暗号用乱数列

中村 勝洋，田中 和恵

1. まえがき

“乱数列”は，主に2つの領域において，必要不可欠なものとして利用されている．1つは，解析困難なシステム評価のためのモンテカルロ・シミュレーション用の乱数列として，もう1つは，データの保護あるいは広く認証のための，暗号用の乱数列としてである．

両乱数列に対しては，乱数列を構成する各ディジットの独立性や無相関性あるいは等頻度性注1）などの性質が要求されるが，特に後者の乱数列の場合には，与えられた乱数列の一部から，その乱数列の他の部分が推定しにくいとか，その乱数列の発生機構や内部状態が推定しにくいとかいった性質までも要求される．

本稿では，後者の暗号用の乱数列に焦点をあて，古典的なシフトレジスタ系列から，最新の理論的成果の話題までも含めて，簡単な入門的解説を試みることにする．

2. ストリーム暗号とシフトレジスタ系列

暗号化方式は，ブロック暗号化方式とストリーム暗号化方式に大別される．ブロック暗号は文字どおり，メッセージを一定長のブロックに区切り，各ブロックごとに独立に暗号化を行なって得られるものである．一方，ストリーム暗号は，**図1**に示す方式にしたがって得られる暗号で，メッセージの各シンボル m_j がキーストリームの対応するシンボル k_j に依存して暗号化され，シンボル c_j となる．ここでキーストリーム $\{k_j\}$ は，暗号化鍵 K なるパラメータに依存して生成される．図1(a)では，キーストリーム発生器（乱数列発生器）の内部状態が，送受で同一となるように，外部から同期をとってやるため，外部同期方式と呼び，図1(b)では，送受の内部状態（レジスタの状態）がたとえ途中でくずれても，一定時間後には，同一となって自動的に回復するため，自己同期方式と呼ぶ．

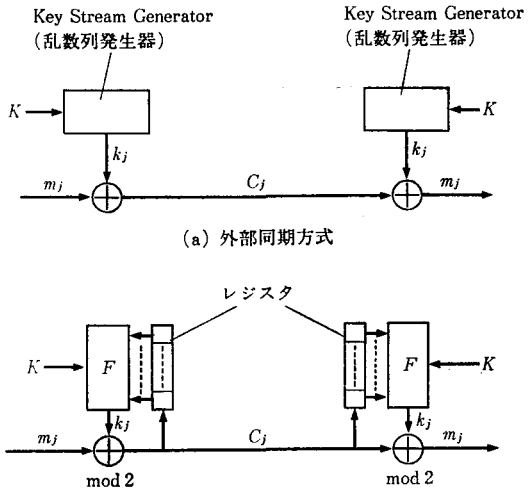

図 1 ストリーム暗号

さて，ここで問題となるのは，キーストリームをいかにして生成するかである．**図2**に示す one-time pad暗号[1]（あるいは，ヴァーナム暗号[2]）では，キーストリーム $\{k_j\}$ を，各ビット k_j が0，1等頻度でかつ独立に生成される非周期的なランダム系列としており，暗号化されるメッセージのビット長とキーストリームのビット長とは等しい．この場合，Shannon[2]が示したように，暗号文のみから，もとのメッセージを知ることは原理的に不可能である．実際，解読者にとっては，暗号文と同じ長さのすべてのビット列がもとのメッセージの候補となることしかわからない．したがって，この暗号方式は，perfect secrecy を与える暗号方式である．

しかしながら，超機密データを扱う場合を除き，実際問題として，メッセージの量と同じ量のキーストリーム

なかむら かつひろ，たなか かずえ
日本電気㈱ C&C情報研究所
〒216 川崎市宮前区宮崎4－1－1

注1）所定の分布にしたがった頻度を持つ系列への変換は容易なので，ここでは等頻度性に限って述べる．

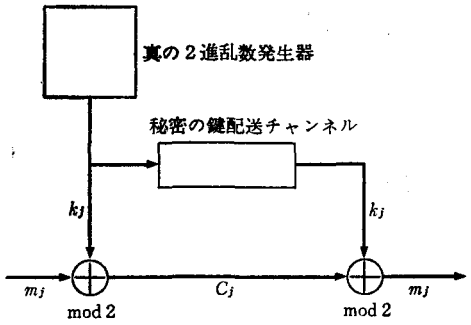

図 2　one-time-pad 暗号

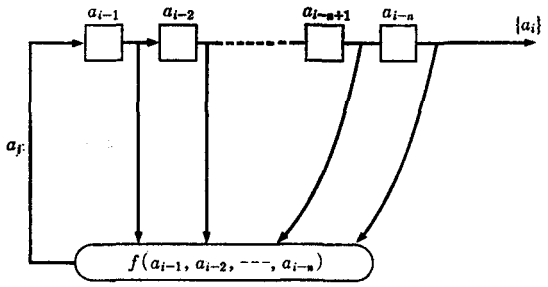

図 3　フィードバック・シフトレジスタ

を別に受信先に送るのは非現実的であり，キーストリームの保管にも問題がある．そこで，見かけ上ランダムなビット列を，適当な長さの種（seed）となるビットパターンから生成していく手法が求められ，ここで，フィードバックシフトレジスタ（Feedback Shift Register; 以後ＦＳＲと略す.）などを使った（擬似）乱数列発生器の利用へとつながるのである．

ＦＳＲの一般的な形を図3に示す．図中の各シンボル a_t は，一般には有限体 GF(q) あるいは整数剰余環 $\mathcal{Z}_q$ の元で，□は，各シンボルを単位時間記憶した後に出力するレジスタである．またフィードバック関数 f は，a_{i-1}, a_{i-2}, …, a_{i-n} の線形あるいは非線形関数である．

古典暗号として有名なヴィジネル暗号[1]やシーザ暗号[1]もよく見れば，$\mathcal{Z}_{26}$の上の最も簡単なFSR系列（この場合f $(a_{i-1}, a_{i-2}, \ldots, a_{i-n}) = a_{i-n}$；特に $n=1$ のときがシーザ暗号）を利用した暗号にほかならない．**図4**にヴィジネル暗号の一例を示す．図において，A～Z のアルファベットは，それぞれ 0～25の数に対応づけられており，演算⊕は，mod 26での加算である．

さて，以下，話の都合上バイナリの（GF(2)上の）ＦＳＲについて考える．n 段のＦＳＲの総数は，2^{2^n} 個であるが，そのうち線形ＦＳＲに限って数えれば，2^n 個ある（$f \equiv 0$ も含む）．したがって，線形 FSR に比べ，非線形 FSR の数は，はるかに多いのであるが，非線形FSR系列よりも線形FSR系列の方が乱数列として解析しやすく，容易に得やすい[3][4]．しかし，暗号用としては，後述するように，解読されやすいため，何らかの非線形性を導入する必要があり，そのため，キーストリーム発生器としては，線形ＦＳＲの部分と，その出力に駆動されて，あるいはその出力に対し，非線形操作・結合を行ないキーストリームを発生させる部分とから成るものを考えることが多い．そこで，本節では，まず基本となる線形ＦＳＲ系列の表わし方や性質について述べる．次節以降では，この乱数性が暗号用としては不十分であることを述べ，線形ＦＳＲ系列に対する非線形操作について検討する．

さて，n 段のレジスタから成る線形ＦＳＲの出力系列，つまり線形ＦＳＲ系列$\{a_t\}$は，次の n 次の線形再帰関係を満たす系列である[5]．

$$a_i = h_1 a_{i-1} + h_2 a_{i-2} + \cdots + h_n a_{i-n} \pmod 2 \qquad (1)$$

（ただし，$h_t=1$ または $0 (j=1 \sim (n-1))$，$h_n=1$；$i=n, n+1, \cdots\cdots$）

(1)式に対し遅延作用素（delay operator）x を適用すれば，系列 $\{a_t\}$ は次式を満たす．

$$(1 - h_1 x - h_2 x - \cdots - h_n x^n)\{a_t\} = 0 \pmod 2 \qquad (2)$$

ここに現われた多項式 $h(x) = 1 - h_1 x - h_2 x - \cdots - h_n x^n$ を，系列 $\{a_t\}$ の**特性多項式**と呼ぶ．

次に $h(x)$ を特性多項式とする FSR 系列 $\{a_t\}$ の表現法として，解析に便利な2通りの方法を記す．

1つは，有理式表現するもので，$A(x) = \sum_{t=0}^{\infty} a_t x^t$ としたとき，$A(x)$は次式で表わされる．ただし，$a_0, a_1, \cdots, a_{n-1}$ は，レジスタの初期値を表わす．

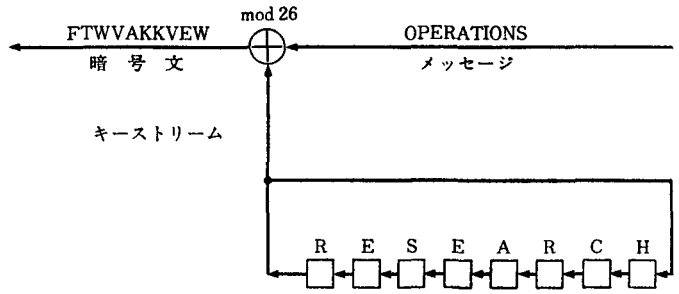

図 4　ヴィジネル暗号の一例

$$A(x)=b(x)/h(x) \tag{3}$$

ただし，

$$b(x)=\sum_{i=0}^{n-1} b_i x^i=\sum_{i=0}^{n-1} a_i x^i+\sum_{j=1}^{n-1}\sum_{k=0}^{n-j-1} h_j a_k x^{j+k} \tag{4}$$

(4)式の関係は，次式のようにも表わせる．

$$\begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix}=\begin{bmatrix} 1 & & 0 \\ h_1 & \ddots & \\ \vdots & \ddots & \\ h_{n-1}\cdots h_1 & & 1 \end{bmatrix}\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \tag{5}$$

(3)式の表現は，いくつかのFSR系列を加算(mod 2)して得られる系列を調べるのに役立つ．

一方，$h(x)$の根を用いて系列$\{a_i\}$を表現する方法もある．$h(x)$の根を$\alpha_0,\alpha_1,\cdots,\alpha_{n-1}$とし，すべて相異なるものとする．また，これらの根のすべてを含む最小の体(つまり，$h(x)$の最小分解体)をGF(2^r)とする．このとき，FSR系列$\{a_i\}$は，

$$a_i=\sum_{j=0}^{n-1} u_j \alpha_j{}^{-i} \tag{6}$$

と表わせる[5]．ただし，$u_0,u_1,\cdots,u_{n-1}$は，初期値$a_0,a_1,\cdots,a_{n-1}$によって一意に定まるGF(2^r)の元である．

特に，$h(x)$が既約多項式のとき，$h(x)$の1つの根をαとすれば他の根は$\alpha^2,\alpha^{2^2},\cdots,\alpha^{2^{n-1}}$となり，最小分解体はGF$(2^n)$である．このとき，FSR系列$\{a_i\}$は，GF$(2^n)$の元$x$をGF(2)の元0または1に写像する線形関数であるトレースTr(x)，

$$\mathrm{Tr}(x)=x+x^2+x^{2^2}+\cdots+x^{2^{n-1}} \tag{7}$$

を用いて，次のように表わせる[13]．

$$a_i=\mathrm{Tr}(B\alpha^{-i}) \tag{8}$$

ここで，BはGF(2^n)の元であり，(3)式で有理式表現された$A(x)$の$x=\alpha$における留数をαで割ったものとなることから，

$$B=b(x)/xh'(x)|_{x=\alpha} \tag{9}$$

ただし，$h'(x)$は$h(x)$の形式的な微分で，たとえば，$h(x)=x^3+x+1$のとき，$h'(x)=3x^2+1=x^2+1$である．(6)あるいは(8)式の表現は，FSR系列同士の積をとって得られる系列などの解析に役立つ．

例 1 $h(x)=1-x^3-x^4$，初期値1,0,0,1のとき，FSR系列$\{a_i\}=100110101111000\cdots$で，系列$\{a_i\}$の周期は15である．また，(3)，(5)式より，$A(x)=\sum_{n=0}^{\infty} a_i x^i=1/h(x)$となる．

一方，(9)式より$B=\alpha^{-3}$であるから，

$a_i=\mathrm{Tr}(\alpha^{-i-3})$ となる □

次に，FSR系列$\{a_i\}$の周期について述べる．任意のiの値に対し，$a_i=a_{i+T}$となる最小のTの値を系列$\{a_i\}$の周期と名づける．任意の非零の周期系列$\{a_i\}$には，次の性質をもつ多項式$h(x)$が存在する[5]．すなわち，系列$\{a_i\}$は，$\tilde{h}(x)$が$h(x)$で割り切れるとき，その時に限り$\tilde{h}(x)\{a_i\}=0$を満足する．このような多項式$h(x)$を，系列$\{a_i\}$の**最小多項式**という．系列$\{a_i\}$の周期は，この最小多項式の**指標**eに等しい，指標eとは，$h(x)$がx^e-1を割り切り，x^v-1 $(0<v<e)$を割り切らないときのeの値のことである．$h(x)$の指標は，$h(x)$の**周期**ともいう．$h(x)$がn次の既約多項式ならば，eは2^n-1の約数であり，特に原始多項式のときは，$e=2^n-1$である．逆にいって，$e=2^n-1$となる多項式のことを**原始多項式**と呼んでいる[6]．一般には，$h(x)$が既約分解されて$h(x)=\prod_i (h_i(x))^{m_i}$となるが，このときの周期は，各既約多項式$h_i(x)$の周期の最小公倍数に$2^j$倍(ただし$2^j$はすべての$m_i$より小さくない最小の整数)した値に等しい[6]．

さて，線形FSR系列$\{a_i\}$の中でも，その特性多項式$h(x)$がn次の原始多項式の場合，n次の多項式の中では最大の周期2^n-1を持つ系列が得られ，この系列のことを特に**M系列**(Maximumlength linear feedback shift register sequence；最大周期系列)と呼んでいる[4]．M系列は，(擬似)乱数としての種々の性質(一様性，無相関性，等)を持ち，さまざまな形で応用されている[4]．(本号の高橋，手塚氏の解説も参照されたい)

3. 線形複雑度と暗号用乱数列の評価基準

線形FSR系列には，良好な乱数性を持つM系列が含まれるが，暗号用乱数としてみれば弱い．特性多項式$h(x)$の次数をnとすれば，$2n$ビットずつの暗号文とメッセージ文との対から，$h(x)$の係数がわかり，解読されてしまう．たとえば，図1(a)におけるキーストリーム発生器として線形FSRを用いた場合，上記$2n$ビットの暗号文とメッセージ文との対から，まず$2n$ビットのキーストリームビット$k_0,k_1,\cdots,k_{2n-1}$がわかる．一方，(1)式から

$$\begin{bmatrix} k_1 & k_2 & \cdots k_n \\ k_2 & k_3 & \cdots k_{n+1} \\ \vdots & \vdots & \vdots \\ k_n & k_{n+1}\cdots & k_{2n-1} \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ & & & 1 & 0 \\ 0 & & \cdots & 0 & 1 \\ h_n & & \cdots & h_2 & h_1 \end{bmatrix} \begin{bmatrix} k_0 & k_1 & \cdots & k_{n-1} \\ k_1 & k_2 & & \vdots \\ \vdots & \vdots & & \vdots \\ k_{n-1} & k_n & \cdots & k_{2n-2} \end{bmatrix} \tag{10}$$

したがって，右辺の k_i を要素とする行列が正則である限り，(10)式は $h_1 \sim h_n$ に関して解くことができ，解読されてしまうことになる．つまり，以後のキーストリーム $\{k_i\}$ がすべてわかってしまう．

そこで，n 次の多項式 $h(x)$ を特性多項式とする線形FSR系列 $\{a_i\}$ に，何がしかの非線形操作をほどこして周期系列 $\{b_i\}$ を得，周期系列 $\{b_i\}$ の最小多項式の次数 l を n に比べてはるかに大きくするといったことが考えられる．前節でも述べたように，任意の周期系列には最小多項式が存在し，その最小多項式を特性多項式とする線形ＦＳＲ系列として，その周期系列をとらえ直すことができる．このとき，その最小多項式の次数 l をその周期系列の**線形複雑度**（linear complexity[7]）と呼ぶ．いいかえれば，その周期系列を生成する最小段数の線形ＦＳＲの段数のことである．周期 $T=2^n-1$ のM系列の線形複雑度は n であり，周期 T の長さに比べて，最も小さい複雑度を持つ．したがって，線形複雑度の観点からいえば，M系列は良い乱数列とはいい難い．ところで，**暗号用乱数列の安全性評価の基準**[10]としては，発生シンボル1，0の等頻度性，系列としての長周期性，無相関性，系列発生の非線形性などがあるが，各発生シンボルが，過去の発生シンボルから原理的にあるいは計算量的に予測不能であるという予測不能性という評価基準もある．これについては5節でさらに詳しく述べる．上記で述べた線形複雑度も1つの評価基準になるが，これは，予測不能性や長周期性，非線形性などの基準ともからみ合った1つの評価基準である．

さて，周期 T の周期系列 $\{b_i\}$ に対する線形複雑度 l は，簡単には次のようにして求めることができる[11]．すなわち，周期系列 $\{b_i\}$ を表わす有理式，$\sum_{i=0}^{T-1} b_i x^i/(1-x^T)$ を約分できるところまで約分した結果を $g(x)/f(x)$ とすれば，$f(x)$ が周期系列 $\{b_i\}$ の最小多項式であり，その次数が線形複雑度となる．一方，任意の系列 $\{b_i\}$ をビットごとに逐次的に処理しながら，系列 $\{b_i\}$ を生成する最小段数のＦＳＲを算出するアルゴリズムも知られている．このアルゴリズムは，誤り訂正符号の分野で，ＢＣＨ符号の復号アルゴリズムの一環として開発されたものであり，**Berlekamp-Masseyアルゴリズム**として広く知られている．系列 $\{a_i\}$ に対し，Berlekamp-Masseyアルゴリズムを適用すると，次のようになる[11]，[16]．

まず，系列 $\{a_i\}_{i=0}^{n-1}$ に対する最小多項式を，

$$C_n(x)=1-C_{n1}x-C_{n2}x^2-\cdots-C_{nln}x^{ln} \tag{11}$$

とする．また，変数 d_n, k_n を

$$d_n=a_n-\sum_{i=1}^{n} C_{ni}a_{n-1} \tag{12}$$

$$k_n=\begin{cases} k_{n-1} & (l_n=l_{n-1}\ \text{のとき}) \\ n-1 & (l_n>l_{n-1}\ \text{のとき}) \end{cases} \tag{13}$$

とする．このとき，

$$C_{n+1}(x)=C_n(x)-\frac{d_n}{d_{kn}}x^{n-kn}C_{kn}(x) \tag{14}$$

$$l_{n+1}=\begin{cases} l_n & (d_n=0\ \text{のとき}) \\ \max\ (l_n, n-(k_n-l_{kn})) & (d_n\neq 0\ \text{のとき}) \end{cases} \tag{15}$$

ただし，初期値として，$C_0(x)=C_{-1}(x)=1$，$l_0=l_{-1}=0$，$k_0=-1$，$d_{-1}=1$ とする．

このアルゴリズムにおいて，l_n が，系列 $\{a_i\}$ の最初の n ビットに対する線形複雑度を与えているわけである．系列 $\{a_i\}$ が，各ビットごとに独立で，0, 1等頻度のランダムな2進乱数列であれば l_n の平均 $E[l_n]$ と分散 $\mathrm{Var}[l_n]$ は，次式で与えられることが知られている[7]．

$$E[l_n]=n/2+(9-(-1)^n)/36-2^{-n}(n/3+2/9) \tag{16}$$

$$\mathrm{Var}[l_n]=86/81-2^{-n}(n/2+(-1)^n n/54 +(-1)^n/81+1) -2^{-2n}(n^2/9+4n/27+4/81) \tag{17}$$

(17)式より，

$$\lim_{n\to\infty}\mathrm{Var}[l_n]=86/81 \tag{18}$$

(16)，(17)式より，真の乱数列の線形複雑度 l_n は，$l_n \simeq n/2$ のラインに添って，分散が約86/81でふらつきながら n とともに増大していくことがわかる．このことは，乱数列の評価基準として利用できる．

一方，周期 2^m あるいは 2^m-1 の2進乱数列に対しては，l_n の値は周期にきわめて近い値となることも知られている[7]．

4. 線形ＦＳＲに対する非線形操作・結合

本節では，1個以上の線形ＦＳＲ系列に対し，非線形操作を加えたり結合したりして得られる系列の性質を，暗号用乱数列の観点から検討する．

まず，同一の線形ＦＳＲから生成される，2つの線形

系列 $\{a_t\}$, $\{b_t\}$ の**積系列** $\{a_t \cdot b_t\}$ を考える[8]. (8)式より，適当な GF(2^n)の元 A, B を用いて，$a_t = \mathrm{Tr}(A\alpha^{-t})$, $b_t = \mathrm{Tr}(B\alpha^{-t})$ とすれば，$a_t \cdot b_t = \sum_{j=0}^{n-1}(A\alpha^{-t})^{2^j} \cdot \sum_{k=0}^{n-1}(B\alpha^{-t})^{2^k} = \sum_{j=0}^{n-1}\sum_{k=0}^{n-1} \cdot A^{2^j}B^{2^k}(\alpha^{2^j+2^k})^{-t}$ となる．$\alpha^{2^j+2^k}$ は，j, k を変化させると ${}_nC_1 + {}_nC_2 = n(n+1)/2$ 通りの元になる．$k \neq j$ のとき，$A^{2^j}B^{2^k} \cdot \alpha^{2^j+2^k} + A^{2^k}B^{2^j} \cdot \alpha^{2^k+2^j}$ が0になり得ないことに注意すれば系列 $\{a_t \cdot b_t\}$ は，$n(n+1)/2$ 個の GF (2^n) の元を用いて表わされる系列となる．つまり，(6)式を考慮すれば積をとることによって，線形複雑度が，n から $n(n+1)/2$ へと増大している．

次に，同様の議論を，同一の線形ＦＳＲから生成される $m\,(\geq 3)$ 個の線形ＦＳＲ系列の積系列に対して行なう[8]．この場合，見かけ上，上と同様の議論で，${}_nN_m = \sum_{i=1}^{m} {}_nC_i$ 個の GF(2^n)の元を用いて表わされる系列となるが，今度の場合，元によっては，その係数が0となる場合もまれに生じ得るので，得られた積系列の線形複雑度は，高々 ${}_nN_m$ である．

次に，n_1 次の多項式 $f_1(x)$, n_2 次の多項式 $f_2(x)$ をそれぞれ特性多項式とする線形ＦＳＲ系列を $\{s_t\}$, $\{v_t\}$ とし，その積系列 $\{r_t\} = \{s_t \cdot v_t\}$ を考える．

$f_1(x)$, $f_2(x)$ が，それぞれ，相異なる根 $w_0, w_1, \cdots, w_{n_1-1}$; $q_0, q_1, \cdots, q_{n_2-1}$ を持つものとすれば，積系列 $\{r_t\}$ は，多項式 $F(x) = \prod_{i=0}^{n_1-1}\prod_{j=0}^{n_2-1}(x - w_i q_j)$ を特性多項式とする線形ＦＳＲ系列である[13]．ただし，$F(x)$は，必ずしも積系列$\{r_t\}$の最小多項式ではない．$f_1(x), f_2(x)$ がともに既約で，n_1 と n_2 とが互いに素ならば，$F(x)$は $n_1 n_2$ 次の既約多項式で，積系列 $\{r_t\}$ の最小多項式となる．したがって，この場合の線形複雑度は $n_1 n_2$ である．

例 2　**図5** (a)はGeffeの乱数列発生器[14]と呼ばれるものである．各線形ＦＳＲ系列に対する特性多項式はすべて既約で，各々の次数 r, s, t は互いに素であるものとすれば，この発生器から出る乱数列の線形複雑度は，上の議論から $sr + (s+1)t$ となる．ここで $(s+1)$となっているのは，反転が，初期状態1の1段の線形ＦＳＲに置き換えられるからである（図5(b)）参照）．　□

さて，いくつかの線形ＦＳＲ系列を非線形結合して乱数列を得る場合，出力される乱数列と各々の線形ＦＳＲ系列との間に相関があれば，各線形ＦＳＲ系列に対する解読の個別攻撃が可能となって，乱数列の強度が下がる．そのため，この無相関性を満たす系列を構成するための非線形結合のあり方に対する条件とか構成法とかも知られている[9]．この場合，無相関性を高めることと，線形複雑度あるいは非線形性を高めることとは，トレード・オフの関係にあり[9]，無相関性の観点からいえば，図5のGeffeの乱数列も良好なものとはいえない．

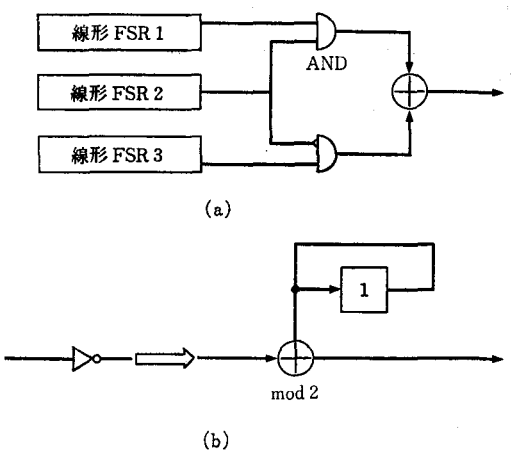

図 5　Geffe の乱数列発生器

また一方，2つの線形ＦＳＲを用意しておき，一方の内部状態をある非線形変換した値で，もう1つの線形ＦＳＲの1つのレジスタを選択し，そのレジスタの中身をその時点での出力とする乱数列生成法も検討されている[13]．なお，暗号用乱数列に対するいろいろな条件を念頭に置いた簡単な乱数列構成法の一案も提案されている[10]．

5.　暗号学的に安全な擬似乱数列発生器

前節までは，明確な定義のないまま，乱数列という言葉を用いてきたが，本節では，より厳密な表現を期し，代わりに“擬似乱数列”という言葉を使うことにする．

擬似乱数列に対しては，その一様性，独立性，生成容易性等の性質のほかに，既出のビット列から次のビットが予測できない性質も望まれる．ここでは，この予測不可性の観点から，暗号学的に安全な擬似乱数列発生器の定義を与える．

定義 5.1　[16]　ランダムなシードからそれより長い予測不可能なビット列を多項式時間で生成する発生器を暗号学的に安全な擬似乱数列発生器という．ここで，予測不可能なビット列とは，どのような多項式時間で動く機械をもってきても，ランダムにシードをとってきた場合，部分ビット列から次のビットが 1/2 より大きな確率で予測できないビット列である．

なお，ランダムなシードより，1ビット長いビット列を発生させる擬似乱数列発生器があれば，それを繰り返し用いることにより，多項式の範囲ではいくらでも長い

予測不可能なビット列を生成できる．

上記定義を満たす擬似乱数列発生器は，ある「難しい問題」を巧妙に組み込むことによって構成する．次にその一例について述べる．

例 3 暗号学的に安全な擬似乱数列発生器の例

「難しい問題」としてブラム（Blum）数の素因数分解および平方剰余問題をとりあげ，これにもとづく擬似乱数列発生器を紹介する[15]．ブラム数とは4で割ったとき余り3である2つの同程度の大きさの素数p,qを掛け合わせた積のことである．積$n=p,q$が大きいとき（512ビット程度），nからp,qに素因数分解するのは難しいとされている．また，平方剰余問題とは，ヤコビ記号[21]が1の数xを与えられたとき，nを法としてxが平方剰余であるか否かを判定する問題である．これはnの素因数分解がわからないと難しいとされている．

そこで，上記の問題の難しさに立脚して次の系列発生器を考える．まず，ブラム数nを設定する．次にランダムなシードとして$r\in\mathcal{Z}_n^*$を選択し，$x_0=r^2 \bmod n$と置く．このランダムなシードに対して，出力$b_0,b_1,\cdots,b_m$を以下のように発生する．各$i(0\leqq i\leqq m)$に対してb_iはx_iの最下位ビットで，$x_{i+1}=x_i^2 \bmod n$である．このとき$b_m,b_{m-1},\cdots,b_1$からb_0は推定できない擬似乱数になっている．（一般に$b_m,\cdots,b_{i+1}$からb_iが推定できない．）このことは，b_0が推定できれば平方剰余問題が解けることにもとづく注2)．

このようにして，ランダムなシードを発生させ，それを二乗，二乗していった数の最下位ビットを必要な数だけ保存しそれを逆向きに利用すれば，予測不可能な擬似乱数列発生器になる．□

定義 5.1は，“予測不可能性”に着眼したものである．しかし，もともと擬似乱数というからには，“一様分布”に近いという性質があるのが望ましい．次に一様分布に近いということを，“一様分布との識別不可能性”に置き換えた擬似乱数列発生器の定義を与える．

定義 5.2 [22] 暗号学的に安全な擬似乱数系列発生器とは，ランダムなシードの入力に対してそれより長いビット列を出力し，その出力分布が一様分布と識別不可能な発生器である．ここで，分布Dが一様分布Uと識別不可能であるとは，どのような多項式時間で動く判別機Mを持ってきても，分布Dからの出力と分布Uからの出力を1/2より大きな確率で判別できないことである．□

なお，“予測不可能性”と“一様分布との識別不可能性”のどちらの意味での発生器も等価であることが証明されている[22]．

これまでに述べた擬似乱数列発生器は，素因数分解や平方剰余問題，さらには離散対数問題などの難しさに仮定を置いて構成されている．このような仮定がどこまで一般的にひろげられるかについての研究が盛んであった（[22],[20],[17]）が，近年，予想されていたところに落ち着いた．すなわち，逆関数を求めるのが難しい“一方向性関数”が存在すれば，擬似乱数系列発生器が存在する，その逆も真である，ということが判明したのである[19],[18]．一方向性関数は，計算論的暗号理論の基本的な概念であり，安全な暗号方式も一方向性関数の存在が条件となっている．一方，“難しい問題の存在”という観点から，$NP\neq P$が示されない限り，一方向性関数の存在も厳密には示せないのである．

6. あとがき

暗号用乱数列を構成する際に基本となる線形フィードバックシフトレジスタ系列の性質や，それに非線形操作をほどこして得られる系列の性質，さらには，暗号学的に安全な（擬似）乱数列発生器の理論的展開に関する最近の話題を中心に解説した．暗号用乱数列に関する話としては，紙面の都合もあって，ごく限られた範囲内のものになってしまったが，この分野への入門的なお話しとして考えていただければ幸いである．この分野は，まだまだ発展途上にあり，今後は離散対数問題や素因数分解をはじめとする具体的な難しい問題にもとづく，より実用的な擬似乱数列発生器の研究開発と，それを通じた，より体系的な構成法の構築が望まれる．

注2) まず，Blum数nの性質を列挙する[15]．nがブラム数の場合，ヤコビ記号が1のxを二乗した$y=x^2 \bmod n$に対し，yの二乗根は$\pm x$と$\pm z$の4つ．$z,-z$のヤコビ記号は-1．$x,-x$のヤコビ記号は1．またyの二乗根のうち平方剰余になっているのは$x,-x$のうちのどちらか．さらに，nが奇数であるから，$x,-x$の下位ビットは異なる．

したがって，例3の発生器が予測可能であれば，ヤコビ記号が1のxの平方剰余性が判定できる．まず$x=x_0$とおいて，例3で述べた$b_1,b_2,\cdots$を生成する．このビット列が予測可能という仮定より，b_0が求められる．このとき，b_0がxのパリティに等しければ，xは平方剰余であり，異なっていれば平方非剰余と判定できる．

文　　献

[1] Kahn, D: *The Code Breakers*. Macmillan, New York, 1972.

[2] Shannon, C. E.: Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28 (1949), 656-715.

[3] Golomb, S. W.: *Shift Register Sequences*. Aegean Park Press, Revised Edition, 1982.

[4] 中村：M系列について，数理科学 No.208, Oct. 1980.

[5] Zierler, N.: Linear Recurring Sequences. *Linear Sequentaial Switching Circuits* (W. Kautz, ed.), Holden Day Inc., San Francisco, 1965.

[6] Berlekamp, E.R.: *Algebraic Coding Theory*. McGraw-Hill, New York, 1968.

[7] Rueppel, R. A.: Linear Complexity and Random Sequences, *Proc. of Eurocrypto* '85 1985.

[8] Key, E. L.: An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators. *IEEE Trans. on IT*, Vol. IT-22 (1976), 732-736.

[9] Siegenthaler, T.: Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications, *IEEE Trans. on IT*, Vol. IT-30 (1984), 776-780.

[10] 岡本，中村：非線形乱数発生方式の一案，S. 61 信学会総合全国大会予稿集.

[11] Gallager, R. G.: *Information Theory and Reliable Communication*, John Wiley and Sons., Inc., 1968.

[12] Groth, E. J.: Generation of Binary Sequences with Controllable Complexity, *IEEE Trans. on IT*, Vol. IT-17 (1971), 288-296.

[13] Jennings : Multiplexed Sequences : Some Properities of the Minimum polynomial. Lecture notes in Science, No. 149. *Gryptography proceeding, Burgfeuerstein*. 1982.

[14] Geffe, P. R.: How to protect data with ciphers that are really hard to break, *Electronics* Jan. (1973), 99-101.

[15] Blum, L., Blum, M., Shub, M.: Comparison of two pseudo-random number generators. In *Advances in Cryptology-Crypto* '82, 61-78. Springer-Verlag, 1982.

[16] Blum, M. and Micali, S.: How to generate cryptographically strong sequences of pseudo-random bits. In *FOCS 82*, 112-117, 1982.

[17] Goldreich, O., Krawczyk, H. and Luby, M.: On the existence of Pseudo-random generators. In *FOCS 88*, 12-24, 1988.

[18] Håstad, J.: Pseudo-random generators under uniform assumption, In *STOC 90*, 395-404, 1990.

[19] Impagliazzo, R., Levin, L. and Luby, M.: Pseudo-random generation from one-way functions. In *STOC 89*, 12-24, 1989.

[20] Levin, L.: One-way functions and pseudo-random generators. In *STOC 85*, 363-365, 1985.

[21] 高木貞治：初等整数論講義．共立出版，1973.

[22] Yao, A.: Theory and applications of trapdoor functions. In *FOCS 82*, 80-91, 1982.