論　文

非線形コンバイナ型乱数生成器の特性
——線形複雑度，相互情報量，無相関性について——

白石　善明[†*a)]　　森井　昌克[†b)]　　植松　友彦[††]　　坂庭　好一[††]

Some Properties on a Non-Linear Combiner Function ——On Linear Complexity, Mutual Information and Correlation Immunity——

Yoshiaki SHIRAISHI[†*a)], Masakatu MORII[†b)], Tomohiko UYEMATSU[††], and Kohichi SAKANIWA[††]

あらまし　擬似乱数生成器は，スペクトル拡散通信や共通鍵暗号方式の一つであるストリーム暗号等に用いられ，特に複数の線形フィードバックシフトレジスタ（LFSR）の出力を非線形結合した擬似乱数生成器（NLCRG）は構造が単純であることから，実用上重要視されている．しかしながら，NLCRG でさえその性質，特に出力系列の性質が完全に解明されているわけではない．先に森安，森井，笠原らは NLCRG の一つの部分クラスであるダイナミック型乱数生成器（DRG）を提案し，その出力系列の解析を試みた．本論文では，DRG の更なる解析を行うとともに，NLCRG のクラスの中での DRG の位置付け，及び一般的な NLCRG の性質，特に線形複雑度，相互情報量について考察を加えている．また，無相関性を有する非線形回路を DRG によって簡単に構成する方法を与えている．

キーワード　擬似乱数，線形フィードバックシフトレジスタ，非線形乱数生成器，線形複雑度，相互情報量，無相関性

1. まえがき

計算機シミュレーションの分野では以前から擬似乱数が重要視され，その生成法や乱数系列の性質について研究が行われてきた [1], [2]．擬似乱数は最近スペクトル拡散通信や秘密鍵暗号方式の一つであるストリーム暗号において使用され，その性能を左右する重要な技術要因であることから，その性質の解明に関する研究が注目されている．特に後者への応用に関しては，「非予測性」という性質が要求されることから，非予測性に関係した性質に対する研究が重要視されている．擬似乱数としては線形フィードバックシフトレジスタ（LFSR：Linear Feedback Shift Register）によって生成される M 系列生成器が有名であり，いくつかの条件を与えることで，乱数として良好な性質を示すことが知られている．また，数学的に解析することも比較的容易であることから様々な研究，応用が行われている．しかしながら，M 系列は非予測性に関して良好な性質を有さないことも知られている．一般に非予測性を重視した擬似乱数生成器として，(1) 複数の LFSR を非線形結合した生成器，(2) (1) にメモリを付加した生成器，(3) べき乗，剰余などの算術演算による生成器，等が存在する．特に (1) は基となっている LFSR の系列が数学的に容易に扱えること，生成器の構成が単純であること等の理由から興味深い研究対象となっている．(1) のいわゆる非線形コンバイナ型乱数生成器は種々提案され，それぞれに対していくつかの性質が示されている．中でも森安，森井，笠原によって提案されたダイナミック型非線形乱数生成器（DRG：Dynamic Random number Generator）[3] は，線形複雑度及び相互情報量という非予測性に基づく性質において優れていることが報告されている [4]．

本論文では，DRG を中心として非線形コンバイナ

† 徳島大学工学部知能情報工学科，徳島県
Faculty of Engineering, The University of Tokushima, Tokushima-ken, 770–8506 Japan
†† 東京工業大学工学部電気・電子工学科，東京都
Faculty of Engineering, Tokyo Institute of Technology, Tokyo, 152–8552 Japan
* 現在，有限会社ナオゼンネットワークス
a) E-mail: zenmei@naozen.co.jp
b) E-mail: morii@is.tokushima-u.ac.jp

型乱数生成器の性質，特に線形複雑度，相互情報量及び無相関性について考察を与える．まず，現在種々提案されている非線形乱数生成器を非線形回路の構成により分類する．特に，DRG の線形複雑度に関する上限式を示し，そこから線形複雑度が DRG において最大となるような非線形回路の構成法を明らかにする．本構成法により，他の非線形コンバイナ型乱数生成器に比較して，線形複雑度を大きく，かつ回路規模を小さくすることが可能となる．また，相互情報量という尺度から非線形コンバイナ型乱数生成器を評価し，DRG が優れていることを示す．更に，無相関性を有する非線形回路を DRG によって簡単に構成する方法を与える．

2. 非線形乱数生成器の分類

2.1 LFSR に基づく非線形乱数生成器

現在，線形フィードバックシフトレジスタ（LFSR）による，様々な非線形乱数生成器が提案されているが，以下の 5 種類に分類することが可能である．

（1） フィルタ型 … 図 1 に示されるように，単一 LFSR のレジスタの値を非線形関数 $f(\boldsymbol{x})$ を通して，最終出力を得る．

（2） コンバイナ型 … 図 2 に示されるように，複数の LFSR からの出力系列を非線形関数 $f(\boldsymbol{x})$ により操作して，最終出力を得る．具体例として，Geffe 型 [5]，Threshold 型 [7] などがある．

（3） マルチプレクサ型 … 図 3 に示されるような，フィルタ型生成器の拡張として，n 個の LFSR の複数のレジスタの値をマルチプレクサに入力して，最終出力を得る．具体例として，Jenning 型 [11]，内積型 [6] などがある．

（4） Stop-and-Go 型 … 図 4 に示されるように，ある LFSR が他の LFSR のシフトクロックを制御する．具体例として，Golmann cascade 型 [17]，Beth-Piper 型 [18]，Alternating 型 [6] などがある．

（5） 複合型 … 上記の型を組み合せた生成器．例として，フィルタ型と Stop-and-Go 型を組み合せた Bilateral 型 [19] がある．

ただし，以上の図において，$x_i(t)$ はある時刻 t で出力される値を表し，また $\boldsymbol{x}(t) = (x_1(t), x_2(t), \cdots, x_n(t))$ とする．非線形関数 $f(\boldsymbol{x})$ は，n 入力 1 出力のブール関数である．本論文ではある時刻 t における乱数生成器の基本的な性質を明らかにす

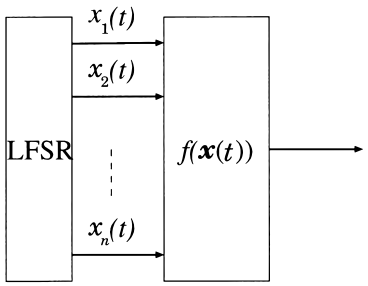

図 1 非線形フィルタ型乱数生成器の一般図
Fig. 1 A class of nonlinear filter generator.

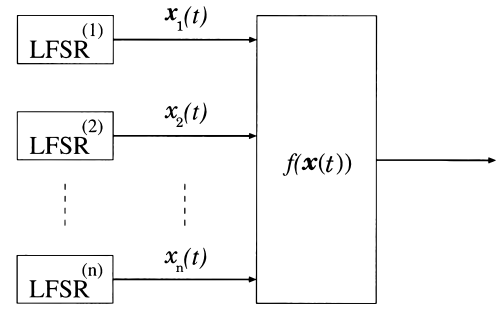

図 2 非線形コンバイナ型乱数生成器の一般図
Fig. 2 A class of nonlinear combiner generator.

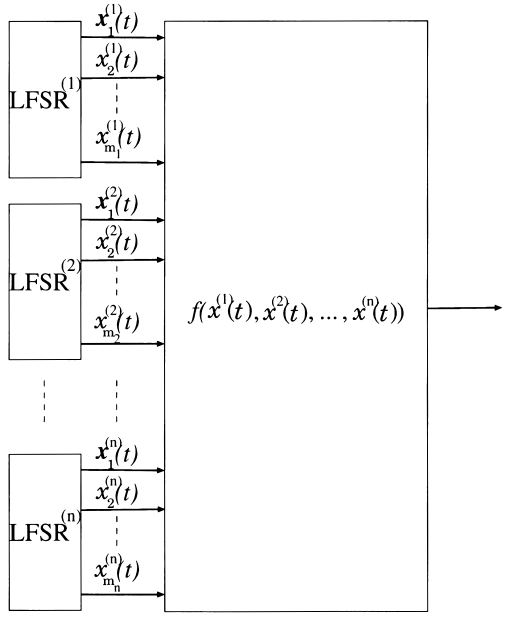

図 3 非線形マルチプレクサ型乱数生成器の一般図
Fig. 3 A class of nonlinear multiplexer generator.

るために，時系列の入出力に依存するメモリを有する非線形結合素子構造の乱数生成器は考察の対象から除外する．例えば，加算型と呼ばれる乱数生成器 [8] はメモリを有するゆえ，本論文では非線形コンバイナ型に含めない．

2.2 ダイナミック型乱数生成器（DRG）

森安，森井，笠原によって非線形コンバイナ型乱数生成器の一つとして提案されているダイナミック型乱数生成器（DRG）は次のように定義される [4]．

［定義 1］ DRG は図 5 に示すように非線形回路 C_0, C_1，$n-1$ 個の駆動 LFSR(LFSR$^{(1)}$〜LFSR$^{(n-1)}$) 及び制御 LFSR(LFSR$^{(n)}$) から構成される．制御 LFSR の出力が “0” のときには C_0 からの出力を，“1” のときには C_1 からの出力を最終出力とする．C_0, C_1 は同じ回路構成を取らないものとし，入力 LFSR の特性多項式には原始多項式を用いる．また，各特性多項式の次数は互いに素であるとする．

本論文では，DRG の線形複雑度，相互情報量を他の非線形コンバイナ型乱数生成器と比較することにより，その優位性を示す．

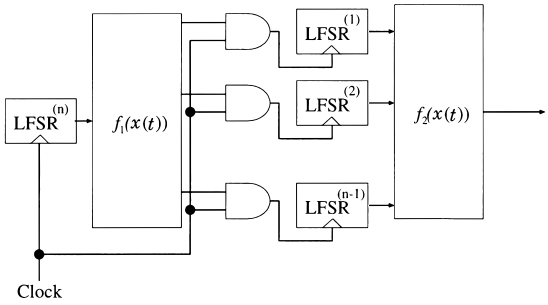

図 4　非線形 Stop-and-Go 型乱数生成器の一般図
Fig. 4　A class of nonlinear Stop-and-Go generator.

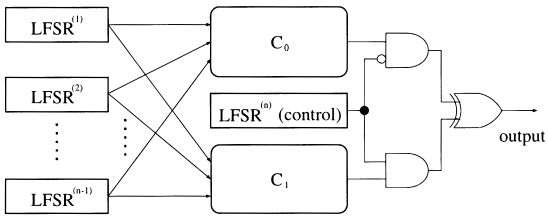

図 5　ダイナミック型乱数生成器の一般図
Fig. 5　A general form of the Dynamic Random Generator.

3. 非線形コンバイナ型乱数生成器の線形複雑度

3.1 一般的な非線形コンバイナ型乱数生成器の線形複雑度

非線形コンバイナ型乱数生成器は，複数の LFSR の出力を AND ゲートと XOR ゲートによって結合し，最終出力を得る．図 6，図 7 に示すように，二つの入力を AND 及び XOR ゲートで結合したときの線形複雑度は，入力 LFSR の線形複雑度が互いに素な数の場合，それぞれそれらの積及び和になる．なお，これらの場合，最終出力系列はそれぞれ線形複雑度が出力系列の特性多項式の次数と一致する単一の LFSR によって作ることができる [8]．

一般的な非線形コンバイナ型乱数生成器の線形複雑度 Λ を考える．非線形関数 f を次のような代数標準形で記述する．

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{i} \in Z_2^n} c_{\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}} \tag{1}$$

ここで，$F_2 := GF(2)$，$Z_2 := \{0, 1\} \subset Z$(整数) とすると，$\boldsymbol{x} = (x_1, \cdots, x_n) \in F_2^n$，$\boldsymbol{i} = (i_1, \cdots, i_n) \in Z_2^n$，$c_{\boldsymbol{i}} \in F_2$ であり，

$$\boldsymbol{x}^{\boldsymbol{i}} = \prod_{j=1}^{n} x_j^{i_j} \tag{2}$$

である．このとき，式 (1) に対応する整数関数 $f^*(\boldsymbol{x}^*)$: $Z^N \to Z$ を次のように定義する．

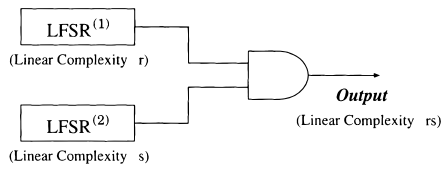

図 6　AND 結合系列
Fig. 6　An output sequence from AND-gate.

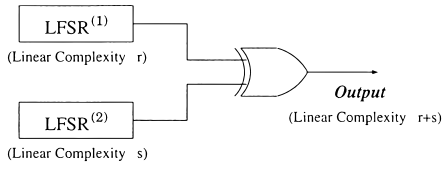

図 7　XOR 結合系列
Fig. 7　An output sequence from XOR-gate.

$$f^*(\boldsymbol{x}^*) \stackrel{\triangle}{=} \sum_{\boldsymbol{i}} c_{\boldsymbol{i}} \boldsymbol{x}^{*\boldsymbol{i}} \tag{3}$$

ここで，$\boldsymbol{x}^* = (x_1^*, \cdots, x_n^*) \in Z^n$ であり，x_i^* は x_i を出力する LFSR の線形複雑度である．また，

$$\boldsymbol{x}^{*\boldsymbol{i}} = \prod_{j=1}^{n} x_j^{*i_j} \tag{4}$$

である [9]．今，LFSR$^{(i)}$ の線形複雑度を L_i とし，それらは互いに素な数であるとする．このとき，$\boldsymbol{L} = (L_1, L_2, \cdots, L_n)$ とすると，線形複雑度 Λ は，

$$\Lambda = f^*(\boldsymbol{L}) \tag{5}$$

のようにして求められる [10]．

3.2 DRG の線形複雑度に対する限界式

DRG の線形複雑度の上界は次の定理で与えられる．

［定理 1］ DRG を構成している LFSR の特性多項式の次数の集合を Ω とする．Ω の要素に 1 を含めた集合の任意の二つ以上の要素の積に 1 を加えたものを要素とする集合を Ω_φ とする．このとき，DRG の線形複雑度 Λ_{DRG} には次式のような限界式が存在する．

$$\Lambda_{DRG} < \sum_{\gamma \in \Omega_\varphi} \gamma \tag{6}$$

（証明）回路 C_0, C_1 の非線形関数をそれぞれ $f_0(\boldsymbol{x}), f_1(\boldsymbol{x})$ とし，対応する $f_0^*(\boldsymbol{L}), f_1^*(\boldsymbol{L})$ の各項を要素とする集合を $\Delta^{(0)}, \Delta^{(1)}$ とする．このとき，

$$\Delta^{(0)} \cup \Delta^{(1)} \subset \Omega_\varphi \tag{7}$$

なる関係が成立し，また回路 C_0, C_1 は同一の回路構成を取らないことから

$$\Delta^{(0)} \cap \Delta^{(1)} = \phi \tag{8}$$

が成立する．

まず，個々の回路 C_0, C_1 と制御 LFSR との関係について考える．制御 LFSR の特性多項式の次数を γ_c とすれば制御 LFSR の第 j 番目のシンボルによって回路 C_0, C_1 の第 j 番目のシンボルのうちの一方が選択されることから，それぞれの回路のみが存在するものと考えて，それぞれの回路から出力される系列の第 j 番目の値 $\tilde{a}_{C_0 j}, \tilde{a}_{C_1 j}$ は，

$$\tilde{a}_{C_0 j} = (Tr(\beta_{\gamma_c}^j) + 1) \cdot \left\{ \sum_{\delta_0 \in \Delta^{(0)}} Tr(\beta_{\delta_0}^j) \right\} \tag{9}$$

$$\tilde{a}_{C_1 j} = Tr(\beta_{\gamma_c}^j) \cdot \left\{ \sum_{\delta_1 \in \Delta^{(1)}} Tr(\beta_{\delta_1}^j) \right\} \tag{10}$$

のように求められる．$Tr(x)$ はトレースを表し，$GF(2^n) \to GF(2)$ の線形写像である [15]．ここで，β_{δ_k} は $GF(2^{\delta_k})$ の原始元である．また DRG の出力は制御 LFSR に依存する，つまりどちらか一方の回路から制御 LFSR によって出力が選択されるので，DRG の出力系列の第 j 番目の値 $\tilde{a}_j$ は

$$\tilde{a}_j = \tilde{a}_{C_0 j} + \tilde{a}_{C_1 j} \tag{11}$$

となる．式 (9)，式 (10) から制御 LFSR と回路 C_0, C_1 を組み合せた回路のそれぞれの線形複雑度 $\Lambda_{C_0}, \Lambda_{C_1}$ はトレースの性質から

$$\Lambda_{C_0} = (\gamma_c + 1) \cdot \sum_{\delta_0 \in \Delta^{(0)}} \delta_0 \tag{12}$$

$$\Lambda_{C_1} = \gamma_c \cdot \sum_{\delta_1 \in \Delta^{(1)}} \delta_1 \tag{13}$$

であり，同様に式 (11) から DRG の線形複雑度は

$$\Lambda_{DRG} = \Lambda_{C_0} + \Lambda_{C_1} \tag{14}$$

と表せる．

ここで，DRG を構成している LFSR の組合せで可能となる線形複雑度を考えると，Λ_{DRG} の範囲は次式のようになる．

$$\Lambda_{DRG} \leqq \sum_{\gamma \in \Omega_\varphi} \gamma \tag{15}$$

今，DRG が最大の線形複雑度が得られる構成，すなわち上式の等号が成立していると仮定する．式 (15) の等号が成立するときは，

$$\Lambda_{\mathrm{MAX}} \stackrel{\triangle}{=} \gamma_c \cdot \left(\sum_{\delta_0 \in \Delta^{(0)}} \delta_0 + \sum_{\delta_1 \in \Delta^{(1)}} \delta_1 \right) + \sum_{\delta_0 \in \Delta^{(0)}} \delta_0 + \sum_{\delta_1 \in \Delta^{(1)}} \delta_1 \tag{16}$$

かつ，

$$\gamma_c \Delta^{(0)} \cup \gamma_c \Delta^{(1)} \cup \Delta^{(0)} \cup \Delta^{(1)} = \Omega_\varphi \tag{17}$$

のように，Ω_φ の 2^n 個の要素をすべて用いた場合である．ここで，

$$\gamma \Delta = \{\gamma \cdot \delta | \delta \in \Delta\} \tag{18}$$

である．式 (12)，式 (13) を用いて式 (16) を書き直すと

$$\begin{aligned}\Lambda_{\mathrm{MAX}} &= \Lambda_{C_0} + \Lambda_{C_1} + \sum_{\delta_1 \in \Delta^{(1)}} \delta_1 \\ &= \Lambda_{DRG} + \sum_{\delta_1 \in \Delta^{(1)}} \delta_1 \end{aligned} \tag{19}$$

となり式 (19) の第 2 項が 0 のとき，すなわち回路 C_1 が存在しないときのみ Λ_{DRG} の最大値が保証される．これは DRG の定義に反するので，式 (6) で DRG の線形複雑度の限界式が与えられることが証明された． □

また，DRG については次の系が成立する．

［系 1］ β_{δ_k} を $GF(2)$ 上の δ_k 次既約多項式の根とし，

$$\Delta_{DRG} \triangleq \gamma_c\Delta^{(0)} \cup \Delta^{(0)} \cup \gamma_c\Delta^{(1)} \tag{20}$$

のように定義すると，DRG の特性多項式 $H_{DRG}(X)$ は

$$H_{DRG}(X) = \prod_{\delta_k \in \Delta_{DRG}} \prod_{l=0}^{\delta_k - 1} (X - \beta_{\delta_k}^{2^l}) \tag{21}$$

で与えられる．

（証明）まず，Δ_{DRG} の各要素が系列の線形複雑度となる特性多項式を，

$$h_{\delta_k} = \prod_{l=0}^{\delta_k - 1} (X - \beta_{\delta_k}^{2^l}) \tag{22}$$

のように $GF(2^{\delta_k})$ の，共役な元を δ_k 個有する元 β_{δ_k} で表す．

DRG が出力する系列は，これらの特性多項式から出力される系列の線形結合であるので，次に線形系列の特性多項式を考える．周期 T を有する系列 $\{a_i\} = (a_1, a_2, \cdots, a_T)$ は，次のような多項式を使った有理表現で表すことができる [15]．

$$A(X) = \frac{\sum_{i=1}^{T} a_i X^{T-i}}{X^T - 1} \tag{23}$$

分母は系列 $\{a_i\}$ を出力する LFSR の特性多項式で，分子は LFSR の初期状態を表す初期値多項式である．更に，LFSR を K 個用いた線形系列 $B(X)$ は LFSR$^{(k)}$ の初期値多項式を $N_k(X)$，特性多項式を $D_k(X)$ とすると次式のように表せる [15]．

$$B(X) = \sum_{k=1}^{K} \frac{N_k(X)}{D_k(X)} = \frac{N(X)}{\prod_{k=1}^{K} D_k(X)} \tag{24}$$

式 (24) は，線形系列 $B(X)$ と等価な系列を生成する単一 LFSR の特性多項式が，各特性多項式 $N_k(X)$ の積を用いて表現できることを示している．

Δ_{DRG} のそれぞれの要素を次数にもつ特性多項式を式 (22) で表し，この特性多項式で生成される系列の線形系列を考えればよいので DRG の特性多項式 $H_{DRG}(X)$ は，

$$H_{DRG}(X) = \prod_{\delta_k \in \Delta_{DRG}} h_{\delta_k} \tag{25}$$

となる．

したがって，式 (21) が成立する． □

3.3 線形複雑度を最大とする DRG の構成法

式 (19) より，DRG の線形複雑度 Λ_{DRG} は，Ω_φ の 2^n 個すべての要素を用いた線形複雑度 Λ_{MAX} から，回路 C_1 の線形複雑度 Λ_{C_1} だけ減少することがわかる．したがって，この Λ_{C_1} の減少を最小にしたときに Λ_{DRG} が最大となる．

DRG の定義から回路 C_0，C_1 ではそれぞれすべての駆動 LFSR の出力を結合しなければならない．このとき，結合した出力系列の線形複雑度が最小となるのは，駆動 LFSR を線形結合したときであることは明らかである．

したがって，回路 C_1 の次数の集合 $\Delta^{(1)}$ は，駆動 LFSR の次数の集合となる．この集合を Ω_ψ と定義する．また，式 (19) から集合 $\Delta^{(1)}$ の和だけ Λ_{MAX} から減少することと，式 (14) のように展開することによって，集合 Ω_φ から集合 $\Delta^{(1)}$ を除いたすべての要素を DRG に用いることができる．

集合 Ω_φ の要素から Ω_ψ の要素を除いた集合 $\Omega_\varphi - \Omega_\psi$ は式 (16)，式 (19) から

$$\gamma_c\Delta^{(0)} \cup \Delta^{(0)} \cup \gamma_c\Delta^{(1)} \tag{26}$$

のように分割できる．ここで $\Delta^{(1)}$ は Ω_ψ であるので，式 (26) から $\Delta^{(0)}$ を求めることができる．

以上をまとめると DRG の線形複雑度を最大にする回路の構成法は次のようになる．

（1） 駆動 LFSR の次数の集合 Ω_ψ を $\Delta^{(1)}$ とする．

（2） $\Omega_\varphi - \Omega_\psi$ を式 (26) のようにして集合 $\Delta^{(0)}$ を求める．

（3） 式 (12)，式 (13) を満たすような回路 C_0, C_1

を求める．

（例 1） 3 入力 DRG (3DRG, 以下では n 入力 DRG を nDRG と呼ぶ)，$LFSR^{(1)}, LFSR^{(3)}$ を駆動 LFSR で線形複雑度を r, s とする．また $LFSR^{(2)}$ を制御 LFSR とし，その線形複雑度を c とする．r, s, c は互いに素である．

（1） Ω_ψ，Ω_φ は次のようになる．

$$\Omega_\varphi = \{1, r, s, c, rs, sc, cr, crs\} \tag{27}$$

$$\Omega_\psi = \{r, s\} \tag{28}$$

Ω_φ のすべての要素を使ったとき，すなわち線形複雑度の最大値 Λ_{MAX} は，

$$\Lambda_{\mathrm{MAX}} = \sum_{\delta \in \Omega_\varphi} \delta \tag{29}$$

となる．駆動 LFSR の次数の集合 Ω_ψ から $\Delta^{(1)}$ は

$$\Delta^{(1)} = \{r, s\} \tag{30}$$

のようになる．

（2） $\Delta^{(0)}$ は

$$\begin{aligned} \Omega_\varphi - \Omega_\psi &= \{1, c, rs, sc, cr, crs\} \\ &= \{c, crs\} \cup \{1, rs\} \cup \{sc, cr\} \end{aligned} \tag{31}$$

より

$$\Delta^{(0)} = \{1, rs\} \tag{32}$$

となる．

これで DRG の線形複雑度は

$$\Lambda_{DRG} = (c+1)(1+rs) + c(r+s) \tag{33}$$

となり，式 (29) と比較すると $\Delta^{(1)}$ の要素分だけ減少していることがわかる．

（3） 式 (33) から回路 C_0, C_1 を設計する．

上の手続きで構成された 3DRG を図 8 に示す．

入力 LFSR の数 n が固定されている場合，**3.3** の構成法による DRG の線形複雑度が，他のいかなる構成法による DRG よりも大きいか，それ以上となることを 3DRG を例に挙げて証明する．

式 (19) において，回路 C_1 の構成により DRG の線形複雑度が大きく変化すること，すなわち Ω_φ の全要素から $\Delta^{(1)}$ の要素だけ線形複雑度が減少することを用いてこの構成法は考案された．したがって，$\Delta^{(1)}$ を Ω_ψ とすることの妥当性について考察する．前節の例では DRG の定義から $\Delta^{(1)}$ は

$$\{r, s\}, \{rs\} \tag{34}$$

の 2 個の集合が候補となる．この 2 個の集合の要素間には

$$r + s < rs, \quad r, s > 0 \tag{35}$$

が成立するので回路 C_1 は線形回路としなければならない．同様の議論により入力 LFSR を 4 個以上用いて DRG を構成するときも回路 C_1 は線形回路でなければならないことがわかる．また，式 (26) のように集合を分割できることは式 (16)，式 (19) により明らかである．

よって前述の構成法で DRG における線形複雑度が最大となることが証明された． □

図 9 に本構成法による 4DRG の例を与える．これは森安，森井，笠原 [4] によって設計された DRG と

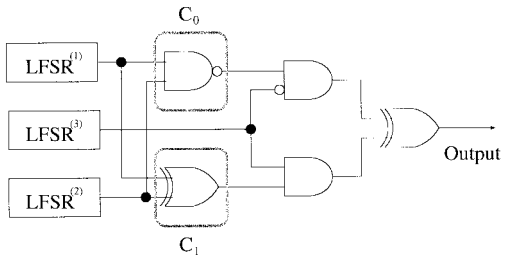

図 8 線形複雑度が最大となる構成例 1
Fig. 8 An example of 3DRG with maximum linear complexity.

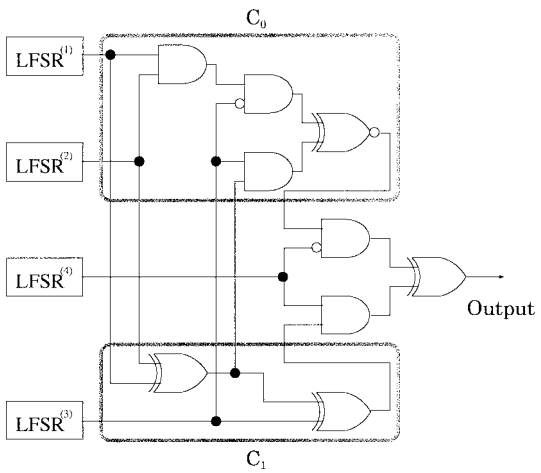

図 9 線形複雑度が最大となる構成例 2
Fig. 9 An example of 4DRG with maximum linear complexity.

同一条件 $(r = 2, s = 3, t = 5, c = 7)$ の下で線形複雑度が 566 となり 50 向上している．

3.4 他の乱数生成器との比較

DRG と代表的な非線形コンバイナ型乱数生成器である，Geffe 型，Threshold 型乱数生成器を比較すると，図 10 のようになる．LFSR のフリップフロップの個数，すなわち乱数生成器の LFSR の総段数が等しいときに，各々の生成器がどの程度の線形複雑度になるかを示した．他の二つの生成器に比べて格段に優れていることがわかる．

また，図 11 に示す Geffe 型を拡張した Key 型生成器 [12] もコンバイナ型の一つであるが，この Key 型

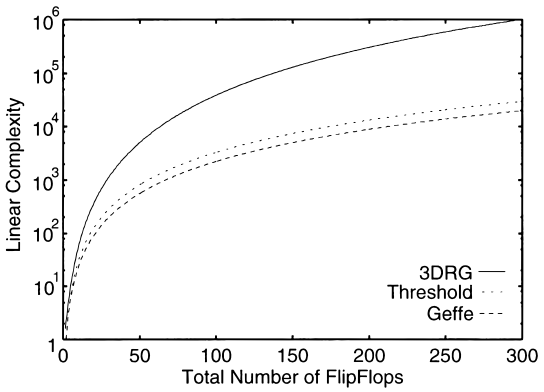

図 10　線形複雑度の比較
Fig. 10　The comparison of 3DRG, Geffe's generator and Threshold generator in terms of linear complexity.

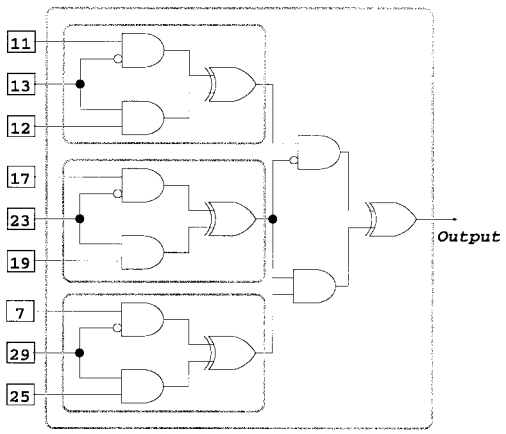

図 11　Key 型生成器
Fig. 11　Key's generator.

と同程度の線形複雑度をもつ 5DRG を **3.3** の構成法で設計したものが図 12 である．両者の回路規模は，表 1 に示されるように，ゲート数は同程度で，DRG では入力 LFSR の総段数を半分程度にしているにもかかわらず，線形複雑度が同程度の生成器を実現できている．

図 13 は，入力数 n の増加に伴う DRG の線形複雑度の変化を示した図である．n を増加させることによって線形複雑度が指数関数的に増大することがわかる．ただし，この図では線形複雑度が最大となるように設計されており，入力 LFSR の段数は DRG においては互いに素なものを用いなければならないので，3DRG の場合は $\{2, 3, 5\}$，4DRG の場合には $\{2, 3, 5, 7\}$ のように，以下順次，入力 LFSR の段数は $11, 13, 17, 19, \cdots$ のように素数を用いていくものとしている．このような小さい段数を使っているために，線形複雑度が約 10^9 までしか現れていないが，段数を

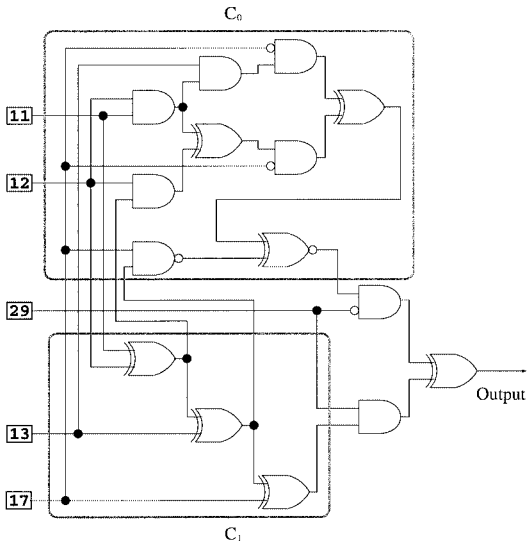

図 12　Key 型生成器と同程度の線形複雑度をもつ 5DRG
Fig. 12　An example of 5DRG with maximum linear complexity.

表 1　5DRG と Key 型生成器との比較
Table 1　The comparison of 5DRG and Key's generator.

	5DRG	Key の生成器
線形複雑度	1,179,307	1,071,561
ゲート数	8(AND) 7(XOR)	8(AND) 4(XOR)
レジスタの総段数	82	156

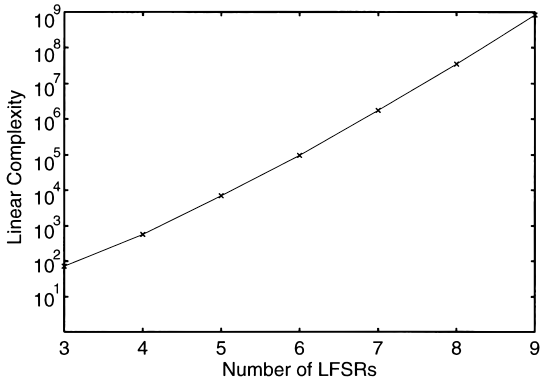

図 13　n 入力 DRG の線形複雑度の最大値の変化
Fig. 13　The profile of maximum linear complexity of nDRG.

大きくすることにより実用に耐えうる線形複雑度を実現することは容易に可能である．

4. ダイナミック型乱数生成器（DRG）の相互情報量

4.1 相互情報量

乱数生成器の無相関性を議論するときには様々な評価方法がある．ここでは相互情報量によって考察する．[定義 2]

$p(x_k)$：　事象 x_k の生起確率
$p(y_l)$：　事象 y_l の生起確率
$p(x_k, y_l)$：　事象 x_k, y_l の同時生起確率

とし，X 及び Y の事象数がそれぞれ s, t であれば，相互情報量 $I(X;Y)$ は次式で与えられる．

$$I(X;Y) = -\sum_{k=1}^{s}\sum_{l=1}^{t} p(x_k, y_l)\log_2 \frac{p(x_k)p(y_l)}{p(x_k, y_l)} \tag{36}$$

相互情報量は入力情報が出力側にどの程度漏洩しているかを定量的に示すものである．この数値が高い乱数生成器ほど未知ビットを推測しやすいということを表すゆえ，入出力間の相互情報量は可能な限り小さい方が暗号用乱数生成器としては望ましい．式 (36) の相互情報量は，非線形関数 $f(\boldsymbol{x})$ の入出力表により求められる．このことから，相互情報量は入力 LFSR の線形複雑度やそれらの非線形関数に対する入力位置には左右されないゆえ，その非線形関数の構造によってのみ決定される．しかし，一般的な非線形コンバイナ型乱数生成器の相互情報量を与えるのは困難であるので，ここでは相互情報量の求め方を例にあげ，次節で同じコンバイナ型に属す乱数生成器と DRG の比較を行う．

表 2　3DRG の入出力状態
Table 2　I/O state of 3DRG.

X_1	X_2	X_3	Z
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

（例 2）　図 8 の相互情報量を求める．表 2 に入出力状態を示す．$LFSR^{(1)}, LFSR^{(2)}, LFSR^{(3)}$ をそれぞれ入力情報源 X_1, X_2, X_3 とし，出力を Z とする．出力側 Z の X_1 に対する相互情報量 $I(Z;X_1)$ は次式で与えられる．

$$\begin{aligned} I(Z;X_1) &= -\left(\frac{3}{8}\log_2\frac{\frac{5}{8}\cdot\frac{1}{2}}{\frac{3}{8}} + \frac{2}{8}\log_2\frac{\frac{5}{8}\cdot\frac{1}{2}}{\frac{2}{8}}\right. \\ &\quad \left. + \frac{1}{8}\log_2\frac{\frac{3}{8}\cdot\frac{1}{2}}{\frac{1}{8}} + \frac{2}{8}\log_2\frac{\frac{3}{8}\cdot\frac{1}{2}}{\frac{2}{8}}\right) \\ &= 0.0487(\text{bit}) \end{aligned} \tag{37}$$

同様に，$I(Z;X_2)$，$I(Z;X_3)$ を求めると次のようになる．

$$I(Z;X_2) = I(Z;X_3) = 0.0487(\text{bit}) \tag{38}$$

4.2 他の乱数生成器の比較

線形複雑度と同様に，コンバイナ型の Geffe 型，Threshold 型生成器と DRG を比較する．ここで，3DRG は図 8，4DRG は図 9 とする．表 3 から，DRG では他の非線形コンバイナ型に属する同程度の回路規模の乱数生成器に比べて入力 LFSR からのキーストリームの漏洩が 1/5 から 1/10 程度に減少しており，非予測性に優れていることがわかる．

線形複雑度が最大となるように設計された n 入力 DRG においては，式 (36) における $p(x_k)$，$p(y_l)$，$p(x_k, y_l)$ が n によって規則的に決定されるので，すべての LFSR の出力 x_i $(for\ all\ i)$ と DRG の出力 z との間の相互情報量 $I^{(n)}$ は次式で求められる．

$$I^{(n)}(z;x_i) = -\left(\frac{2^{n-2}-1}{2^n}\log_2\frac{1}{2}\cdot\frac{2^{n-1}-1}{2^{n-2}-1}\right.$$

表 3　相互情報量の比較
Table 3　The comparison in mutual information.

3DRG(3 入力)	すべての LFSR で 0.0487(bit)
4DRG(4 入力)	すべての LFSR で 0.0114(bit)
Geffe 型 (3 入力)	0.1887(bit) 0(bit) [clock LFSR] 0.1887(bit)
Threshold 型 (M 入力)	すべての LFSR で 0.189(bit)[M=3] 0.104(bit)[M=5]

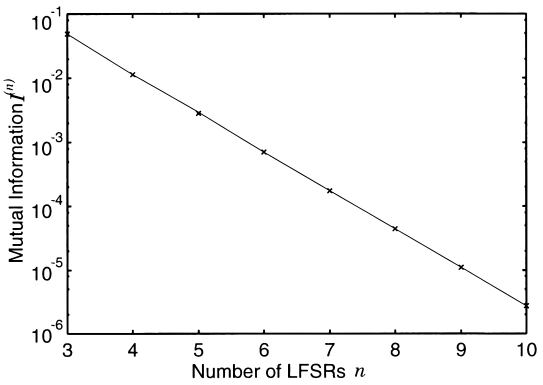

図 14　n 入力 DRG の相互情報量
Fig. 14　The profile of mutual information of nDRG with maximum linear complexity.

$$
\begin{aligned}
&+\frac{2^{n-2}+1}{2^n}\log_2\frac{1}{2}\cdot\frac{2^{n-1}+1}{2^{n-2}+1}\\
&+\frac{2^{n-2}}{2^n}\log_2\frac{1}{2}\cdot\frac{2^{n-1}-1}{2^{n-2}}\\
&+\frac{2^{n-2}}{2^n}\log_2\frac{1}{2}\cdot\frac{2^{n-1}+1}{2^{n-2}}\Bigg)\\
=\ &-\frac{1}{4}\log_2\frac{(2^{2n-2}-1)^2}{2^{2n}(2^{2n-4}-1)}\\
&-\frac{1}{2^n}\log_2\frac{(2^{n-1}+1)(2^{n-2}-1)}{(2^{n-2}+1)(2^{n-1}-1)}
\end{aligned}
\tag{39}
$$

式 (39) を用いて DRG の入力 LFSR の個数による相互情報量の変化を図 14 に示す．n の増加に伴って，相互情報量は指数関数的に減少していることから，非線形関数の入力数を増加させることにより入力情報の漏洩を偏りなく分散させることが可能であると言える．

5.　無相関な非線形関数

5.1　無相関な非線形関数

$X_i,\ i=1\cdots n$ をランダム変数とするとき，

$$I(X_{i_1},X_{i_2},\cdots,X_{i_m};Z)=0 \tag{40}$$

を満たす関数を m 次の無相関な n 入力の非線形関数という．すなわち，n 個のランダム変数から m 個を選んだとき，$Z=f(X_1,X_2,\cdots,X_m)$ が統計的に独立な関数ということである．

この無相関な関数を構成する具体的な定理が Siegenthaler [13] によって与えられている．

[定理 2] [13]　$\boldsymbol{X}=(X_1,X_2,\cdots,X_n)$ とし，$f_1(\boldsymbol{X})$, $f_2(\boldsymbol{X})$ を m 次の無相関な関数とすると，

$$
\begin{aligned}
&f(X_1,X_2,\cdots,X_{n+1})\\
&\quad=X_{n+1}f_1(\boldsymbol{X})+(X_{n+1}+1)f_2(\boldsymbol{X})
\end{aligned}
\tag{41}
$$

は $n+1$ 入力の m 次の無相関な関数 f となる．□

ここで，定理 2 の f_1,f_2 の初期化は，次のように選べばよいことが知られている [13].

$$
\begin{aligned}
f_1(x_1,x_2,\cdots,x_{m+2}) &= x_1+x_2+\cdots\\
&\quad +x_m+x_{m+1} \qquad (42)\\
f_2(x_1,x_2,\cdots,x_{m+2}) &= x_1+x_2+\cdots\\
&\quad +x_m+x_{m+2} \qquad (43)
\end{aligned}
$$

非線形関数の非線形性と無相関性はトレードオフになるがゆえ，無記憶である無相関な関数を設計することは線形複雑度を犠牲にする．Geffe 型生成器のような従来のコンバイナ型乱数生成器では実現できなかった無相関な非線形関数を，同じコンバイナ型に属す DRG により簡単に構成できることを次節で示す．

5.2　DRG による無相関な非線形回路の構成法

定理 2 の式 (41) においては，f_1,f_2 が DRG の制御 LFSR の値によって選択される回路とみなすことができる．したがって，設計時に要求される無相関性の次数をもつ DRG を構成することは容易で，その手順は以下のとおりである．

（1）　回路 $C_0^{(0)},C_1^{(0)}$ を初期化する．すなわち，回路 $C_0^{(0)},C_1^{(0)}$ の結合関数 $f_0^{(0)},f_1^{(0)}$ を要求する m 次の無相関な関数とする．これら回路 $C_0^{(0)},C_1^{(0)}$ を，制御 LFSR で選択するように $DRG^{(0)}$ を設計する．このとき，DRG の入力 LFSR は回路 $C_0^{(0)},C_1^{(0)}$ への入力が $(m+2)$ 個と制御 LFSR なので，$m+3$ 個となる．

（2）　DRG の入力 LFSR が要求される個数 n となるまで，すなわち以下の手続きを $i=1\cdots n-(m+3)$ 回繰り返す．

（a）　$DRG^{(i-1)}$ を回路 $C_0^{(i)}$ とする．

（b）　$DRG^{(i-1)}$ の入力 LFSR を次の置換規則に

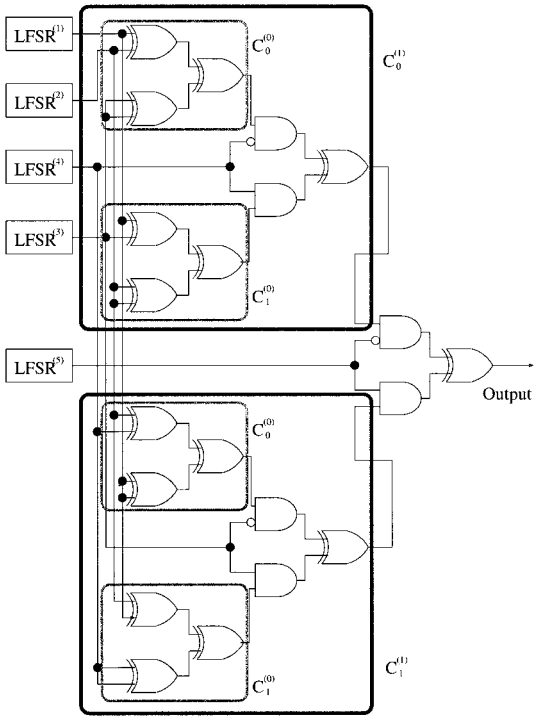

図 15　1 次の無相関な 5 入力 DRG
Fig. 15　An example of 5DRG with first order correlation immunity.

基づいて置換し，それらを入力とする回路を $C_1^{(i)}$ とする．入力 LFSR をそれぞれ $LFSR^{(k)}$ とする．
置換規則：$k = k + i \pmod{m + 3 + (i - 1)}$
（c）　$LFSR^{(m+3+i)}$ を制御 LFSR として $DRG^{(i)}$ を設計する．
（例 3）　1 次の無相関な 5 入力 DRG を図 15 に示す．

6. むすび

本論文では，種々提案されている非線形乱数生成器を四つのタイプに分類し，その一つである非線形コンバイナ型乱数生成器の性質について考察を与えた．特に，非線形コンバイナ型乱数生成器の一つとして提案されている，DRG の従来知られていなかった線形複雑度に対する上界式を示し，入力 LFSR の数が同一の DRG のうちで，線形複雑度が最大となる構成法を明らかにした．既存の非線形コンバイナ型乱数生成器より，回路規模を小さくしても，線形複雑度を大きくすることができる．また，相互情報量についても非線形コンバイナ型の他の生成器と比較することにより優れていることを示した．更に，DRG により無相関な関数を簡単に設計する方法を与えた．従来の記憶をもたない非線形コンバイナ型乱数生成器では無相関性を有する生成器は存在しなかった．線形複雑度，相互情報量，無相関性という点について，DRG は同じコンバイナ型に属する他の乱数生成器に比して非予測性に優れた系列を生成できることを示した．

本論文で考察した線形複雑度，相互情報量，及び無相関性は乱数生成器の非予測性に対する代表的な評価尺度であるが，おのおの非予測性の十分条件ではなく，必要条件となっている．田中，金子らは非線形コンバイナ型乱数生成器の構成が既知として，その出力系列から初期値を求める問題に着目し，DES 等の解読法として著名な線形解読法を導入することにより，予測性の評価を与えている [20], [21]．今後は田中，金子らの評価を含めて，総合的な評価，新しい評価法，及び現在までの評価法に基づく非予測性に優れた乱数生成器の構成を研究する予定である．

文　献

[1] S.W. Golomb, Shift register sequences, Aegean Park Press, Laguna Hills, California, 1982.
[2] 柏木　濶，“M 系列再発見，” 計測制御，vol.20, no.2, pp.236–245, Feb. 1981.
[3] 森安峰嗣，森井昌克，笠原正雄，“非予測性を重視した乱数生成器の提案，” システム制御情報学会論文誌，vol.7, no.11, pp.479–481, July 1994.
[4] T. Moriyasu, M. Morii, and M. Kasahara, “Nonlinear pseudorandom number generator with dynamic structure and its properties,” Proc. Symposium on Cryptography and Information Security, SCIS94-8A, Biwako, Japan, Jan. 1994.
[5] P.R. Geffe, “How to protect data with ciphers that are really hard to break,” Electronics, vol.46, no.1, pp.99–101, Jan. 1973.
[6] C.G. Günther, “Alternating step generators controlled by de Bruijin sequences,” Proc. Eurocrypt’87, pp.5–14, Amsterdam, The Netherlands, April 1987.
[7] J.O. Bruer, “On pseudo random sequences as crypto generators,” Proc. Int. Zurich Seminar on Digital Communications, pp.157–161, Zurich, Switzerland, 1984.
[8] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin, 1986.
[9] R.A. Rueppel, “When shift registers clock themselves,” Proc. Eurocrypt’87, pp.53–64, Amsterdam, The Netherlands, April 1987.
[10] R.A. Rueppel, “Stream ciphers,” in Contemporary Cryptology, ed. G.T. Simmons, pp.65–134, IEEE Press, New York, 1992.
[11] S.M. Jennings, “Multiplexed sequences: Some prop-

erties of the minimum polynomial," Proc. Workshop Cryptography, pp.189–206, Burg Feuerstein, Germany, March 1982.
[12] E.L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," IEEE Trans. Inf. Theory, vol.IT-22, no.6, pp.732–736, June 1976.
[13] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," IEEE Trans. Inf. Theory, vol.IT-30, no.5, pp.776–780, May 1984.
[14] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," IEEE Trans. Comput., vol.C-34, no.1, pp.81–85, Jan. 1985.
[15] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, Spread Spectrum Communications, Computer Science Press, Maryland, 1985.
[16] 辻井重男，笠原正雄，暗号と情報セキュリティ，昭晃堂，東京，1989.
[17] D. Gollmann, "Transformation matrices of clock-controlled shift registers," Proc. Cryptography and Coding III, pp.197–210, Cirencester, UK, 1991.
[18] T. Beth and F.C. Piper, "The stop-and-go generator," Proc. Eurocrypt'84, pp.88–92, Paris, France, April 1984.
[19] K.C. Zeng, G.H. Yang, and T.R.N. Rao, "On the linear consistency test(LCT) in cryptanalysis with applications," Proc. Crypto'89, pp.164–174, Santa Barbara, California, USA, Aug. 1990.
[20] 田中秀磨，金子敏信，"非線形コンバイナ型乱数生成器に対する線形攻撃," 信学論（A），vol.J79-A, no.8, pp.1360–1368, Aug. 1996.
[21] 田中秀磨，大石智也，金子敏信，"非線形コンバイナ型乱数生成器に対する線形攻撃 (2)," 暗号と情報セキュリティシンポジウム，SCIS97-32A, Jan. 1997.

（平成 11 年 8 月 4 日受付，12 年 2 月 9 日再受付）

白石　善明　（正員）

平 7 愛媛大・工・情報卒．平 9 同大大学院博士前期課程了．平 12 徳島大大学院博士後期課程了．工博．現在，(有）ナオゼンネットワークスに勤務．情報セキュリティ，コンピュータネットワークの研究に従事．IEEE，情報処理学会各会員．

森井　昌克　（正員）

平 1 阪大大学院工学研究科通信工学専攻博士課程了．同年京都工繊大助手．平 2 愛媛大講師．平 4 同助教授．平 7 徳島大教授．代数的符号理論，離散数学，ディジタル信号処理アルゴリズム，情報セキュリティ及びコンピュータネットワーク等の研究・教育に従事．IEEE，計測自動制御学会，情報処理学会，システム制御情報学会，日本応用数理学会，画像電子学会，情報理論とその応用学会各会員．工博．

植松　友彦　（正員）

昭 57 東工大・工・電気電子卒．昭 59 同大大学院修士課程了．同年同大・工・電気電子助手．同講師を経て平 3 同助教授．平 4 北陸先端大・情報科学研究科助教授．平 9 東工大・工・電気電子工学科助教授．工博．情報理論，特にシャノン理論の研究に従事．昭 63 年度本会篠原記念学術奨励賞受賞．平 4 年度並びに平 7 年度本会論文賞受賞．著書「文書データ圧縮アルゴリズム入門」,「よくわかる通信工学」,「現代シャノン理論」など．IEEE，情報理論とその応用学会各会員．

坂庭　好一　（正員）

昭 47 東工大・工・電子卒．昭 52 同大大学院博士課程了．工博．同年同大学院総合理工学研究科助手．同大工学部助手，助教授を経て，現在，同大学院理工学研究科教授．通信理論，符号理論，信号処理等の研究に従事．昭 57，平 2，平 4，平 6 年度電子情報通信学会論文賞受賞．IEEE，情報理論とその応用学会，情報処理学会，映像メディア学会，電気学会各会員．