SPN 構造における線形変換層の一設計法

神田雅透[†,†††] 高嶋洋一[††] 松本勉[†††]
青木和麻呂[†,☆] 太田和夫[†,☆☆]

本稿では，SPN（Substitution-Permutation-Network）構造における線形変換層の構成法について検討する．具体的には，線形変換層を有限体 GF(2) 上の $m \times m$ 行列として表現することによって，差分解読法や線形解読法に対して耐性を有し，かつ効率的な実装が可能となるような線形変換層の構成法を提案する．さらに，$m = 8$ の場合について，このアルゴリズムを用いた線形変換層の分岐数が 5 となる最適な線形変換層の構成例を示す．その際，最適な安全性を持つ線形変換の候補の中から特に 32-bit CPU で効率的な実装が可能となるものを選択し，実際に線形変換層を構成している．また，排他的論理和のみで構成される線形変換層は，実装環境に応じた様々な効率的な実装に等価変形できることも示す．最後に，暗号全体の最大差分特性確率や最大線形特性確率の上界値と線形変換層の分岐数との関係を述べる☆1.

On the Design of Linear Transformation Layers for SPN Structures

Masayuki Kanda,[†,†††] Youichi Takashima,[††]
Tsutomu Matsumoto,[†††] Kazumaro Aoki[†,☆] and Kazuo Ohta[†,☆☆]

In this paper, we research on a design of linear transformation layers for SPN (Substitution-Permutation-Network) structures. More precisely, we represent the linear transformation layers as an $m \times m$ matrix P in the finite field GF(2), and propose an algorithm for constructing the efficient linear transformation layers which are invulnerable to differential and linear cryptanalysis. In the case of $m = 8$, we give an example of designing an optimal linear transformation layer whose branch number is 5 by using this proposed algorithm. The layer is selected in terms of efficient implementation on the recent 32-bit CPUs in particular. Furthermore, we show that a technique of implementing the linear layer efficiently depends on computational circumstances, since the layer can be constructed with bitwise exclusive ORs. Finally, the relationship between the upper bounds of the maximum differential and linear characteristic probability and branch numbers of linear transformation layer is described.

1. はじめに

差分解読法[4]や線形解読法[17]は共通鍵暗号に対する強力な解読法である．そこで，最近のブロック暗号の設計では，最低限，差分解読法や線形解読法に対して十分に安全であることを示すことが強く望まれている．

差分解読法（線形解読法）に対する安全性を示す評価指標としては，最大平均差分確率（最大平均線形確率）に関するものと最大差分特性確率（最大線形特性確率）に関するものとが知られている．

最大平均差分確率は，入出力の差分値のみを特定し，各段の差分値は特定しないすべての差分経路☆2を考慮するときの導出確率の最大値であり，差分解読法に対する厳密な安全性評価を与えるものである[15]．しかし，計算機によって最大平均差分確率を厳密に評価することは本質的にきわめて困難であり，現在のところ，暗号設計時に利用できる評価指標ではない．また，最

† NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories
†† NTT サイバーソリューション研究所
NTT Cyber Solution Laboratories
††† 横浜国立大学
Yokohama National University
☆ 現在，NTT コミュニケーションズ
Presently with NTT Communications
☆☆ 現在，電気通信大学
Presently with University of Electro-Communications

☆1 本稿の初期バージョンは，SAC'98 で発表されている[12]．

☆2 暗号化の過程で，与えられた平文の差（入力差分）がどのような差分に変化しながら暗号化され，最終的に暗号文の差（出力差分）になるかを表す状態遷移のことを差分経路という．

大平均差分確率の上界値による評価指標もあるが，この評価指標によって差分解読法に対する安全性を保証するためには，ラウンド関数での最大平均差分確率が十分に小さくなることが必須条件となる[18]．このことは，暗号設計上の制約条件が強く，設計自由度が小さいことを意味する．

一方，最大差分特性確率は，入出力の差分値だけでなく，各段の差分値も特定した差分経路に関する導出確率[4]の最大値である．この確率による安全性評価は，最大平均差分確率で考慮しているすべての差分経路の中から最大確率をとる1つの差分経路だけを取り出した場合の評価に相当するので，最大平均差分確率による評価ほど厳密ではない．しかし，現在のところ，攻撃者は，最大差分特性確率を算出するためのアルゴリズムと同じアルゴリズムを使って攻撃に利用する差分経路を探索する手法しか知られていないので，最大差分特性確率による評価であっても暗号設計には有効な評価指標である．特に，最大差分特性確率の上界値による評価指標では，一般に，ラウンド関数での最大差分特性確率と段数からだけで安全性評価を行うことができる．このことから，ラウンド関数での最大差分特性確率を導出するだけで，即座に（段数に依存した）暗号全体の安全性評価が可能である[10),14),22)]．ここで重要な点は，段数を多くすることができるのであれば，ラウンド関数での最大差分特性確率を必ずしも十分に小さくする必要はないということである．これによって，ラウンド関数の設計自由度が大きくなり，差分解読法に対する耐性を有しながら効率的な実装ができることを重視した設計が可能となる．

以上のことは，最大平均線形確率[20]と最大線形特性確率[17]についても同様である．

そこで，我々は，最大差分特性確率および最大線形特性確率の上界値を指標☆とするブロック暗号の設計法を検討している．この評価指標に適した構成として，SPN（Substitution-Permutation-Network）構造を利用するものがある．SPN構造の場合，一般に暗号全体が非線形変換部分である s-box（置換表，Substitution-layerともいう）と線形変換部分である線形変換層（拡散層，Permutation-layer，Diffusion-layerともいう）とで構成されているため，最大差分特性確率および最大線形特性確率の上界値を，s-box自体が有する安全性（s-boxの耐性）と線形変換層の特性を利用して評価することができる[10),22)]．したがって，差分解読法や線形解読法に対する安全性が高い s-boxと線形変換層をどのように設計するかという点が設計上のポイントとなる．

本稿では，文献12)を参考に，差分解読法や線形解読法に対する高い安全性と効率的な実装との両立が可能となるような線形変換層の設計法，ならびに安全性評価について考察する．対象とする線形変換層は，有限体 GF(2) 上の $m \times m$ 行列 P で表される，すなわち排他的論理和（XOR）だけで構成されるものとする．

具体的な設計法は，[a] GF(2) 上の $m \times m$ 行列 P を利用して，差分解読法や線形解読法に対して最適な安全性を持つ線形変換の候補を導出すること，および [b] 最適な安全性を持つ線形変換の候補の中から効率的な実装ができるような線形変換層を選択し，実際に構成すること，の2段階のステップで構成される．また，XORのみで構成される線形変換層は様々な等価変形した実装を容易に作り出すことが可能であることから，[b] で構成した線形変換層が実装環境に応じて効率的な実装に等価変形できることも示す．

本稿の構成は以下のとおりである．2章で本稿で利用する表記および定義を説明する．3章で行列 P を利用して最適な線形変換層を構成する方法を述べ，4章で具体的な $m = 8$ の場合の構成について検討する．5章で行列 P を利用した線形変換層に関する考察を行った後，6章でまとめを述べる．

2. 準　　備

2.1 線形変換層の表記

本稿では，s-boxの入出力ブロック長を n-bitとした，mn-bitの入出力ブロック長からなるSPN構造を考察対象とする（**図1**）．なお，拡大鍵の挿入は各 s-boxの前で排他的論理和により行われるものと仮定し，本稿では鍵挿入層についての議論は行わないことにする．

線形変換層は，有限体 GF(2) 上の $m \times m$ 行列 P で表されるものとする．すなわち，

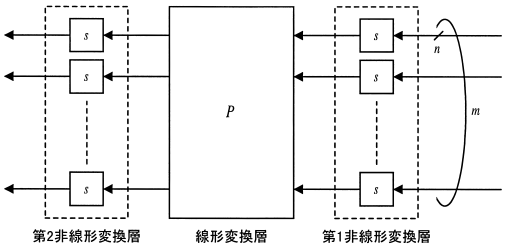

図1 SPN構造
Fig. 1 SPN structure.

☆ 強度概観評価尺度ともいう[13]．

$$P:\ \mathrm{GF}(2^n)^m \mapsto \mathrm{GF}(2^n)^m:$$
$$(x_1, x_2, \ldots, x_m) \to (y_1, y_2, \ldots, y_m)$$
$$y_j = \oplus_{i=1}^{m} p_{ji} x_i$$

ただし，$p_{ji} \in \mathrm{GF}(2)$ は行列 P の j 行 i 列の要素を表す．

このように表現された線形変換層は，上式から分かるように，計算上は n-bit 単位での線形変換を行うものであり，また実装上は XOR だけで構成できることになる．特に，$n = 8$ であればバイト単位での線形変換ということになるので，ワード幅が 8-bit 以上のいずれのプラットフォームにおいても効率的な実装が可能になると期待される．

2.2 定　　義

定義 1（Active s-box）差分解読法では入力差分値が非零である s-box，線形解読法では出力マスク値が非零である s-box のことを active s-box という．
注意：s-box が全単射であるときには，出力差分値が非零である s-box や入力マスク値が非零である s-box も active s-box となる．

定義 2（分岐数[22]）線形変換層 P に対する分岐数 $\mathcal{B}$ を以下のように定義する．

$$\mathcal{B}(P) = \min_{X \neq 0}(w(X) + w(P(X)))$$

ただし，$X = (x_1, x_2, \ldots, x_m) \in \mathrm{GF}(2^n)^m$ であり，$w(X)$ は X の非零要素数，すなわち $w(X) = \#\{1 \leq i \leq m | x_i \neq 0\}$ として表される．

分岐数 $\mathcal{B}$ は，線形変換層への入力データが少なくともどの程度の出力データに影響を与えるかという，線形変換層でのデータ拡散性を示す指標であると同時に，攻撃者が入出力データを制御する困難性を示す指標でもある．すなわち，入力データの小さな変化がどれだけ多くの出力データに影響を与えることになるのか，また出力データの小さな変化を導くにはどれだけ多くの入力データの制御が必要となるのか，という点について最悪ケースでの評価値を分岐数 $\mathcal{B}$ が与えることになる．したがって，差分解読法および線形解読法に対する安全性の観点からは分岐数 $\mathcal{B}$ が大きいほど望ましい．

定義 3 s-box における最大差分確率を p_s，差分経路での active s-box の総数を α とする．このとき，最大差分特性確率 $\mathcal{P}_d$ は $\mathcal{P}_d \leq p_s^\alpha$ を満たす．また，s-box における最大線形確率を q_s，線形経路での active s-box の総数を β とすると，最大線形特性確率 $\mathcal{P}_l$ についても $\mathcal{P}_l \leq q_s^\beta$ が成り立つ．

なお，active s-box の総数 α，β は分岐数 $\mathcal{B}$ と段数に依存するので，この観点からも分岐数 $\mathcal{B}$ が大きいほど望ましい．

3. 線形変換層の探索手法

本章では，2.1 節で示した SPN 構造における最適な線形変換層を探索する手法を示す．なお，“最適である” とは，線形変換層の中で差分解読法や線形解読法に対する安全性が最も高くなることと，n-bit XOR の個数が最少となる構成であることの両方を同時に満たすことを意味するものとする．

3.1 行列 P の決定

行列 P は線形変換層の入力データと出力データとの関係を表しているだけであり，線形変換層の構成を規定しているわけではない．逆にいえば，線形変換層の実現構成（実装）が違っても，それらの線形変換層の入力データと出力データとの関係を表す行列 P が同じであるならば，それらは同じ特性を持つものと判断できる．つまり，ある行列 P が与えられたとき，それを実現する線形変換層の構成は一般に複数存在することになるが，それらはいずれも同じ特性を持つことを意味する．

そこで，第 1 ステップとして，差分解読法および線形解読法に対する安全性が高くなるような行列 P を決定する．ここで，差分解読法や線形解読法に対する安全性が高いということは，2.2 節の定義からも分かるように，線形変換層の分岐数 $\mathcal{B}$ が最大になることと同値であることに注意されたい．

(1) 差分特性について

2 つのデータ a，a^* の差分を $\Delta a = a \oplus a^*$ と表すとする．このとき，GF(2) 上の $m \times m$ 行列による線形変換層による差分値の変化（差分特性）は

$$\begin{aligned}\Delta y_j = y_j \oplus y_j^* &= (\oplus_{i=1}^{m} p_{ji} x_i) \oplus (\oplus_{i=1}^{m} p_{ji} x_i^*) \\ &= \oplus_{i=1}^{m} p_{ji}(x_i \oplus x_i^*) \\ &= \oplus_{i=1}^{m} p_{ji} \Delta x_i\end{aligned}$$

と表されるので，差分特性に対する分岐数 $\mathcal{B}_d$ は線形変換層に対する分岐数 $\mathcal{B}$ と一致する．したがって，GF(2) 上の $m \times m$ 行列 P の行列要素の候補は，以下の探索アルゴリズムによって決定される．

探索アルゴリズム

Step1 安全性しきい値 T $(2 \leq T \leq m)$ を設定する．

Step2 ハミング重みが $T - 1$ 以上となる列ベクトルの集合 C を用意する．

Step3 C より m 個の列ベクトルの組 P_c を選択する．すべての組を検査し終わるまで以下を繰り返す．

Step3-1 P_c について，分岐数 B_d を求める．このことを $B_d(P_c)$ と書く．

Step3-2 $B_d(P_c) \geq T$ ならば，その m 個の列ベクトルで構成される行列 P_c を候補行列として採用する．

Step4 すべての候補行列の中で，最大の分岐数 B_d の値を与える行列 P と $\mathcal{B}_d = B_d(P)$ の値を出力する．また，候補行列が 1 つもなければ “NULL” を出力する．

安全性しきい値 T は，候補行列における差分特性の分岐数 $\mathcal{B}_d$ を T 以上に限定する値であると同時に，Step2 で効率良く探索の枝切りを行い，行列の探索範囲を制限するために利用する値である．設計者としては，$\mathcal{B}_d$ が最大となるような行列 P を求めたいのであるから，T を $T = m, m-1, \ldots, 3, 2$ の順に減らしていくことで，候補行列 P を効率良く発見できる．

(2) **線形特性について**

データ a に関する，ある特定されたビット位置での値の排他的論理和を $a \cdot \Gamma a$ で表すものとする．ここで，$\cdot$ はベクトルの内積を表す．また，Γa は，その特定されたビット位置を表すためのベクトル情報であり，マスクという．このとき，GF(2) 上の $m \times m$ 行列による線形変換層に対して，差分特性と線形特性の間に以下に示すような双対性が存在する．

定理 1 線形変換層が全単射であり，GF(2) 上の $m \times m$ 行列 P で表されているとする．このとき，マスク値の変化（線形特性）は，P の転置行列 P^t で与えられる．すなわち，

$$\Gamma x_j = \oplus_{i=1}^{m} [p_{ji}]^t \Gamma y_i = \oplus_{i=1}^{m} p_{ij} \Gamma y_i$$

ただし，$\Gamma X = (\Gamma x_1, \Gamma x_2, \ldots, \Gamma x_m) \in \mathrm{GF}(2^n)^m$ は線形変換層の入力マスク値，$\Gamma Y = (\Gamma y_1, \Gamma y_2, \ldots, \Gamma y_m) \in \mathrm{GF}(2^n)^m$ は出力マスク値である．

（証明）線形変換層は，$y_i = \oplus_{j=1}^{m} p_{ij} x_j$ で表されるので，

$$\begin{aligned} Y \cdot \Gamma Y &= \oplus_{i=1}^{m} \left((\oplus_{j=1}^{m} (p_{ij} \cdot x_j)) \cdot \Gamma y_i \right) \\ &= \oplus_{i=1}^{m} \left(\oplus_{j=1}^{m} (p_{ij} \cdot x_j \cdot \Gamma y_i) \right) \\ &= \oplus_{j=1}^{m} \left((\oplus_{i=1}^{m} (p_{ij} \cdot \Gamma y_i)) \cdot x_j \right) \end{aligned}$$

となる．一方，線形変換層は全単射かつ線形変換との仮定より，$X \cdot \Gamma X = Y \cdot \Gamma Y$ を満たす．したがって，$X \cdot \Gamma X = \oplus_{j=1}^{m} (x_j \cdot \Gamma x_j)$ であるので，

$$\Gamma x_j = \oplus_{i=1}^{m} p_{ij} \Gamma y_i = \oplus_{i=1}^{m} [p_{ji}]^t \Gamma y_i$$

が導かれる．

Q.E.D.

定理 1 により，線形特性に対する分岐数 $\mathcal{B}_l$ は，行列 P の転置行列 P^t で表される線形変換層に対する分岐数と一致する．この値は必ずしも線形変換層の分岐数 $\mathcal{B}$ と一致するとは限らないので，前述の探索アルゴリズムから得られた候補行列について，その転置行列の分岐数を検査する必要がある（その転置行列について Step3 を再検査する）．この検査の結果，$\mathcal{B}_l \geq T$ となることが示された候補行列が，最終的に差分解読法および線形解読法に対する安全性が高い線形変換層を表す行列 P となる．なかでも，$\mathcal{B}_d$，$\mathcal{B}_l$ とも最大値をとる行列 P が最適な線形変換層を構成する候補となる．

3.2 線形変換層の構成の決定方法

行列 P が与えられたとき，それに対応する線形変換層の構成を決める手法を示す．ここでは，n-bit XOR の個数が最少となる構成を最適な構成であるとする．具体的に構成を求める手法は以下のとおりである．

構成決定アルゴリズム

Step1 2 つの行を選択し，一方の行（a 行）について，もう一方の行（b 行）との XOR 演算を行う．これを基本演算と呼ぶ．

Step2 基本演算のみを用いて，行列 P が単位行列 I になるように変形を行い，そのときに行った基本演算の回数を数える．そして，基本演算の回数が最少となるような変形手順を求める．

Step3 線形変換層を構成するために，Step2 で求めた変形手順の逆順に，そのときの基本演算で選択した a 行，b 行に相当する第 a データ，第 b データについて，第 a データに第 b データとの XOR 結線を行う

例として，

$$P_E = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

について考える．構造決定アルゴリズムによって，行列 P_E の 2 行目に 1 行目を加え，次に 1 行目に 4 行目を加える，というように繰り返していき，単位行列 I になるまで変形を行う．具体的な変形の様子を以下に示す．

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow[(1 \to 2)]{} \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\xrightarrow[(4 \to 1)]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

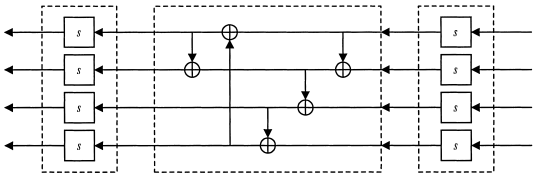

図 2 行列 P_E による線形変換層の構成例
Fig. 2 Example of linear transformation layer represented as the matrix P_E.

$$\xrightarrow[(3\to 4)]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow[(2\to 3)]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow[(1\to 2)]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

上記の変形では，5 回の基本演算で行列 P_E から単位行列 I に変形されている☆．つまり，行列 P_E で表されるような線形変換層は 5 つの XOR で構成できることを示している．具体的には，上記変形の逆順に，まず第 2 データに第 1 データとの XOR 結線を行い，次に第 3 データに第 2 データとの XOR 結線を行う，というように XOR 結線を行っていく．このようにして結線を行った結果，行列 P_E で表される線形変換層は**図 2** の構成となる．

4. $8n$-bit 線形変換層の設計

本章では，$m = 8$ のときの線形変換層の設計について具体的に考察する．

4.1 行列 P の決定方法

3.1 節の探索アルゴリズムを用いて，$\mathcal{B}_d$ が最大となるような 8×8 行列 P を求める．ただし，線形変換層は全単射，すなわち $\mathrm{rank}(P) = 8$ であるとする．

このとき，$m = 8$ での分岐数 B_d を以下のように求めることができる．なお，以下の添え字 i はすべて $1 \le i \le 8$ であり，p_{ij} は GF(2) 上の行列 P の i 行 j 列の要素である．

定義 4 B_d を，以下の示す B_0 から B_{10} の中の最小値であると定義する．

- 任意の 1 列（a 列）について，

$$B_0 = 1 + \min_{a} \#\{p_{ia} | p_{ia} \neq 0\}$$

- 任意の 2 列（a, b 列）について，

$$B_1 = 2 + \min_{(a,b)} \#\{(p_{ia}, p_{ib}) | p_{ia} \oplus p_{ib} \neq 0\}$$

- 任意の 3 列（a, b, c 列）について，

$$B_2 = 3 + \min_{(a,b,c)} \#\{(p_{ia}, p_{ib}, p_{ic}) | p_{ia} \oplus p_{ib} \oplus p_{ic} \neq 0\}$$

$$B_3 = 3 + \min_{(a,b,c)} \#\{(p_{ia}, p_{ib}, p_{ic}) | ((0,0,0),(1,1,1)) \text{ 以外}\}$$

- 任意の 4 列（a, b, c, d 列）について，

$$B_4 = 4 + \min_{(a,b,c,d)} \#\{(p_{ia}, p_{ib}, p_{ic}, p_{id}) | condA\}$$

$$condA = \left\{ \begin{array}{l} (0,0,0,1),(0,0,1,0), \\ (0,1,0,0),(1,0,0,0), \\ (0,1,1,1),(1,0,1,1), \\ (1,1,0,1),(1,1,1,0) \end{array} \right\}$$

$$B_5 = 4 + \min_{(a,b,c,d)} \#\{(p_{ia}, p_{ib}, p_{ic}, p_{id}) | condB\}$$

$$condB = \left\{ \left[\begin{array}{l} (0,0,0,0),(1,1,0,0), \\ (0,1,1,1),(1,0,1,1) \end{array} \right] \text{以外} \right\}$$

$$B_6 = 4 + \min_{(a,b,c,d)} \#\{(p_{ia}, p_{ib}, p_{ic}, p_{id}) | condC\}$$

$$condC = \left\{ \left[\begin{array}{l} (0,0,0,0),(1,0,1,0), \\ (0,1,1,1),(1,1,0,1) \end{array} \right] \text{以外} \right\}$$

$$B_7 = 4 + \min_{(a,b,c,d)} \#\{(p_{ia}, p_{ib}, p_{ic}, p_{id}) | condD\}$$

$$condD = \left\{ \left[\begin{array}{l} (0,0,0,0),(1,0,0,1), \\ (0,1,1,1),(1,1,1,0) \end{array} \right] \text{以外} \right\}$$

$$B_8 = 4 + \min_{(a,b,c,d)} \#\{(p_{ia}, p_{ib}, p_{ic}, p_{id}) | condE\}$$

$$condE = \left\{ \left[\begin{array}{l} (0,0,0,0),(0,1,1,0), \\ (1,0,1,1),(1,1,0,1) \end{array} \right] \text{以外} \right\}$$

$$B_9 = 4 + \min_{(a,b,c,d)} \#\{(p_{ia}, p_{ib}, p_{ic}, p_{id}) | condF\}$$

$$condF = \left\{ \left[\begin{array}{l} (0,0,0,0),(0,1,0,1), \\ (1,0,1,1),(1,1,1,0) \end{array} \right] \text{以外} \right\}$$

$$B_{10} = 4 + \min_{(a,b,c,d)} \#\{(p_{ia}, p_{ib}, p_{ic}, p_{id}) | condG\}$$

$$condG = \left\{ \left[\begin{array}{l} (0,0,0,0),(0,0,1,1), \\ (1,1,0,1),(1,1,1,0) \end{array} \right] \text{以外} \right\}$$

B_0〜B_{10} は，直感的にいえば，線形変換層への入力差分の非零要素数 $w(\Delta X)$ が決められた（右辺第 1 項）ときに出力差分の非零要素数 $w(P(\Delta X))$ の最小

☆ なお，行列 P_E では基本演算回数 5 回が最少であることが実験により確認されている．

値がいくつになるか（右辺第2項）を表しており，その合計の最小値（左辺）が入力差分値 ΔX に対する差分特性の分岐数となる．たとえば，入力差分の非零要素数が2であるとき，その差分値を Δx_a，$\Delta x_b(\neq 0)$ と表す．このとき，$\Delta y_i = p_{ia}\Delta x_a \oplus p_{ib}\Delta x_b$ となり，特に $\Delta x_a = \Delta x_b$ とすると，$\Delta y_i = (p_{ia} \oplus p_{ib})\Delta x_a$ である．したがって，出力差分の非零要素数は

$$\#\{\Delta y_i | \Delta y_i \neq 0\} = \#\{(p_{ia} \oplus p_{ib}) | p_{ia} \oplus p_{ib} \neq 0\}$$

となる．ゆえに，この場合の分岐数は B_1 で与えられることになる．

B_0〜B_3 の導出方法は文献11)に詳しく記述されている．また，B_4〜B_{10} の導出は，4つの非零な入力差分値である x_a，x_b，x_c，x_d の関係ごとに求められる26個の条件の中から選択された7つである．26個から7つを選択する方法は，文献11)に記述されている，任意の3列についての条件式6つから B_2，B_3 の2つを選択した方法と同様の手法により決められる．

3.1節の探索アルゴリズムにより，行列 P を探索した結果，$\mathcal{B}_d \geq 6 = T$ となるような行列は存在せず，$\mathcal{B}_d = 5$ となるような行列は10080個存在した．これらの候補行列はいずれも，列（行）ハミング重みが6となるものが4つ，5となるものが4つ，の合計44となるように構成されている．さらに，これらの行列はすべて，転置行列での分岐数も $\mathcal{B}_l = 5$ となることが確認できる．

4.2 構成決定

上記の10080個について，3.2節で述べた方法により構成を求める．ただし，全数探索的に構成を決めることは，たとえば16個のXOR結線を使うとして，$(8 \times 7)^{16} \approx 2^{93}$ 程度の計算量☆が必要であり，実行不可能である．一方，単位行列から8個のXOR結線で求められる行列のハミング重みは最大42であるので，8個以下のXOR結線で分岐数が5となるような線形変換層を構成することはできない．

そこで，我々は，実用性の観点から $n = 8$ とした64-bitの線形変換層を意識し，さらに現在主流の32-bit CPUで効率的な処理ができるように，処理単位が32-bitとなる構成を考えることにした．具体的には，**図3**(A)に示すように，線形変換層の内部が8入力4出力のボックス4個で構成される構造に限定することにした．各ボックスの内部は，図3(B)に示すように，4つのXORで構成されており，すべての入力ラインが1回ずつXORを通過するものとする．したがって，線形変換層全体では，16個のXOR結線で構成されることになる．このとき，$(4 \times 3 \times 2 \times 1)^4 \approx 2^{18}$ 程度の計算量となり，十分に全数探索が実行可能となる．

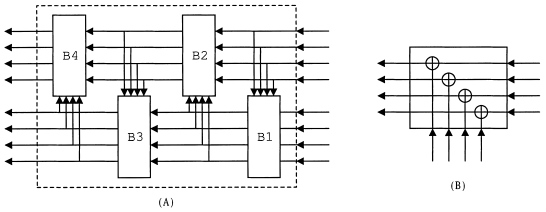

図3 考慮する線形変換層の構造
Fig. 3 Limitation on structures of linear transformation layer.

3.2節のアルゴリズムに従い，上記の10080個の行列のうち，図3の構造を満たしつつ，16回の基本演算で単位行列 I となるものがあるかどうかを探索した．この結果，57個の構成☆☆がみつかった．

その中の1つの行列 P を以下に示す．さらにその行列を利用したラウンド関数の構成図を**図4**に示す．

$$P = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

5. 考察

5.1 符号理論との関連

Rijmenらは文献22)で，符号理論でいうところの最小ハミング距離を差分解読法や線形解読法に対する安全性評価の指標となる分岐数（定義2）として導入した．これにより，線形変換層を行列表現した場合，$(2m, m)$ 線形符号の特性から分岐数 $\mathcal{B}$ の最大値が決定されることになり，最大でも $m + 1$ で抑えられる（Singletonの限界式[25]）．特に，最小ハミング距離が $m + 1$ となる符号を最大距離分離符号（MDS符号：Maximum Distance Separable code）といい，この符号特性を利用して設計された暗号に，SHARK[22]，SQUARE[5]，Rijndael[6]，Twofish[23]，Hierocrypt[21]などがある．

☆ 同じXOR結線を2回続けて行うことはしないなどの条件を設定できるため，現実には 2^{93} の計算量を必要としない．しかし，仮に 2^{32} の計算量が削減できたとしても事実上実行不可能である．

☆☆ 同じ行列でありながら複数の構成をとるものも存在したので，57個の行列が選択されたわけではない．

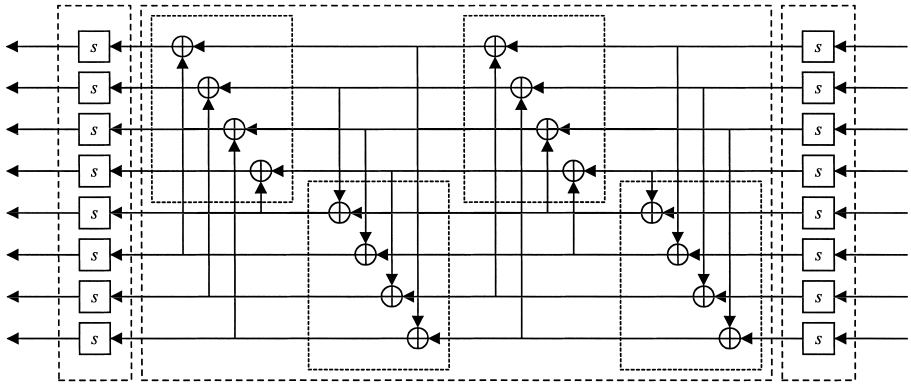

図 4 $m = 8$ の場合の線形変換層の構成例
Fig. 4 Example of linear transformation layer in the case of $m = 8$.

Shimizu らは文献 24) で，何らかの形で SPN 構造を有し，線形変換層が行列表現可能な暗号のうち，DES[19]，E2[9]，Twofish，SAFER K-64[16]，CRYPTON[7]，Serpent[1]，Rijndael，SQUARE，SHARK について，分岐数を含む線形変換層の特性を検証している．その中で，本稿が対象としているような GF(2) 上の行列で表される線形変換層の探索は，2 元 $(2m, m)$ 線形符号における最小距離が最大となるような符号語の探索と考えることもできると指摘している．さらに，符号理論により，2 元 $(16, 8)$ 線形符号での最小距離の最大値が 5 であることが確認できるので，4 章で示した分岐数 $\mathcal{B}_d = \mathcal{B}_l = 5$ が最大であることが理論的にも保証される．

差分解読法や線形解読法に対する安全性の観点からは，分岐数が大きいほど望ましいことはすでに述べた．その意味で，MDS 符号を利用するほうが分岐数を理論的最大値にすることができることから，安全性の観点だけを重視して線形変換層を設計するのであれば，2 元線形符号を利用するよりも MDS 符号を利用するほうが望ましいと考えられる．しかし，現実には，MDS 符号を暗号設計に用いる場合でも，実装上の都合☆により，ほとんどの場合，GF(2^8) または GF(2^4) 上の $(8, 4, 5)$ 線形符号を利用することになる．したがって，MDS 符号を利用している線形変換層であっても実際の分岐数は 5 であり，2 元 $(16, 8)$ 線形符号を利用した線形変換層の分岐数と変わらないことに注意されたい．

5.2 GF(2) 上の行列表現による線形変換層の特徴

GF(2) 上の行列で表現される線形変換層では XOR だけで実装可能であることから，様々な等価変形した実装を容易に作り出すことができる．たとえば，$m = n = 8$ のときの図 4 に示した構成では，**図 5** や**図 6** に示す等価変換した構成を作り出すことができる．図 5 では，線形変換層の入力側にある s-box を 8-bit 入力 32-bit 出力の置換表とすることにより，線形変換層はわずか 8 個の 32-bit XOR と 1 回の巡回シフトだけで実装されることが分かる[3]．また，図 6 では，線形変換層の処理を 32-bit レジスタとすることにより，4 個の 32-bit XOR と 4 回の巡回シフトおよび s-box の結果の 32-bit レジスタへ入力（一般には 6 回のシフトと 6 個の 32-bit OR の組合せで実現可能）で実装できる．**表 1** に線形変換層の入力側にある s-box と組み合わせたときの実装結果をまとめる．ここでは，s-box は 1 種類であるとする．なお，ここであげた実装例以外にも等価な構成を作ることができることに注意されたい．

表 1 に示すように，使用メモリ量や基本演算のサイ

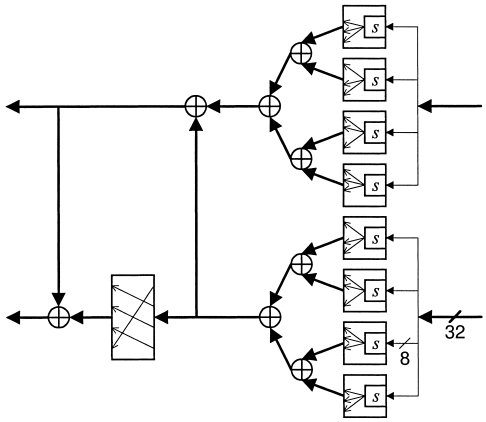

図 5 32-bit 処理単位での線形変換層の構成例（PC 向き）
Fig. 5 Example of linear transformation layer based on 32-bit operations (for PCs).

☆ 現在の実装環境の主流は 32-bit PC クラスであると考えてよいので，32-bit PC クラスで高速な処理が可能となる必要がある．

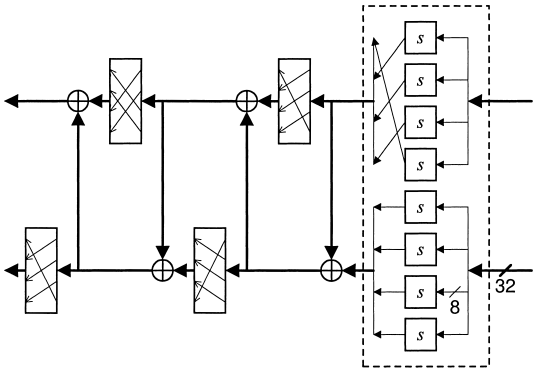

図 6 少メモリ，32-bit 処理単位での線形変換層の構成例（高機能 IC カード向き）
Fig. 6 Example of linear transformation layer based on 32-bit operations and small memory requirement (for high-end smart cards).

表 1 $m = n = 8$ としたときの実装例
Table 1 Implementation examples in the case of $m = n = 8$.

	図 4	図 5	図 6
s-box の実装メモリ量	256B	4KB	256B
主な演算単位	8-bit	32-bit	32-bit
8-bit XOR 回数	16	0	0
32-bit XOR 回数	0	8	4
巡回シフト回数	0	1	4
シフト回数	0	0	6
OR 回数	0	0	6

ズなどの実装環境に応じて，実際の実装方法を使い分けることができる点が GF(2) 上の行列表現による線形変換層の特徴である．

5.3 最大差分特性確率・最大線形特性確率の上界値

2.2 節で述べたように，SPN 構造における差分解読法や線形解読法に対する安全性評価として線形変換層の分岐数が用いられてきた．具体的には，図 1 に示すような線形変換層が非線形変換層に挟まれる構造であるとき，active s-box の定義と分岐数の定義式の関係から，active s-box の個数と分岐数が等しい．

このことから，暗号全体が**図 7** のように線形変換層と非線形変換層との繰返しで構成されている SPN 暗号について，以下の結果が知られている．

定理 2（SPN 暗号に対する安全性評価[22]）s-box の最大差分確率を p_s，差分特性に対する線形変換層の分岐数を $\mathcal{B}_d$ とする．このとき，$2r$ 段の SPN 暗号での最大差分特性確率の上界値は $p_s^{r\mathcal{B}_d}$ で与えられる．また，s-box の最大線形確率を q_s，線形特性に対する線形変換層の分岐数を $\mathcal{B}_l$ とすると，同様に最大線形特性確率の上界値は $q_s^{r\mathcal{B}_l}$ で与えられる．

この定理が SHARK の提案以降の SPN 暗号における差分解読法や線形解読法に対する安全性の評価指標となっている．

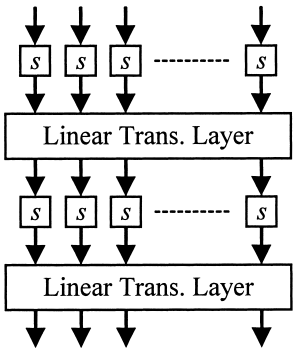

図 7 SPN 暗号
Fig. 7 SPN ciphers.

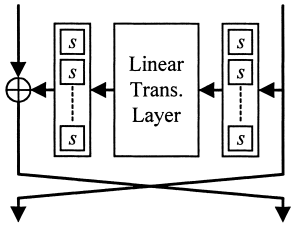

図 8 S-P-S 型ラウンド関数を利用した Feistel 暗号
Fig. 8 Feistel ciphers with S-P-S round function.

これに対し，Feistel 暗号は，暗号全体としてみれば，線形変換層と非線形変換層との繰返しで構成されているわけではないので，active s-box の個数と分岐数との関係から暗号全体の安全性を検討した結果はなかった．そこで，我々は Feistel 暗号においても SPN 暗号と同様の評価指標を求めている．詳細については，紙面数の都合上別稿にて報告するので，ここでは結果のみを報告する．

定理 3（文献 10)）ラウンド関数の構造が**図 8** で表されている Feistel 暗号であるとする．また，s-box の最大差分確率と最大線形確率をそれぞれ p_s，q_s とし，差分特性と線形特性に対する線形変換層の分岐数をそれぞれ $\mathcal{B}_d$，$\mathcal{B}_l$ とする．このとき，ラウンド関数が全単射であるならば，最大差分特性確率と最大線形特性確率の上界値はそれぞれ以下のように表される．

$$\begin{aligned} &3r,\ 3r+1 \text{ 段のとき} \ : \ p_s^{2r\mathcal{B}_d},\ q_s^{2r\mathcal{B}_l} \\ &3r+2 \text{ 段のとき} \quad : \ p_s^{(2r+1)\mathcal{B}_d},\ q_s^{(2r+1)\mathcal{B}_l} \end{aligned}$$

定理 4（文献 8)）ラウンド関数の構造が**図 9** で表されている Feistel 暗号であるとする．また，s-box の最大差分確率と最大線形確率をそれぞれ p_s，q_s とし，差分特性と線形特性に対する線形変換層の分岐数をそれぞれ $\mathcal{B}_d$，$\mathcal{B}_l$ とする．このとき，ラウンド関数が全

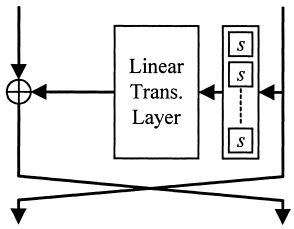

図 9 S-P 型ラウンド関数を利用した Feistel 暗号
Fig. 9 Feistel ciphers with S-P round function.

単射であるならば，$4r$ 段 Feistel 暗号における最大差分特性確率と最大線形特性確率の上界値は

$$p_s^{r\mathcal{B}_d+\lfloor r/2\rfloor},\ q_s^{r\mathcal{B}_l+\lfloor r/2\rfloor}$$

と表される．

5.4 実装環境の変化

本稿では，4 章で線形変換層の構成例を示すとき，安全性と 32-bit CPU における効率的な実装との両立を特に意識した．これは，現在の主流となっている計算機環境が 32-bit CPU であることを反映したものである．

しかし，本稿で述べた考え方そのものは，32-bit CPU での効率的な線形変換層の設計に限定されるものではない．たとえば，行列 P を 16×16 行列とすれば，128-bit のラウンド関数での構成に利用できるであろう．

また，実際の効率的な線形変換層の構成を決定する際にも，図 3 であげるような構造の代わりに，並列処理性などに適したラウンド関数の構造を反映して，線形変換層の構成を探索することも可能である．本稿で指摘したい重要なことは，“ラウンド関数の構造を反映するルール” に従って，行列 P から単位行列 I になるように変形すること（構造決定アルゴリズム Step2）によって，実際の線形変換層が構成されるという点である．求められた線形変換層が効率的に実装できるかどうかは，定めたルールが効率的に実装できるようなラウンド関数の構造を反映したものであるかに依存している．つまり，このルール自体が設計すべき計算機環境に依存して決まるのである．

6. ま と め

本稿では，SPN 構造における線形変換層の設計について検討した．具体的には，線形変換層を，GF(2) 上の $m\times m$ 行列 P として表現した後，行列 P および差分特性と線形特性に対する線形変換層の分岐数の最大値を利用して構成する方法を述べた．これにより，差分解読法や線形解読法に対して耐性を有するような線形変換層を効率良く設計できる．例として $m=8$ の場合を取り上げ，このアルゴリズムを用いた線形変換層の分岐数が 5 となる最適な線形変換層の構成例を示した．その際，最適な安全性を持つ線形変換の候補の中から特に 32-bit CPU で効率的な実装が可能となるものを選択し，実際に線形変換層を構成した．また，XOR のみで構成される線形変換層は，実装環境に応じた様々な効率的な実装に等価変形できることも示した．

さらに，線形変換層における行列表現と符号理論との関係や，暗号全体の最大差分特性確率や最大線形特性確率の上界値と線形変換層の分岐数との関係などについても考察を行った．

本稿での成果は，128 ビットブロック暗号 E2[9] ならびに Camellia[2] でのラウンド関数における線形変換層の設計に利用されている．両方の暗号で利用されている線形変換層も実際に図 4 と同様にして求められたもので，分岐数も $\mathcal{B}_d=\mathcal{B}_d=5$ となる最適なものである．したがって，暗号全体としての差分解読法や線形解読法に対する安全性が定理 3 もしくは定理 4 により評価され，これらの解読法に対して安全であることが示されている．

参 考 文 献

1) Anderson, R., Biham, E. and Knudsen, L.R.: SERPENT, *The 1st Advanced Encryption Standard Candidate Conference* (1998). `http://www.cl.cam.ac.uk/~rja14/serpent.html`
2) Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J. and Tokita, T.: Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms, *Selected Areas in Cryptography—7th Annual International Workshop, SAC2000*, Lecture Notes in Computer Science, Vol.2012, pp.39–56, Springer-Verlag, Berlin (2001).
3) Aoki, K. and Ueda, H.: Optimized Software Implementations of *E2*, *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E83-A, No.1, pp.101–105 (2000).
4) Biham, E. and Shamir, A.: Differential cryptanalysis of DES-like cryptosystems, *Journal of Cryptology*, Vol.4, No.1, pp.3–72 (1991). The extended abstract appeared at *CRYPTO'90*.
5) Daemen, J., Knudsen, L.R. and Rijmen, V.: The block cipher SQUARE, *Fast Software Encryption—4th International Workshop, FSE'97*, Lecture Notes in Computer Sci-

ence, Vol.1267, pp.149–165, Springer-Verlag, Berlin (1997).
6) Daemen, J. and Rijmen, V.: RIJNDAEL, *The 1st Advanced Encryption Standard Candidate Conference* (1998). `http//www.esat. kuleuven.ac.be/~rijmen/rijndael/`
7) Future Systems, Inc.: CRYPTON, *The 1st Advanced Encryption Standard Candidate Conference* (1998). `http//crypt.future. co.kr/~chlim/crypton.html`
8) Kanda, M.: Practical Security Evaluation against Differential and Linear Cryptanalyses for Feistel Ciphers with SPN Round Function, *Selected Areas in Cryptography—7th Annual International Workshop, SAC2000*, Lecture Notes in Computer Science, Vol.2012, pp.324–338, Springer-Verlag, Berlin (2001).
9) Kanda, M., Moriai, S., Aoki, K., Ueda, H., Takashima, Y., Ohta, K. and Matsumoto, T.: *E2*—A New 128-Bit Block Cipher, *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E83-A, No.1, pp.48–59 (2000).
10) Kanda, M., Takashima, Y. and Matsumoto, T.: A round function structure consisting of few *s*-boxes (Part I) (in Japanese), IEICE Technical Report, ISEC97-18 (1997).
11) Kanda, M., Takashima, Y. and Matsumoto, T.: A round function structure consisting of few *s*-boxes (Part II) (in Japanese), *The 1998 Symposium on Cryptography and Information Security, SCIS'98*, 2.2.D (1998).
12) Kanda, M., Takashima, Y., Matsumoto, T., Aoki, K. and Ohta, K.: A strategy for constructing fast round functions with practical security against differential and linear cryptanalysis, *Selected Areas in Cryptography—5th Annual International Workshop, SAC'98*, Lecture Notes in Computer Science, Vol.1556, pp.264–279, Springer-Verlag, Berlin (1999).
13) Kaneko, Y. and Matsumoto, T.: Effectiveness of Outline Measures of Strength against Differential and Linear Cryptanalysis, *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E82-A, No.1, pp.130–133 (1999).
14) Knudsen, L.R.: Practically Secure Feistel Ciphers, *Fast Software Encryption—Cambridge Security Workshop*, Lecture Notes in Computer Science, Vol.809, pp.211–221, Springer-Verlag, Berlin (1994).
15) Lai, X., Massey, J.L. and Murphy, S.: Markov ciphers and differential cryptanalysis, *Advances in Cryptology—EUROCRYPT'91*, Lecture Notes in Computer Science, Vol.547, pp.17–38, Springer-Verlag, Berlin (1991).
16) Massey, J.L.: SAFER-K64: A Byte Oriented Block-Ciphering Algorithm, *Fast Software Encryption—Cambridge Security Workshop*, Lecture Notes in Computer Science, Vol.809, pp.1–17, Springer-Verlag, Berlin (1994).
17) Matsui, M.: Linear cryptanalysis method for DES cipher, *Advances in Cryptology—EUROCRYPT'93*, Lecture Notes in Computer Science, Vol.765, pp.386–397, Springer-Verlag, Berlin (1994).
18) Matsui, M.: New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis, *Fast Software Encryption—Third International Workshop*, Lecture Notes in Computer Science, Vol.1039, pp.205–218, Springer-Verlag, Berlin (1996).
19) National Bureau of Standards: *Data Encryption Standard*, FIPS-PUB-46 (1977).
20) Nyberg, K.: Linear Approximation of Block Ciphers, *Advances in Cryptology—EUROCRYPT'94*, Lecture Notes in Computer Science, Vol.950, pp.439–444, Springer-Verlag, Berlin (1995).
21) Ohkuma, K., Muratani, H., Sano, F. and Kawamura, S.: The Block Cipher Hierocrypt, *Selected Areas in Cryptography—7th Annual International Workshop, SAC2000*, Lecture Notes in Computer Science, Vol.2012, pp.72–88, Springer-Verlag, Berlin (2001).
22) Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A. and Win, E.D.: The cipher SHARK, *Fast Software Encryption—3rd International Workshop*, Lecture Notes in Computer Science, Vol.1039, pp.99–112, Springer-Verlag, Berlin (1996).
23) Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. and Ferguson, N.: Twofish, *The 1st Advanced Encryption Standard Candidate Conference* (1998). `http//www.counter pane.com/twofish.html`
24) Shimizu, H. and Kaneko, T.: On the Diffusion Layer of Block Ciphers (in Japanese), IEICE Technical Report, ISEC99-72 (1999).
25) Singleton, R.C.: Maximum Distance *Q*-nary Codes, *IEEE Trans. Inf. Theory*, Vol.IT-10, pp.116–118 (1964).

(平成 12 年 11 月 29 日受付)
(平成 13 年 3 月 9 日採録)

神田 雅透

昭和 44 年生．平成 3 年東京工業大学工学部（電気電子工学）卒業，平成 5 年同大学院修士課程修了．同年日本電信電話株式会社（NTT）入社．情報セキュリティに関する研究と実用化に従事．現在，NTT 情報流通プラットフォーム研究所研究主任．平成 10 年より横浜国立大学大学院博士課程在籍．電子情報通信学会，IACR 各会員．

高嶋 洋一

昭和 37 年生．昭和 60 年横浜国立大学工学部（情報工学）卒業，昭和 62 年同大学院修士課程修了．平成 2 年同大学院博士課程（電子情報工学）修了，工学博士．同年日本電信電話株式会社（NTT）入社．画像符号化に関する研究を経て情報セキュリティに関する研究開発に従事．現在，著作権保護システムに関する研究開発に従事．NTT サイバーソリューション研究所主任研究員．電子情報通信学会会員．情報理論とその応用学会会員．

松本 勉（正会員）

昭和 33 年生．昭和 61 年東京大学大学院博士課程（電子工学）修了，工学博士．同年横浜国立大学工学部専任講師．現在，同大学大学院環境情報研究院教授．昭和 56 年より主として暗号や情報セキュリティの研究・教育に従事.「明るい暗号研究会」を数人の仲間とともに創り研究をはじめた．ASIACRYPT'96（韓国，慶州）プログラム委員長．ASIACRYPT 2000（京都，国際暗号学会主催）実行委員長．電子情報通信学会より「情報セキュリティの基礎理論」への貢献に関して業績賞を受賞．

青木和麻呂

昭和 44 年生．平成 5 年早稲田大学理工学部（数学科）卒業，平成 7 年同大学院修士課程修了．同年より平成 13 年まで NTT 研究所に勤務．その間，情報セキュリティの研究と実用化に従事．現在，NTT コミュニケーションズに勤務．理学博士．電子情報通信学会 SCIS 論文賞（平成 7，8 年），学術奨励賞（平成 9 年）受賞．

太田 和夫（正会員）

昭和 29 年生．昭和 54 年早稲田大学大学院修士課程修了．同年より平成 13 年まで日本電信電話公社（現 NTT）研究所に勤務．その間，情報セキュリティの研究と実用化に従事．平成 3〜4 年，Massachusetts Institute Technology 客員研究員．平成 7〜10 年，電気通信大学大学院客員教授．平成 9 年〜現在，早稲田大学理工学部情報学科非常勤講師．平成 11〜12 年，Massachusetts Institute Technology 客員教授．現在，電気通信大学情報通信工学科教授．理学博士．電子情報通信学会業績賞，小林記念特別賞（平成 5 年），電気通信普及財団テレコムシステム技術賞受賞（平成 10 年）.「情報セキュリティの科学」（講談社 ブルーバックス，共著),「暗号と認証」（培風館 情報理論とその応用シリーズ 4，共著),「暗号・ゼロ知識証明・数論」（共立出版，共編),「計算理論の基礎」（共立出版，監訳）等．