambda &= \frac{1}{m}\sum_{i=1}^{m} \ln\left|\frac{f^i(x_0+1) - f^i(x_0)}{1}\right| \\ &= \frac{1}{m}\ln\left|\frac{f(x_0+1) - f(x_0)}{1}\right| + \cdots + \ln\left|\frac{f(x_{m-1}+1) - f(x_{m-1})}{1}\right|\end{aligned} \tag{b-7}$$

ただし，(a-7)連鎖則を以下として適用

$$\begin{aligned}f^1(x_0) &= f(x_0) = x_1, \\ f^2(x_0) &= f(f(x_0)) = f(x_1) = x_2 \\ f^3(x_0) &= f(f(f(x_0))) = f(x_2) = x_3\end{aligned} \tag{b-8}$$

また，設計関数は各反復サイクル毎に切り捨てられる下位ビット（小数点以下の値）を一時的に記憶させ，次サイクル計算過程に反映される仕組みのため，精度補正に用いられる値（xb）も計算上，有効とさせるべきである．従って(b-7)式の関数 f は，

$$\begin{aligned}f^i(x_0) &= f(x_{i-1}) + xb/M \\ f^i(x_0+1) &= f(x_{i-1}+1) + xb/M + 1\end{aligned} \tag{b-9}$$

のように，各計算サイクル毎に精度補正値 xb/M を加え算出した．計算量は，各 A 値について 16384 個の初期値が生成する軌道×それぞれ 64 回の反復とした．

演算結果は <u>1.0E-10 以下の誤差（32-bit 演算精度（1/32-bit = 2.32E-10 以下の誤差））で理論値と一致しており，正のリアプノフ指数値を得ることが判った．つまり，設計関数はカオス条件(a-4)を満たしている．</u>

上記より，ある軌道に近づく隣接軌道は，反復ステップを経ることに互いに指数関数的に拡散されていく様子が

わかる．しかし，本設計関数は整数演算化による切り捨て操作や量子化状態総数が小さい点など，ある時点で軌道が縮退（一致）する場合がある．ただし，本方式は，パラメータを定期的に変動させる仕組み，かつ，鍵固有の変化パターンを行うよう設計されているため，いずれは異なるパラメータ帯を歩む運命にあり，ある時点で一致した軌道は次第に離れていくよう設計されている．

次項にて定量化を試みる．

b)-1 パラメータ A の軌道拡散寄与

a)-1 項，a)-2 項では，設計関数のリアプノフ指数値は正であり，また，実測値は理論値と 1.0E-10 の精度で一致するため，隣接軌道は常に拡散関係を保ちカオス条件を満たすことを示した．また，仮に軌道が一致した場合でも，本方式は鍵固有のパラメータ変化を行う仕組みのため，鍵が異なれば必ず軌道差が生じる仕組みであることを説明した．

ここでは，偶然にも軌道が一致した場合について，異なる鍵により軌道差が生じる仕組みを，パラメータ A について定量化し示す．

設計関数を簡単に(c-1)～(c-3)と表すと，

$$\text{if}\,(x > M)\quad x = 2M - x \tag{c-1}$$

$$f(A,B,x) = \frac{A}{M}x + B \tag{c-2}$$

$$M = 2^{15} = 32768,\quad 57310 \leqq A \leqq 61408 \tag{c-3}$$

パラメータ A, A+1 の最小差異によって与えられる写像関数より制御される２つの軌道を考え，それぞれ初期値 x は２軌道で同一の場合を考えると，１回の写像後の値は(c-4)，(c-5)である．

$$f(A,B,x) = Ax/M+B \tag{c-4}$$
$$f(A+1,B,x) = (A+1)x/M+B \tag{c-5}$$

また，説明上，$Ax = \alpha M + \beta$ とすると，(c-4)，(c-5)はそれぞれ(c-6)，(c-7)であり，

$$f(A,B,x) = \alpha + \beta/M+B = (\alpha+B)+\beta/M \tag{c-6}$$
$$f(A+1,B,x) = (A+1)x/M+B = (\alpha+B)+(\beta+x)/M \tag{c-7}$$
（$0 \leqq \beta < M$）

１回の反復後の両軌道差は

$$\Delta = x/M \tag{c-8}$$

である．

特に(c-7)式の算差$(\beta+x) \geqq M$ のとき，整数値に繰り上げが生じ，

$$f(A+1,B,x) = (A+1)x/M+B = (\alpha+B+1)+\beta'/M \tag{c-9}$$

となり，２軌道間は確実に 1 の軌道差が生じることとなる．この時点では成立確立は 1/2 である．

次に，軌道差(c-8)が決定的な軌道差となるために要する反復数を考える．常に２軌道間は，A，A+1 のパラメータが連続して与えられるとすると，２回目の反復では(c-8)の差異は，(c-10)に拡大される．

$$\Delta_2 = (A/M)(x/M) \tag{c-10}$$

以降 s 回目の反復では，(c-11)のように拡大される．

$$\Delta_s = (A/M)^{s-1}(x/M)\quad (S \geqq 2) \tag{c-11}$$

求めたいのは．算差Δ_s が決定的な軌道差となるための条件(c-12)を満たすために必要な最低反復回数 s である．

$$\Delta_s \geqq 1 \tag{c-12}$$

ここで，拡散に最も遅い条件，x=17，A=A0=57310（A の最小値）として(c-11)を計算し，(c-15)を満たすような s 値を見積もると，

$$s \geqq 15 \tag{c-13}$$

である．つまり，遅くとも 15 回の反復後には確実な軌道差となる．本方式では，(c-6)，(c-7)の算差部の β，$\beta+x$ は一時的に記憶され，次ステップ以降の計算に反映される仕組みのためこの考え方は有効である．

一方，本方式はパラメータを定期変動させ，かつ，パラメータ全領域を効率良く巡回する仕組みのため，平均的条件，x～M/2=16384，A=A0+ΔA/2=59359 として再計算すると，

$$s \geqq 3 \tag{c-14}$$

を得る．これより，

- ある時点で軌道が一致する
- ２軌道間で低拡散係数 A0，A0+1 が連続して与えられる

のような最悪条件下でも，最長 15 回，平均で 3 回の反復後には確実な軌道差となる．尚，上記算出条件が成立するのは，２軌道間でパラメータ B が全て一致し，パラメータ A の差異が常に 1 を連続する場合であり，発生確率は非常に稀である．この条件が成立する回数を w 回とすると，

$$P_w = 1/(4111^w \times (4099/2)^w \times (65535-17)) \tag{c-15}$$

であり，特に w=15(=s)となる確立は $P_{15} = 1/10^{108}$ である．さらに２軌道の一致は，同時刻（計算の同一サイクル）にて生じることと定義すると，発生はさらに稀でありほとんど生じないことを述べておく．

上記より，一度軌道差が生じた場合，a)-1 項，a)-2 項での隣接軌道拡散の説明に帰着でき, 如何なる場合でも必ず軌道差が生じ全体として乱雑性が保てる仕組みと説明できる.

b)-2 **パラメータ B の軌道拡散寄与**

前項同様パラメータ B が軌道差へ与える様子を述べる.

ここでは，パラメータ B，B+1 の最小差異によって与えられる写像関数より制御される２つの軌道を考え, それぞれ初期値 x は２軌道で同一の場合を考えると，１回の写像後の値は(c-16)，(c-17)である.

$$f(A,B,x) = Ax/M+B \quad \text{(c-16)}$$
$$f(A,B+1,x) = Ax/M+B+1 \quad \text{(c-17)}$$

B は軌道差に直結しており，(c-16)，(c-17)より，明らかに 1（1 以上）の軌道差を生じる．一度軌道差が生じた場合，a)-1 項，a)-2 項での隣接軌道拡散の説明に帰着でき，如何なる場合でも必ず軌道差が生じ全体として乱雑性が保てる仕組みと説明できる.

６．まとめ

今回は，カオスの暗号応用，および認証応用について，特にカオス生成コア部を共有し「守秘」と「識別／認証」機能を同時提供する手法について述べた.

また, カオス算出上の常識である浮動小数点演算を用いず, 写像系カオスの２次元幾何学構造を根拠とする整数値拡大体を考え，整数演算，ビット演算のみで構成する手法を与えた．これよりプロセッサ非依存，かつコプロセッサを持たない小規模システムへの応用可能性を示した.

ここで整数演算の不利点対策として起用したパラメータ可変関数は, パラメータ変化の最大周期を擬似乱数周期長として理論値確定し，かつ，パラメータ範囲を効率良く巡回する仕組みを与えたためカオス拡散の度合い（リアプノフ指数）が鍵値に依存せず一定（鍵値による性能差なし）を得るなどの副効果を与えた. 純粋カオスはパラメータによって周期長，リアプノフ指数はバラつく傾向にあり，かつ理論値推定は困難であった. これら定量化は特に暗号応用などでは不可欠である.

一方，検証として８種の統計的乱数検証を行った．また, リアプノフ指数を切り口とする理論検証を行い, 整数演算化を行った場合でもパラメータ可変関数の導入より解決できることを述べた.

今後は，より多角的，かつ大量データに対する統計的検証の充実化と，逆解析困難性の定量化，攻撃法に対する検証，小規模システムへの実装実験等が課題である.

７．参加企業及び機関

・東芝情報システム株式会社
「未踏ソフトウェア創造事業」におけるプロジェクト管理組織としての参加

契約件名：

H12 年度未踏ソフトウェア創造事業：「カオス現象を応用し複合的機能を備えた新暗号アルゴリズムの開発」

H13 年度未踏ソフトウェア創造事業：「カオス暗号＋認証方式での認証局提案とコンテンツ配信，購買応用」

８．参考文献

[1] D.E.Kunuth (1981), Random Numbers / The Art of Computer Programming, Addison Wesley

[2] 伏見正則 (1989), 乱数, 東京大学出版会

[3] william Feller (1957), An Itroduction to Probability and its applications, John Wiley & Sons, Inc.

[4] G.L.Baker. and J.P.Gollub. (1990), *Chaotic Dynamics an Introduction* , Cambridge University Press

[5] 長島弘幸, 馬場良和 (1992), カオス入門, 培風館

[6] 香田徹 (1998), 離散力学計のカオス, コロナ社

[7] Douglas R.Stinson (1995), CRYPTOGRAPHY:Theory and Practice, CRC Press, Inc.

[8] 岡本龍明, 太田和夫, 今井秀樹, 松本 (1995) 暗号・ゼロ知識証明・数論, 共立出版

[9] W.H. Press, B.P. Flannery, S.A. Teukolsky, W.T. Vetterling (1988), Numerical Recipes, Cambridge University Press.

[10] 高宇振 (1995), デジタル式カオス信号による情報の隠蔽・復号化方法および装置, 特開平 7-334081

[11] 香田徹 (1995), 暗号システム, 特開平 9-116533

[12] 日立製作所 (2000), 仕様書 MULTI-S01 暗号, IPA 暗号技術公募に関する「暗号技術仕様書，自己評価書」

[13] 奥富秀俊(2001), H12 年度 IPA 未踏ソフトウェア創造事業成果報告書

[14] 奥富秀俊(2002), H13 年度 IPA 未踏ソフトウェア創造事業成果報告書

[15] 奥富秀俊(2001), 整数演算型カオス写像を用いた擬似乱数発生手法と暗号応用について, CSS2001 予稿集