解　説　論　文

# 共通鍵暗号の安全性評価

Cryptanalysis on Common Key Ciphers

**金子敏信** Toshinobu KANEKO

**アブストラクト**　共通鍵ブロック暗号の安全性評価技術は，全数探索法とショートカット法に分類される．ショートカット法は，暗号アルゴリズムの内部構造の知識を利用して，攻撃の効率化を図る方法である．本稿では，1990 年以降の代表的な，ショートカット法である，差分攻撃，線形攻撃，高階差分攻撃から最近の，AES に対する関連鍵攻撃や Biclique 攻撃まで，その原理を紹介する．

**キーワード**　共通鍵ブロック暗号，安全性評価 ，差分攻撃，線形攻撃，高階差分攻撃，関連鍵攻撃，Biclique 攻撃

**Abstract**　There are two types of methods for evaluating the security of common key block ciphers: brute-force attacks and short-cut methods. For the latter, we investigate the internal structure of the cipher to find a defect and use it for an attack. In this paper, we illustrate the principles of the following typical short-cut methods from 1990 to 2012: differential cryptanalysis, linear cryptanalysis, higher-order differential attack, related-key attack for AES, and biclique attack methods.

**Key words**　Common key block cipher，Security evaluation，Differential cryptanalysis，Linear cryptanalysis, Higher-order differential attack, Related-key attack, Biclique attack

## 1. はじめに

公の研究対象としての暗号は，1976 年に米連邦政府標準として制定された DES(Data Encryption Standard) に始まる[1]．制定時においては，鍵の長さ (56 bit) に関し論争があった[2]．鍵の総当りで解読する方法を，全数探索法 (Brute Force Method) という．全数探索法は，暗号アルゴリズムの内部構造には関係なく，任意の暗号に対し適用できるが，基本的には $2^{\text{鍵ビット数}}$ 回の暗号化計算量となる．これに対し，暗号アルゴリズムの内部構造に関する知識を利用し，少ない計算量で攻撃を目指す手法をショートカット法 (Short Cut Method) という．

本稿では，以下，主要なショートカット法について紹介する．1990 年までは，DES に関し，全数探索法よりも効率の良い解読法は，発見されていなかった．Biham と Shamir により提案された差分攻撃 (Differential cryptanalysis) は，ショートカット法の一つであり，暗号アルゴリズム構成部品における，差分伝搬特性を積み上げ，平文差分と暗号文差分の相関を利用して，鍵を推定する方法である．全数探索より少ない計算量で攻撃が可能であるという初めての見積もりを，1992 年に示している[3]．

計算機実験を含めて，DES が，全数探索より少ない計算量で，攻撃可能であることを示したのは 1993 年の松井による線形解読 (Linear cryptanalysis)[4],[5]である．そこでは，構成部品の入出力の線形相関を線形近似式として表現し，それを積み上げることにより，平文，暗号文間の線形近似式を線形特性として導き，利用する．

差分攻撃，線形攻撃は，ラウンド関数を繰り返す構造の共通鍵暗号に対し汎用に適用できる攻撃法であり，それに対処すべく暗号設計理論も進歩し，差分／線形攻撃に対する証明可能安全性の理論となった[6]～[8]．この理論では，差分攻撃／線形攻撃のみに対する安全性しか保障されない．1994 年に Knudsen は，差分／線形攻撃に対する証明可能安全性を持つプロトタイプ暗号 $\mathcal{KN}$ が，高階差分攻撃で容易に解読できることを示している[9]．高階差分 (Higher order diffarential) は，Lai が提案し[10]，XOR 差分の概念を複数回繰り返し適用するものであるが，差分攻撃における差分伝搬とは異なり，確率的な概念は用いられていない．

ハードウェア能力の進歩，暗号解読技術の進展に配慮し，NIST は，1997 年に DES の後継暗号を公募した．後継標準暗号 AES(Advanced Encryption Standard)[11]は，Daemen, Rijimen の提案する Rijndael[12]を基にしたものである．

AES は，SPN 構造を持ち，差分／線形解読に対する証明可能安全性を持つ暗号である．これら解読法に対しては 4 段で，安全性が保障される(注1)．平文を攻撃者が自由に選び対応する暗号文を得て攻撃を行う選択平文攻撃において，AES に関し最も成果を上げていたのは，Ferguson らの手法[13]である．そこでは

金子敏信　正員：フェロー　東京理科大学理工学部電気電子情報工学科
E-mail　kaneko@ee.noda.tus.ac.jp
Toshinobu KANEKO, Fellow, Member (Faculty of Sciences and Engineering, Tokyo University of Science, Noda-shi, 278-8510 Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.7 No.1 pp.14–29 2013 年 7 月


(注1)：正確には，次章で述べるショートカット部が 4 段以上となると安全．

高階差分攻撃の一種である SQUARE 攻撃を使用し，7 段まで，全数探索より少ない計算量で攻撃可能と見積もられている．

最近になり，仕様段数 (full round) の AES に対して，全数探索より少ない計算量で攻撃が可能とする論文[14],[15]が発表された．

Biryukov らの 2009 年の論文[14]は，攻撃条件として関連鍵攻撃 (Related-Key Cryptanalysis) を想定し，攻撃手法として，差分攻撃の流れを汲むブーメラン攻撃を使用している．共通鍵ブロック暗号の内部構造は通常，データランダム化部と鍵処理部に分かれるが，彼らの攻撃は，この両部分における差分の伝搬を互いに打ち消し合うよう巧妙に接続し，高い確率で成立する特性を構成している．

Bogdanov らの 2011 年の論文[15]では，Biclique（完全 2 部グラフ）攻撃が提案されている．そこでも，データランダム化部と鍵処理部の差分の伝搬を同時に解析し，データ入力差分と鍵差分にある関係を持たせるならば，少ない段数では，互いに干渉せず，入力データを一方の頂点，出力データを他方の頂点とし，枝を鍵集合とする，Biclique 表現が可能であることを利用している．

本稿では，次章で，攻撃条件等を述べ，第 3〜7 章において差分攻撃，線形攻撃，高階差分攻撃，関連鍵攻撃，Biclique 攻撃の原理をまとめる．

## 2. 共通鍵ブロック暗号と攻撃モデル

### 2.1 共通鍵ブロック暗号

代表的な共通鍵ブロック暗号の内部構造を，図 1 に示す．

その内部は，鍵処理部とデータランダム化部に分かれる．前者は，秘密鍵 $K$ から，データランダム化部で使用する段鍵 $K_1, K_2, \ldots$ を生成する．後者は，段鍵 $K_1, K_2, \ldots$ に依存して

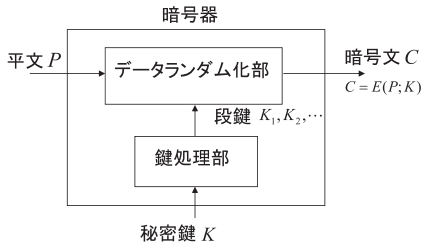



**図 1　共通鍵ブロック暗号**

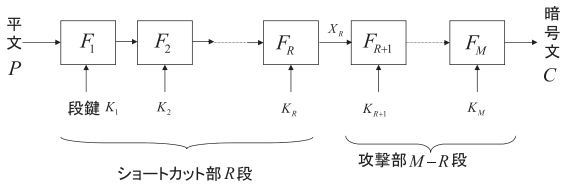



**図 2　データランダム化部**

平文ブロック $P$ をかくはんし，暗号文ブロック $C = E(P;K)$ に変換する．

データランダム化部は，図 2 のように，段関数と呼ばれる比較的簡単な関数を積み重ねた構造 (積暗号 (product cipher)) になっている．各段関数においては，入力データを段鍵 $K_i$ に従いかくはんし出力とする．この段関数の繰返し回数を段数という．

### 2.2 全数探索法とショートカット法

暗号解読とは，与えられた条件下で，秘密鍵 $K$ またはそれと等価なものを見いだすことである．手法は，大別して，全数探索法 (brute force method) とショートカット法 (short cut method) に分かれる．

前者は，鍵総当り法ともいい，計算機能力に依存する方法であり，少数の平文 $P$，暗号文 $C$ 対が与えられたとき，$C = E(P;K)$ の関係を鍵 $K$ の候補の総当りで解く手法である．暗号の内部構造に関する知識を使わない．鍵のビット数を $|K|$ として，その攻撃計算量は，$2^{|K|}$ の暗号化計算となる．鍵のビット数は，計算機の能力の進歩を考えても，探索しつくせない計算量になるように選定される．実際に全数探索法で解いた例として，1999 年の DES Challenge III[16]や 2002 年の RC5-64 Challenge[17]がある．前者では，DES 解読用の専用ハードウェアとネット上の PC の共同作業で 56 bit 鍵を 22 時間で解き，後者は，RC5 の 64 bit 鍵をネット上の PC の共同作業 4 年で解読している．その後，このような解読コンテストはないが，計算機能力の進歩を考えるならば，現在では，80 bit 未満の鍵は，全数探索法の餌食となる可能性があると言える．

後者は，暗号アルゴリズムの内部を解析し，その知識を利用して，全数探索法の計算量 $2^{|K|}$ より少ない計算量で解読を目指す方法であり，本稿で取り上げるのはこちらの話題である．

### 2.3 攻撃条件

共通鍵暗号の攻撃を，攻撃者に許される条件で分類すると以下となる．

**暗号文単独攻撃**　暗号文のみを使う攻撃

**既知平文攻撃**　与えられた平文暗号文組のみを使う攻撃

**選択平文攻撃**　攻撃者が都合が良いように選んだ平文に対応する暗号文を手に入れて行う攻撃

**関連鍵攻撃**　攻撃者が自由に秘密鍵を操作した上で行う選択平文攻撃．なお，鍵の操作は，攻撃が自明とならない範囲に制限される．

後ろに行くほど，攻撃者の自由度は増加し，攻撃は易しくなるが，逆に，そのような攻撃条件が成立する可能性は小さくなる．暗号文単独攻撃は，平文の冗長性（統計的偏り）を利用し，解読するものであり，古典的な暗号に適用例がある．

### 2.4 ショートカット法の基本原理

共通鍵ブロック暗号の，データランダム化部を，図 2 に模式

的に示す．段関数は，$F_1, F_2, \ldots, F_M$ であり，$M$ 段暗号である．この $M$ 段を，$R$ 段のショートカット部と $M-R$ 段の攻撃部に分け，その境界のデータ（$R$ 段目出力）を $X_R$ とする．$i = 1, 2, \ldots$ 組目の平文を $P(i)$，$R$ 段目出力を $X_R(i)$，暗号文を $C(i)$ とする．その関数として特徴量 $\mathcal{H}(X_R(i))$ を選ぶ．特徴量は，同一組 (同一の $i$) 内のデータの関数でもよいし，組間にまたがる $\mathcal{H} = X_R(i) \oplus X_R(i+1)$ 等であってもよいが，次の条件を満たすように選ぶ．

**特徴量 $\mathcal{H}(X_R(i))$ の条件**

（1） 段鍵 $K_1, \ldots, K_R$ によらず，平文 $P(i)$ から推定可能なもの．

1.a 段鍵に依存する場合は，その影響が少ないもの．そのように平文 $P(i)$ を選択することも可．

1.b 確率的推定でもよいが，理想乱数と区別可なもの．

（2） 段関数 $F$ の構成要素の解析結果を容易に，$R$ 段暗号系全体に拡張できるもの．

特徴量の選定ができた場合，平文側から推定された特徴量 $\mathcal{H}(X_R(i))$ と，暗号文 $C(i)$ 側から段鍵 $K_{R+1}, \ldots, K_M$ を使って復号計算で求めた $X_R(i)$ の特徴量を突き合わせすれば攻撃ができる．復号計算を $F^{-1}(C(i); K_{R+1}, \ldots, K_M)$ とすれば，攻撃に使用する方程式は

$$\mathcal{H}(X_R(i)) = \mathcal{H}(F^{-1}(C(i); K_{R+1}, \ldots, K_M)) \qquad (1)$$

となる．これは，未知数 $K_{R+1}, \ldots, K_M$ の方程式であり，平文と暗号文の関係式

$$C = E(P; K_1, K_2, \cdots, K_M) \qquad (2)$$

を使って，暗号系全体を一度に攻撃するのに比べ，容易である．特徴量の推定が確率的に成立する場合，真の段鍵 $K_{R+1}, \ldots, K_M$ であれば高い確率でこの式が成立し，偽の段鍵であれば，$X_R(i)$ を乱数であると考えた程度の確率で成立すると期待され，この確率の違い (成立回数の違い) で，段鍵候補の真偽が判定できる．

どのような特徴量を選ぶかにより，次章以降で紹介する差分攻撃，線形攻撃，高階差分攻撃となる．

ショートカット法は，暗号の内部構造を解析して，導くものであり，そのような考察が不要な全数探索法より，攻撃性能が良くなければ，意味がない．攻撃性能は，攻撃計算量 ($T$)，必要な平文・暗号文対の組数である必要データ量 ($D$)，攻撃アルゴリズムにおいて必要な記憶容量 ($M$) で評価される．

既知平文攻撃の攻撃条件では，鍵のビット数を $|K|$ として，鍵を総当りする全数探索法の攻撃計算量は，$T_B = 2^{|K|}$ である．選択平文攻撃の攻撃条件では，暗号のブロック長を $b$ とするならば，攻撃対象の暗号器を借用して，平文 $P$ を総当たりして，対応する暗号文を手に入れてしまえば，鍵を知らなくても，解読が可能である．これをテーブル法という．これも全数探索と考えるならば，その攻撃のデータ量は $D_B = 2^b$，データ入手に必要な計算量は $T_B = 2^b$ の暗号化計算であるが，攻撃時は，テーブル索引のみであり，計算量は，ほとんど 0 である．この方法の記憶容量は，$M_B = 2^b$ である．特定のショートカット法が，意味を持つのは，その $T$，$D$，$M$ を，このような自明な攻撃のコスト $T_B$,$T_D$,$T_M$ と比較して，何らかの優位性がある場合である．

## 3. 差分攻撃

差分攻撃は，1990 年に Biham らにより提案[18]された手法であり，攻撃条件は，選択平文攻撃である．その後，1992 年に，DES に対し，全数探索法に比べ少ない計算量で攻撃が可能であるとの見積もりを出している[3]．攻撃に必要な平文数は，$2^{47}$ 組である．

### 3.1 差分確率

二つの $n$ bits データ $X$ と $X^*$ の差分（XOR 差分）は

$$X \oplus X^* = \Delta X \qquad (3)$$

である．差分攻撃においてデータは，常に $(X, X^*)$ のように対で考え，その差分値 $\Delta X$ に注目する．

図 2 において，平文対 $(P, P^*)$ を，その差分 $\Delta P = P \oplus P^*$ が攻撃者が決めた値となるように選び，特徴量も対データの差分

$$\mathcal{H}(X_R, X_R^*) = X_R \oplus X_R^* \qquad (4)$$

として捉える．

多くの共通鍵ブロック暗号において段関数 $F$ は，段鍵の XOR 加算と非線形層 (S 層) と線形層（P 層）の縦続接続構造 (SP 構造) である．S 層では，S-box を並列に配置する．S-box は，入出力 bit 数が 4〜8 bit 程度の小さな規模の非線形変換である．図 3 の鍵加算と $n$ bits 入力 S-box を考える．平文対 $(P, P^* = P \oplus \Delta P)$ を入力したとき，S-box 入力対 $(X, X^*)$ の差分は，

$$\Delta X = X \oplus X^* = (P \oplus K) \oplus (P^* \oplus K) = \Delta P \qquad (5)$$

となる．平文差分 $\Delta P$ を固定し，平文 $P$ を一様分布で選んだとき，S-box 入力対 $(X, X^*)$ においては，入力差分 $\Delta X = \Delta P$ で，$X$ が一様分布で選ばれることになる．出力差分が $\Delta Y$ となる確率は，入力差分が $\Delta X$ となる全ての入力対 $2^n$ 通りに対し S-box 出力対を調べることにより，次式となる．これを差分確率 DP（Differential Probability）と呼び $DP(\Delta X \to \Delta Y)$ と表記する．

$$DP(\Delta X \to \Delta Y) = \frac{\#\{X | S(X) \oplus S(X \oplus \Delta X) = \Delta Y\}}{2^n} \qquad (6)$$

ここで，$\#\{X | S(X) \oplus S(X \oplus \Delta X) = \Delta Y\}$ は，$2^n$ 通りの全ての入力対 $(X, X^*) = (X, X \oplus \Delta X)$ に対し，S-box 出力差分が $\Delta Y$ となる回数を表す．入力 bit 数 $n$ が小さければ，全ての

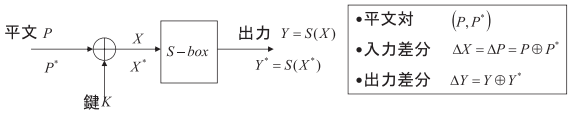



**図 3** S-box と鍵加算

差分の組 $(\Delta X, \Delta Y)$ に対し，計算機による総当りで，差分確率 $DP(\Delta X \to \Delta Y)$ を求めることは，容易いことである．差分確率表を作成する計算量は，素朴に計算する場合，$X$ 及び $\Delta X$ の総当りであり，$2^{2n}$ 回の S-box 計算となる．

この差分確率は，XOR 加算される鍵 $K$ には依存しない．図 3 において，平文 $P$ が一様分布であれば，入力差分 $\Delta P$ に対し，出力差分 $\Delta Y$ が，確率 $DP(\Delta X = \Delta P \to \Delta Y)$ で期待される．

## 3.2 並列 S-box と SP 型 $F$ 関数の差分確率

図 4 のように，S-box が並列に並んだ構造を考える．差分 $\Delta P$ は，鍵の XOR 加算を，そのまま通り抜け $\Delta X = \Delta P$ となるので，この図面で，鍵加算は省略し，また，入力は，$(X, X^*)$ の対で，与えられるが，$X^*$ も省略してある．入力 $X = (X_1, X_2)$ が二つの S-box に入り，出力 $Y = (Y_1, Y_2) = (S_1(X_1), S_2(X_2))$ となる．この構造の差分確率を考える．入力差分 $\Delta X = (\Delta X_1, \Delta X_2)$ に対し，出力差分が $\Delta Y = (\Delta Y_1, \Delta Y_2)$ となる確率は，入力 $X$ が一様分布で選ばれていれば

$$DP(\Delta X \to \Delta Y) = DP(\Delta X_1 \to \Delta Y_1) DP(\Delta X_2 \to \Delta Y_2) \quad (7)$$

と，各 S-box の差分確率の積となる．

図 5 のように $n$ bits 入力 $m$ bits 出力の S-box が $l$ 個，並列に設置され，その後に線形変換 $M$ が配置されている SP 型 $F$ 関数の差分確率も同様に求められる．$N$ bits 入力 $X = (X_1, X_2, \ldots, X_l)$ が並列 S-box で処理され，$ml$ bit の S 層出力 $Y = (Y_1, Y_2, \ldots, Y_l)$ となり，それが $GF(2)$ 上の $N \times ml$ 行列 $M$ で変換され $N$ bits の出力 $Z$ となるとする．差分 $\Delta Y$ も，行列 $M$ で変換され，$F$ 関数出力差分 $\Delta Z = (M \Delta Y^T)^T$ となる(注2)．$\Delta Y$ に対し $\Delta Z$ は，一意に定まるため，$F$ 関数の差分確率は

$$DP(\Delta X \to \Delta Z) = DP(\Delta X \to \Delta Y)$$

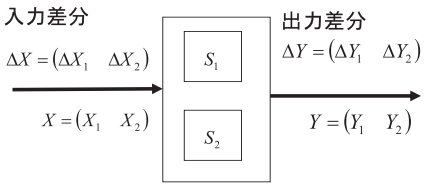



**図 4 並列 S-box**

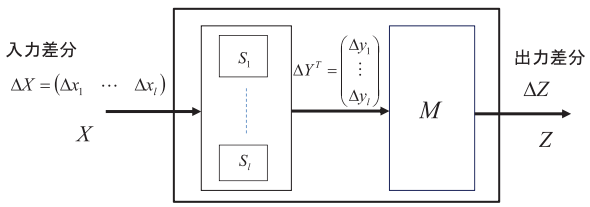



**図 5 $F$ 関数**

(注2)：$(\cdot)^T$ は，$(\cdot)$ の転置を表す．

$$= \prod_{i=1}^{l} DP(\Delta X_i \to \Delta Y_i) \quad (8)$$

で与えられる．

## 3.3 差分特性確率

図 6 のように，$F$ 関数が直列に接続された構造を考える．

入力差分 $\Delta X_0$ に対し，1 段目の出力差分 $\Delta X_1$ が確率 $DP\{\Delta X_0 \to \Delta X_1\}$ で期待できる．これが，2 段目入力差分である．2 段目 $F$ 関数入力 $X_1$ が一様分布ならば，出力差分 $\Delta X_2$ は，そのうちで，$DP(\Delta X_1 \to \Delta X_2)$ の割合で期待できる．差分が各段で，$\Delta X_0 \to \Delta X_1 \to \Delta X_2$ と伝わる確率を，各段の差分確率の積として見積もることができる．

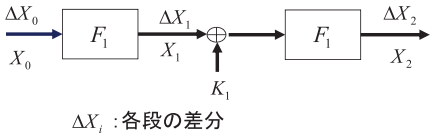
$$DCP(\Delta X_0 \to \Delta X_1 \to \Delta X_2) = DP(\Delta X_0 \to \Delta X_1) DP(X_1 \to \Delta X_2) \quad (9)$$

このように構成部品の差分確率の積として見積もられた確率を，差分パス $\Delta X_0 \to \Delta X_1 \to \Delta X_2$ の差分特性確率（Differential Characteristic Probability）と言い DCP と表す．差分特性確率 DCP の積も，式を展開すれば，差分確率 DP の積であり，これも差分特性確率である．しかしながら，差分特性確率は，入力差分 $\Delta X_0$ に対し，出力差分が $\Delta X_2$ となる差分確率を必ずしも表しているものではない．一つの理由は，1 段目出力差分が $\Delta X_1$ となるとき，2 段目 $F$ 関数入力 $X_1$ は，一様分布では無く，特定の値に偏っていることである．しかし鍵 $K_1$ が，一様分布で選ばれているならば，$X_1$ は一様分布であり，鍵平均の差分特性確率とみなすこともできる．二つ目の理由は，2 段目入力差分が，$\Delta X_1$ 以外でも，出力差分が $\Delta X_2$ となることがあり得ることである．これをマルチパスという．これら考慮すると，鍵が一様分布で選ばれているならば，(鍵平均) 差分確率は，

$$DP_{AVK}(\Delta X_0 \to \Delta X_2) = \sum_{\Delta X_1} DP(\Delta X_0 \to \Delta X_1) DP(X_1 \to \Delta X_2) \quad (10)$$

となる．鍵平均差分確率は，差分特性確率より小さくなることはない．

鍵平均差分確率を求めることは，一般には難しく，差分攻撃においては，差分特性確率を評価量とする．すなわち，差分パスが与えられれば，鍵平均の意味では，その差分特性確率以上の確率で，期待する出力差分が得られることを，攻撃の根拠とする．




$\Delta X_i$ : 各段の差分

**図 6 複数段 $F$ 関数**

### 3.4 差分攻撃

差分攻撃で使用する入力差分は $\Delta \neq 0$ の差分である．$\Delta P = 0$ の場合は，自明な差分と呼ばれ，攻撃に使用することはできない．攻撃方程式が，任意の鍵に対し成立し，鍵を特定することができないからである．攻撃に必要な選択平文差分組 $(P, P^* = P \oplus \Delta P)$ の数 $N_{\Delta P}$ は

$$N_{\Delta P} \propto DCP^{-1} \tag{11}$$

と，差分特性確率 $DCP$ の逆数に比例する．比例定数は，攻撃方程式の構造及びその解法に依存する．多くの場合，DCP の逆数の数倍あれば鍵の特定が可能となる．

図 2 のような繰返し型暗号に対する差分攻撃は，以下である．準備として，最大差分特性確率 $DCP_{Max}$（または十分大きな特性確率) を与える差分パスを探索する．

**準備 1**　段関数 $F$ の差分（特性）確率を求める

**準備 2**　$R$ 段の差分パス $\Delta P \rightarrow \Delta X_1 \rightarrow \cdots \Delta X_R$ で，差分特性確率を最大にするものを探す．

最大差分特性確率は，

$$DCP_{Max} \tag{12}$$
$$= \max_{\Delta P = \Delta X_0 \neq 0, \Delta X_1, \cdots, \Delta X_R} \prod_{i=0}^{R-1} DP(\Delta X_i \rightarrow \Delta X_{i+1})$$

となる．差分攻撃は，この最大差分特性確率を与える入力差分 $\Delta P$ に従い平文対を用意し下の手順で行う．

**攻撃 1**　平文 $P$ をランダムに選び，平文対 $(P, P^* = P \oplus \Delta P)$ を多数用意し，対応する暗号文対 $(C, C^*)$ を手に入れる．この平文対に対し $R$ 段目出力差分 $\mathcal{H}(X_R, X_R^*) = X_R \oplus X_R^* = \Delta X_R$ が，確率 $DCP_{Max}$ で期待される．

**攻撃 2**　その暗号分対を用いて，攻撃方程式において関係する段鍵 $K_{R+1}, \cdots, K_M$ を最ゆう推定する．

最ゆう推定の基本的な考え方は以下のとおりである．段鍵 $K_{R+1}, \cdots, K_M$ を仮定し，暗号文対 $(C, C^*)$ から $R$ 段目出力差分 $X_R \oplus X^*$ を逆算する．平文対に対し $R$ 段目出力差分が $\Delta X_R$ となっていて，仮定した段鍵が正しければ，逆算した $R$ 段目出力差分も，この $\Delta X_R$ に一致する．それ以外の場合，逆算した $X_R, X_R^*$ はランダムな値と考えられ，その差分が $\Delta X_R$ に一致する確率は，($|X_R| = N$ として)，$2^{-N}$ である．したがって，$DCP_{Max} > 2^{-N}$ であれば，$DCP^{-1}$ の数倍程度の選択平文組を使って，真の段鍵 $K_{R+1}, \cdots, K_M$ を見分けることが可能となり，この攻撃が成功する．

## 4. 線形攻撃

線形攻撃は，1993 年に松井により提案[4],[5]された手法であり，既知平文攻撃である．暗号器入出力の線形相関を攻撃に利用する．DES に対する攻撃実験を実際に行い全数探索法より少ない計算量で攻撃が可能であることを示した初めてのショートカット攻撃である．攻撃に必要な平文組数は，$2^{43}$ 組である．

### 4.1 線形確率

図 7 の $n$ bits 入力，$m$ bits 出力の S-box を考える．S-box 入力 $X = (x_1, \cdots, x_n)$，出力 $Y = (y_1, \cdots, y_m)$ に対し，線形近似式，例えば，

$$y_1 = x_1 \oplus x_2 \tag{13}$$

を考える．線形近似式は，その左辺及び右辺で選ぶ入出力 bit を指定すれば一意に定まる．この例では，入力 bit に対し $n$ 次元ベクトル $\Gamma_X = (1, 1, 0, \cdots, 0)$，出力 bit に対し $m$ 次元ベクトル $\Gamma_Y = (1, 0, \cdots, 0)$ と指定すればよい．この bit 指定ベクトルを使うと線形近似式は，ベクトルの内積 $(\cdot)$ を使い

$$\Gamma_Y \cdot Y = \Gamma_X \cdot X \tag{14}$$

と表現できる．線形近似式において，ビットを指定するベクトル $\Gamma_X, \Gamma_Y$ を線形マスク（またはマスク）という．線形攻撃においては，特徴量として $X$ の線形和 $H(X) = \Gamma_X \cdot X$ を使用する．線形近似式の成立確率は，入力 $X$ が一様分布であれば，

$$Prob(\Gamma_Y \cdot Y = \Gamma_X \cdot X) \tag{15}$$
$$= \frac{\#\{X | \Gamma_Y \cdot S(X) \oplus \Gamma_X \cdot X = 0\}}{2^n}$$

となる．この線形確率表を作成する計算量は，素朴に計算する場合，$X$,$\Gamma_X$,$\Gamma_Y$ を総当りして $2^{3n}$ となる．この計算は一次 RM 符号の復号問題であり，高速アダマール変換 (FHT)[19]を使用して $n2^{2n}$ の計算量で行える．$n$ が小さい場合，十分計算可能である．この式を，$X = P \oplus K$ を用いて書き換える．$P$ と $K$ で選択するビット $\Gamma_P$，$\Gamma_K$ が，同一 $(\Gamma_X = \Gamma_P = \Gamma_K)$ であるとして，次式となる．

$$\Gamma_Y \cdot Y = \Gamma_X \cdot (P \oplus K) \tag{16}$$

更に，未知の鍵 $K$ のみ左辺に残せば，この式は，鍵ビットの線形和を $P$，$Y$ の線形和で近似する式となる．

$$\Gamma_X \cdot K = \Gamma_Y \cdot Y \oplus \Gamma_X \cdot P \tag{17}$$

鍵の線形和の値は，0 or 1 の 2 通りであり，それは，線形近似式の“ 成立 ”or“ 不成立 ”に対応する．鍵を推定する能力を考えれば，線形近似式の性能は，成立確率が $\frac{1}{2}$ からいかに離れているか，すなわち $|\frac{1}{2} - Prob\{\Gamma_Y \cdot Y = \Gamma_X \cdot X\}|$ で評価される．これを線形近似式の偏差 (bias) と言う．偏差の最大値を 1 に正規化し，それを二乗したものを線形確率 $LP$ と定義する(注3)．式

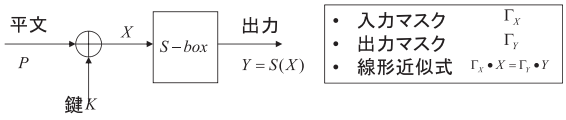



**図 7**　S-box と鍵加算 (線形近似)

(注3)：二乗するのは，差分攻撃との形式上の双対性を見やすくするためである．線形攻撃を取り扱う論文で，線形近似式のこの評価量の表現は偏差，2*偏差と変遷し，現在は線形確率の表現が主流である．

(17) の線形近似式は，$\Gamma_X$ と $\Gamma_Y$ で指定できる．線形近似式を明示し，$LP(\Gamma_X \to \Gamma_Y)$ と表記する．

$$LP(\Gamma_X \to \Gamma_Y) \tag{18}$$
$$= (2(\frac{1}{2} - Prob(\Gamma_Y \cdot Y = \Gamma_X \cdot X)))^2$$

図 4 と図 7 を比較するならば，注目する差分 $\Delta X$,$\Delta Y$ が，マスク $\Gamma_X, \Gamma_Y$ に置き換わっている．次節以降の説明において図を省略した場合，差分攻撃の説明図に於ける“ 差分 ”を“ マスク ”に置き換えて，理解して頂きたい．

### 4.2 並列 S-box と SP 型 $F$ 関数の線形確率

図 8 の並列 S-box の線形近似を考える．入力マスク $\Gamma_{\mathbf{X}} = (\Gamma_{X1}, \Gamma_{X2})$，出力マスク $\Gamma_{\mathbf{Y}} = (\Gamma_{Y1}, \Gamma_{Y2})$ であり，これらは，各 S-box $S_i$ の入出力 $X_i$,$Y_i$ に対するマスク $\Gamma_{Xi}$,$\Gamma_{Yi}$ を表す．それぞれの線形近似式は，

$$\Gamma_{X1} \cdot X_1 = \Gamma_{Y1} \cdot Y_1 \tag{19}$$
$$\Gamma_{X2} \cdot X_2 = \Gamma_{Y2} \cdot Y_2 \tag{20}$$

であり，この二つの式を辺々加算し，線形近似式

$$\Gamma_X \cdot X = \Gamma_Y \cdot Y \tag{21}$$

としたときの，線形確率は，

$$LP(\Gamma_X \to \Gamma_Y) \tag{22}$$
$$= LP(\Gamma_{X1} \to \Gamma_{Y1}) LP(\Gamma_{X2} \to \Gamma_{Y2})$$

となる．“ 式 (21) が成立するのは，式 (19)，(20) が両方とも成立するまたは両方とも不成立であるときである ”ことから線形近似式の成立確率を求め，それを線形確率に変換すれば，式 (22) は容易に確認できる(注4)

図 5 の SP 型 $F$ 関数の場合も同様である．各 S-box の線形確率の積として，$F$ 関数入力から，S 層出力までの線形確率が得られる．$F$ 関数出力 $Z$ までの線形近似式では，(線形和として選ぶ $Z$ のビットを線形マスク $\Gamma_Z$ が指定していることに注意すれば)

$$\Gamma_Z M = \Gamma_Y \tag{23}$$

を満たす $\Gamma_Z$ に対し，線形確率は

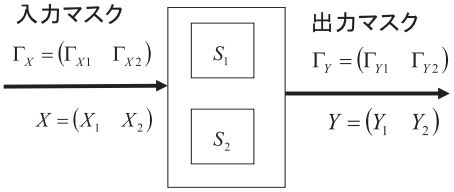



**図 8　並列 S-box(線形近似)**

$$LP(\Gamma_X \to \Gamma_Z) = LP(\Gamma_X \to \Gamma_Y) \tag{24}$$

で与えられる．

### 4.3 線形特性確率

図 6 の構造においても，差分特性確率と同様の議論を線形攻撃においても行うことができる．1 段目の入出力マスクが $(\Gamma_{X0}, \Gamma_{X1})$，2 段目の入出力マスクが $(\Gamma_{X1}, \Gamma_{X2})$ であるならば，それぞれの段の線形近似式

$$\Gamma_{X0} \cdot X_0 \oplus \Gamma_{X1} \cdot X_1 = \Gamma_{X0} \cdot K_1 \tag{25}$$
$$\Gamma_{X1} \cdot X_1 \oplus \Gamma_{X2} \cdot X_2 = \Gamma_{X1} \cdot K_2 \tag{26}$$

を加算すれば，

$$\Gamma_{X0} \cdot X_0 \oplus \Gamma_{X2} \cdot X_2 = \Gamma_{X0} \cdot K_1 \oplus \Gamma_{X1} \cdot K_2 \tag{27}$$

が得られ，入力 $X_0$ と，出力 $X_2$ の線形和で，鍵の線形和 $\Gamma_{X0} \cdot K_1 \oplus \Gamma_{X1} \cdot K_2$ を表す近似式となる．このように，中間段の変数を消去し，入出力の線形和とするには，1 段目の出力マスクと 2 段目の入力マスクが等しいことが必要である．得られた近似式の有効性は線形確率の積で見積もることができる．

$$LCP(\Gamma_{X0} \to \Gamma_{X2}) \tag{28}$$
$$= LP(\Gamma_{X0} \to \Gamma_{X1}) LP(\Gamma_{X1} \to \Gamma_{X2})$$

このように構成部品の線形確率の積として見積もられた確率を，線形パス $\Gamma_{X0} \to \Gamma_{X1} \to \Gamma_{X2}$ の線形特性確率（Linear Characteristic Probability）と言い LCP と表す．線形特性確率 LCP の積も，式を展開すれば，線形確率 LP の積であり，これも線形特性確率である．差分特性確率 DCP の議論と同じく，一様分布性とマルチパスの問題があり，LCP は，必ずしも線形近似式の有効性を表しているものではないが比較的に容易に求めることができるので，線形攻撃の際の評価量として用いられる．

### 4.4 線 形 攻 撃

線形攻撃も基本的には差分攻撃と同じである．準備として，段関数 $F$ の線形（特性）確率を求め，それをつないで，平文入力 $P = X_0 \oplus K_0$ から $R$ 段目出力 $X_R$ に至る線形パス $\{\Gamma_{X0} \to \Gamma_{X1} \cdots \Gamma_{XR} \neq 0\}$ の中で，最大線形特性確率 $LCP_{Max}$（または十分大きな特性確率) を与える線形パスを探索する．出力マスク $\Gamma_{XR} \neq 0$ の条件は，差分攻撃の入力差分 $\Delta X_0 \neq 0$ に対応するものであり，$\Gamma_{XR} = 0$ の線形パスは，自明で，攻撃に利用できないからである．最大線形特性確率は

$$LCP_{Max} \tag{29}$$
$$= \max_{\Gamma_{X0}, \Gamma_{X1}, \cdots, \Gamma_{XR} \neq 0} \prod_{i=0}^{R-1} LCP(\Gamma_{X_i} \to \Gamma_{X_{i+1}})$$

となる．線形攻撃において，必要な平文数 $N_{LC}$ は，

$$N_{LC} \propto LCP^{-1} \tag{30}$$

(注4)：二つの線形近似式を XOR 加算した線形近似式の偏差は，二つの式の偏差の積を 2 倍したものであることを松井は示し，それを Piling-up lemma と呼んだ．線形確率で Piling-up lemma を示せば式 (22) である．

**表 1　$GF(2^n)$ の写像**

| $S(X)$ | $DP_{Max}$ | $LP_{Max}$ | 次数 | 条件 |
|---|---|---|---|---|
| $X^{2^k+1}$ | $2^{s-n}$ | | 2 | $s = gcd(k, n)$ |
| $X^{2^k+1}$ | | $2^{s-n}$ | | $s = gcd(k, n)$, $\frac{n}{s}$ = 奇数 |
| $(X^{2^k+1})^{-1}$ | $2^{1-n}$ | $2^{1-n}$ | $(n+1)/2$ | $gcd(k, n) = 1$, $n$ = 奇数 |
| $X^{-1}$ | $2^{1-n}$ | $2^{2-n}$ | $n-1$ | $n$ = 奇数 |
| $X^{-1}$ | $2^{2-n}$ | $2^{2-n}$ | $n-1$ | $n$ = 偶数 |

となる．比例定数は，攻撃方程式の構造及びその解法に依存する．したがって $LCP^{-1}$ の数倍程度の既知平文とそれに対応する暗号文があれば，攻撃に成功すると考えてよい．

## 4.5　差分攻撃/線形攻撃に関わる研究の発展

差分攻撃と線形攻撃は，共通鍵暗号に対する汎用的な攻撃法であり，多数の暗号に対し適用されている．各種暗号の攻撃耐性について，興味のある方は，文献(20)，(21)等を参照されたい．以下，技術的側面に関し，その後の研究の進展を概観する．

### 4.5.1　最強の S-box

差分攻撃/線形攻撃の効率の指標は，最大差分確率 $DP_{Max}$/最大線形確率 $LP_{Max}$ である．この確率が小さいほど，差分攻撃/線形攻撃に対し強い．$n$ bits 入力の非線形関数においてこれらの最大確率の理論的最小値は，$D(L)P_{Max} \geqq 2^{1-n}$ である．拡大体 $GF(2^n)$ 上の単項式の 1 対 1 写像に関し，表 1 の結果が知られている[21]．入力ビットサイズ $n$ が奇数の場合は，この最少値を実現する写像がある．この写像は，差分攻撃/線形攻撃に対し最強な S-box を与える．$n$ = 偶数 の場合は，$2^{2-n}$ であり，しばらくの間，それが最強の S-box と信じられ，近年の暗号の多くは，AES を含め，$X^{-1}$ 関数をベースとした S-box を使用している．しかし，多項式写像まで考えれば，その限りではない．$GF(2^6)$ において，最大確率 $2^{-5}$ を与える写像が，最近，示されている[22]．

### 4.5.2　証明可能安全性

差分攻撃/線形攻撃に対し，最強な実用暗号の具体的構成法は，知られていない．Feistel 型暗号(注5)の場合，段関数の最大差分確率/最大線形確率が $p_{max}$ の場合，4 段以上であれば，その $DP_{Max}/LP_{Max}$ は，高々$2p_{max}^2$ であることが証明されている[23],[24]．この事実と，前述の最強の S-box を組み合わせ，提案者らは，“ 証明可能安全な暗号 (Provably Secure Cipher) ” と呼び，プロトタイプ暗号 $\mathcal{KN}$ が示されている[25]．しかし，この安全性は差分攻撃/線形攻撃に対して，主張しているのみであることに注意が必要である．この考えを使って，最初に提案された実用暗号が MISTY[26],[27]である．MISTY には，Feistel 構造の MISTY1 と，その変形構造の MISTY2 がある．

(注5)：DES 構造の暗号．DES は，IBM の研究者 Feistel の設計した暗号 Lucifer を基にして設計されている．その構造を，開発者にちなみ Feistel 構造という．

### 4.5.3　Truncate 差分/線形確率

データブロック長を $n$ bits として，そのうちの一部 $(n' < n)$ bit の差分のみに着目して，差分伝搬を考える攻撃を Truncate 差分 (切詰め差分) 攻撃という．当初は，攻撃法として提案[9]された．着目していない部分の差分は，何でもよく，その部分に関しては，差分が一様分布していると考え線形部においてもパスの接続性に確率を導入している．ここでは，複数種類の差分を同一視しており一部マルチパス的な評価も意図している．

### 4.5.4　活性 S-box 数

複数種類の差分/線形マスクを同一視する思想は，暗号の差分/線形攻撃耐性評価技術として使用することができる．暗号の非線形要素が $n$ bits 入出力の S-box の場合，$n$ bits を 1 Byte と考え，差分/線形マスクをバイト単位に，零であるか非零であるかの 2 種類に分類する．これも Truncate 差分/線形マスク (丸め差分/マスク) という入力差分/出力マスクが非零である場合，その S-box を活性 S-box という．暗号全体に接続可能な Truncate 差分/線形パスを探索し，そのようなパスにおいて，活性 S-box の数の最小値を $ASD_{min}(ASL_{min})$ としよう．S-box の最大差分 (線形) 確率を $DP_S/LP_S$ とするならば，その暗号の最大差分/線形特性確率 $DCP_{Max}/DLP_{Max}$ の上界は，

$$DCP_{Max} \leqq DP_S^{ASD_{min}} \tag{31}$$

$$LCP_{Max} \leqq LP_S^{ASL_{min}} \tag{32}$$

で与えられる．

### 4.5.5　実用的安全な暗号

暗号のブロック長を $N$ bits として，最大差分/線形特性確率が $DCP_{Max} < 2^{-N}/DCP_{Max} < 2^{-N}$ であるならば，全ての平文を用いても，攻撃に必要な平文・暗号文組数に達しない．この条件をに対する安全性条件と考えることもできる．この安全性判断を“ 実用的安全な暗号 (Practically Secure Cipher)” という[28]．Truncate 差分/線形パス探索により，その最大確率の上界が $DP_S^{ASD_{min}} < 2^{-N}/LP_S^{ASL_{min}} < 2^{-N}$ となれば，差分攻撃/線形攻撃に対し実用的に安全である．鍵ビット長 $|K|$ がブロック長 $N$ より大きい場合は，安全側に倒し，攻撃計算量が鍵の総当りよりも大きくなるという条件にし，最大確率の判断基準を $2^{-|K|}$ との比較で行うことが多い．

### 4.5.6　差分/線形攻撃の変形

差分攻撃，線形攻撃から派生した様々な攻撃がある．差分攻撃と線形攻撃を組み合わせた攻撃が，DES に対し[29]，また，FEAL に対し[30]行われており，限定的ではあるが効果を上げている．これらは，差分線形攻撃と呼ばれる．差分の概念は，XOR 演算に限定されず，一般化できる．算術差分を用いた手法が IDEA(International Data Encryption Algorithm) に対し適用されている[31]．IDEA は，Lai らが提案した暗号 PES[31]を基に作られた暗号であり，当時輸出規制が掛かっていた DES

の代替を意識したものである．IDEA のように，解析の困難さを意図し，複数の代数系の演算を用いて構成される暗号においては，適切な差分演算を選ぶことが必要である．線形攻撃において，複数の線形近似式を用いたり[32],[33]，一部に二次関係式を用いたり[34]して，効率を上げる試みも行われている．差分攻撃では，$2^{-N}$ より大きな差分確率を攻撃に使う．逆に，発生しない出力差分 $DP(\Delta P \to \Delta X_R) = 0$ を使う攻撃が，不能差分攻撃である[35]．式 (1) において，暗号文から逆算したとき $\Delta X_R$ を与えるような鍵 $K_{R+1}, \ldots, K_M$ は，偽として排除し，真の鍵を浮かび上がらせる攻撃である．その原理から，少ない平文・暗号文組数では，攻撃が成立しないが，攻撃に必要な平文数が多い場合，成果を上げている[20]．

## 5. 高階差分攻撃

### 5.1 高階差分

高階差分は，差分概念の拡張として，Lai が提案したものである[10]．$n$ bits 入力，$m$ bits 出力の関数

$$Y = F(X) : GF(2)^n \to GF(2)^m \tag{33}$$

を考える．差分 $a$ を，入力 $x$ に与えたときの出力の差分を，差分 $a$ に対する $F(X)$ の 1 階差分と呼び $\Delta^{(1)}_{(a)}Y$ と書く．

$$\Delta^{(1)}_{(a)}Y = F(X) \oplus F(X \oplus a) \tag{34}$$

この 1 階差分 $\Delta^{(1)}_{(a)}Y$ も，一般には $X$ の関数である．これに対し，別の差分 $b$ を使い，差分を考えたものを，差分 $a, b$ に対する 2 階差分と呼び，$\Delta^{(2)}_{(a,b)}Y$ と書く．

$$\Delta^{(2)}_{(a,b)}Y = \Delta^{(1)}_{(b)}(\Delta^{(1)}_{(a)}Y) \tag{35}$$

この繰返しで，$i = 1, 2, \cdots$ 階差分が定義できる．差分 $a$ に対する $\mathbf{Y}$ の 1 階差分を $\Delta^{(1)}_{(a)}Y = F^{(1)}$ と表記して，上式は次のように変形できる．

$$\begin{aligned}
&\Delta^{(2)}_{(a,b)}Y \\
&= F^{(1)}(X) \oplus F^{(1)}(X \oplus b) \\
&= F(X) \oplus F(X \oplus a) \oplus F(X \oplus b) \oplus F(X \oplus a \oplus b) \\
&= \sum_{\alpha \in V^{[2]}(a,b)}^{\oplus} F(X \oplus \alpha)
\end{aligned} \tag{36}$$

ここで，$V^{[2]}(a,b)$ は，独立な二つのベクトル $a, b$ で張られる二次元ベクトル空間を表す．また，$\sum^{\oplus} F(X \oplus \alpha)$ は，$F(X \oplus \alpha)$ の総 XOR 和を表す．$i$ 階差分も同様であり，独立な $i$ 個のベクトル $a_1, a_2, \cdots a_i$ に対する $Y = F(X)$ の $i$ 階差分は，

$$\Delta^{(i)}_{(a_1,a_2,\cdots,a_i)}Y = \sum_{\alpha \in V^{[i]}(a_1,a_2,\cdots,a_i)}^{\oplus} F(X \oplus \alpha) \tag{37}$$

である(注6)

(注6)：この右辺において，$\sum^{\oplus}$ を和と考えるならば，$F(X)$ の総和 (Integral) と見ることができる．$F(X)$ の総和の性質を使って攻撃する手法を Integral 攻撃[36]という．

### 5.2 SQUARE 攻撃

図 3 の S-box が $n$ bits 入出力で，1 対 1 写像であるとする．平文 $P$ として，全種類の値 $2^n$ 通りを 1 回づつ入力したとする．このようなデータ集合の性質を **All**(以下性質 **A**) と表現する．このとき，S-box 入力 $X$ の集合も性質 **A** を持つ．S-box が 1 対 1 写像であるので，その出力 $Y$ の集合も性質 **A** を持つ．

この $2^n$ 通りの入力 $\{X(i)\}$ に対し出力 $Y(i)$ の総和を求めれば

$$\mathcal{H} = \sum^{\oplus} Y(i) = 0 \tag{38}$$

である．これは，図 3 の鍵 $K$ には依存しない．式 (37) と比較するならば，上式は，この S-box 入力の $n$ 次元空間を張る $n$ 個の基底ベクトルを用いた $n$ 階差分である．このように，S-box の入力ビットサイズの全データを入力し，暗号系の途中段 (R 段目) の S-box 出力が全通り（またはその線形和）であるならば，その総和を特徴量 $\mathcal{H}$ として利用した攻撃が可能である．この攻撃法を SQUARE 攻撃[37]という．これは高階差分攻撃の一種であるが，入力データの集合としての性質に着目することにより，ある種の高階差分の振舞いを直観的に解析することができる手法である．

### 5.3 ブール代数次数と高階差分

関数を $GF(2)$ 上の代数式（ブール代数式）で表したときの最高次数を（ブール代数）次数という．例えば，

$$y = x_1x_2 + x_3 \quad x_i \in GF(2) \tag{39}$$

ならば，$y$ の次数は二次であるという．$n$ bits 入力，$m$ bits 出力の関数 $Y = F(X)$，$Y \in GF(2)^m, X \in GF(2)^n$ であれば，出力ベクトル $Y = (y_1, \cdots, y_m)$ の要素 $y_i = f_i(X)$ の次数を考え，その最大値を $Y$ の次数という．

高階差分に関し，よく使われる性質について以下で述べる．

#### 5.3.1 次数と高階差分

暗号関数 $Y = F(X)$ の次数が $d$ ならば，$d+1$ 階差分は 0，$d$ 階差分は定数となる．

$$\Delta^{(d+1)}Y = 0 \tag{40}$$

$$\Delta^{(d)}Y = const \tag{41}$$

これは，入力差分 $V^d(a_1, a_2, \cdots a_d)$ の取り方には依存しない．この性質は，式 (39) を例に，2 階，3 階差分を計算すれば，容易に確認できるであろう．

#### 5.3.2 1 対 1 関数の高階差分

$n$ bits 入出力の 1 対 1 関数 $Y = F(X)$ の $n$ 階差分は 0 である．

$$\Delta^{(n)}Y = 0 \tag{42}$$

この性質は，式 (38) の説明を参照．

### 5.3.3 高階差分の線形性

関数の和の高階差分は，高階差分の和である．$Y = F_1(X) \oplus F_2(X)$ に対し，次式が成り立つ．

$$\Delta^{(d)} Y = \Delta^{(d)} F_1(X) \oplus \Delta^{(d)} F_2(X) \qquad (43)$$

この性質は，高階差分の XOR 総和表現式 (37) から自明である．

## 5.4 高階差分攻撃の原理

Jakobsen と Knudsen は，文献(25)で高階差分攻撃を定式化している．そこで示されている暗号 $\mathcal{KN}$ は，64 bit ブロックの Feistel 型暗号であり，3 段で差分攻撃/線形攻撃に対し証明可能安全性を持つ．プロトタイプ暗号であり，ラウンド数の指定はないが，ここでは説明のため 7 段暗号として，そのデータランダム化部を図 9 に示す．高階差分攻撃の原理を，$\mathcal{KN}$ 暗号を用いて，説明する．ラウンド関数 $F$ は，$GF(2^{33})$ 上の $X^3$ 関数の前後に，拡大アフィン変換及び 1 bit 放棄の縮小転置を施した 32 bit 入出力関数であり，ラウンド鍵 $K_i$ は 33 bit である．標数 2 の拡大体 $GF(2^{33})$(注7)のべき乗関数を $GF(2)$ 上の式で表したときの次数（ブール代数次数) は，べき指数の 2 進表現のハミング重みで与えられる．このラウンド関数 $F$ のブール代数次数は，二次である．

図には，64 bit 入力 $(P_L, P_R)$ の左半分 $P_L$ に差分を入力し，右半分 $P_R$ は，固定値としたときの各部の次数の見積もりを記入してある．変数は，$P_L$ の各ビットである．$F$ 関数の次数は二次であり，各部の次数の上限は，$F$ 関数を通過するごとに 2 倍になると推定される．6 段目右半分 $H$ の次数は 16 次であり，式 (40) から，17 階の高階差分入力を左半分平文 $P_L$ に入れれば，$H$ の 17 階差分は 0 であることが保障される．7 段目の鍵 $K_7$ を仮定すれは，暗号文 $C = (C_L, C_R)$ から $H$ は，復号計算することができる．高階差分は，式 (37) のように総 XOR 和で表現でき，17 階差分入力となる平文 $P$ に対応する暗号文 $C$ の集合を $\mathcal{C}$ とすれば，鍵 $K_7$ が満たすべき方程式 (攻撃方程式) は，次式となる．

$$\Delta^{(17)} H = \sum_{C \in \mathcal{C}}^{\oplus} C_L \oplus F(C_R \oplus K_6) \qquad (44)$$

この式を，33 bit 鍵 $K_7$ の総当たり計算で解くならば，攻撃計算量は，$2^{17} * 2^{33} = 2^{50}$ の $F$ 関数計算量である．真の鍵は常に式を満たすが，この攻撃方程式は，32 bit 幅の式であり，偽鍵がこの式を満たす確率は $2^{-32}$ である．したがって，一組の 17 階差分でこの攻撃方程式を確認すると偽鍵が 2 組程度と真鍵の合計 3 組の鍵候補が生き残る．もう一組の 17 階差分を用意して，生き残り鍵を攻撃方程式で確認すれば，真の鍵が高い確率で確定できる．攻撃計算量は，$2^{50} + 2^{17} * 3 \approx 2^{50}$ の $F$ 関数計算である．7 段 $\mathcal{KN}$ 暗号の暗号化処理には，$F$ 関数 7 回の処理が必要である．攻撃計算量を暗号化処理を単位に表せば，$2^{50}/7 \approx 2^{47.2}$ 暗号化計算となる．

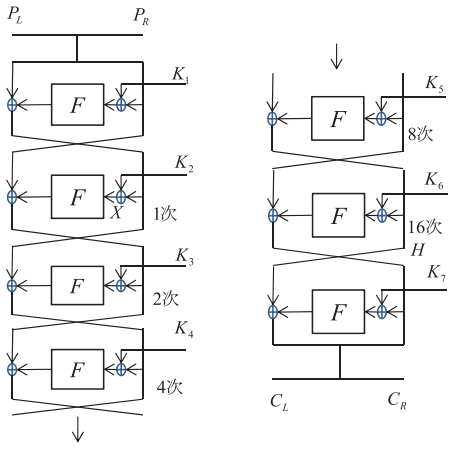



**図 9** $\mathcal{KN}$

(注7)：$GF(2^n)$ は，基礎体 $GF(2)$ を $n$ 次拡大したものであり，基礎体の位数を標数という．

## 5.5 高階差分攻撃研究の発展

効果的な高階差分攻撃は，平文入力としての高階差分入力の選択と攻撃方程式の効率的な解法により，得ることができる．ここでは，高階差分攻撃のように，暗号の代数的構造に着目する研究を概観する．

### 5.5.1 攻撃方程式の高速解法

前節の高階差分攻撃では，攻撃方程式を関係する鍵の全数探索で解いている．一般に攻撃方程式は，関係する段鍵 $K_{R+1}, \cdots, K_N$ の各ビットに関し高次のブール代数式となるが，高次項も独立な未知数と考えれば，線形方程式として取り扱うことができ解法の高速化を図ることができる．この手法を線形化法という[38],[39]．論文(38)では，式 (41) を使い，差分階数を下げて必要平文数を半減し，攻撃方程式を線形化手法で解くことにより，前節の手法に比べ $2^{27}$〜$2^{52}$ の高速化を計り，$\mathcal{KN}$ 暗号 9 段まで攻撃可能としている．

線形化法における未知数の係数は暗号文の関数となるが，その線形独立性を調べ線形従属なものについて，未知数の和を新たな未知数に置き換え，解くべき未知数の数を減らし攻撃を効率化できる．この手法を線形和法といい[40]，MISTY1 の高階差分攻撃において，線形和法で計算量を削減した報告がなされている[41]．この解法と 46 階差分特性を組み合わせ，7 段 MISTY1 が鍵の総当りより少ない計算量で攻撃可能であることが示されている[42]．

### 5.5.2 mod 2 頻度分布法

$n$ 階の高階差分は，$2^n$ 個の総 XOR 和であり，攻撃方程式では，非線形関数出力 $2^n$ 個の総 XOR 和が行われる．同一値の XOR 和は 0 であることを使用して，解法の高速化を図ることができる．図 10 の簡易モデルで説明する．図には，暗号文（の一部バイト）$C_1, C_2$ から $H$ までの復号経路が示してある．復号関数 $F^{-1}$ 内の $S_1, S_2, S_3$ は，$m$ bits 入出力の S-box,

$K_1, K_2, K_3$ は段鍵とする．ここで，$n$ 階差分攻撃を考え，図の $H$ の高階差分が 0 であるとする．攻撃方程式では，$2^n$ 組の暗号文 $(C_1, C_2) \in \mathcal{C}$ に対し，$H$ を計算し，総 XOR 和が 0 であるか否かを調べることになる．

$$\Delta^{(n)} H = \sum_{C \in \mathcal{C}}^{\oplus} F^{-1}(C_1, C_2; K_1, K_2, K_3) \qquad (45)$$

$2m$ bit の暗号文 $(C_1, C_2)$ が $2^n$ 組あり，それを値で分類する．値は $2^{2m}$ 種類しかなく，$2m < n$ の場合，同一の暗号文が複数回発生することになる．偶数回発生した暗号文は，同一の $H$ を与えるので，その XOR 和は 0 である．したがって，頻度分布表 $P(x, y) = \#\{(C_1, C_2) | C_1 = x, C_2 = y, (C_1, C_2) \in \mathcal{C}\}$ を作成し，その頻度が奇数，すなわち mod 2 頻度分布

$$P_2(x, y) = \#\{(C_1, C_2) | C_1 = x, C_2 = y, (C_1, C_2) \in \mathcal{C}\} mod\, 2 \qquad (46)$$

が 1 の値 $(x, y)$ に対し，$F^{-1}$ を計算すればよい．$P_2(x, y) = 1$ となる $(x, y)$ 組の数は，高々$2^{2m}$ 組，期待値として $2^{2m-1}$ である．式 (45) を，そのまま計算するのに比べ $F^{-1}$ 関数の計算回数が，$2^n$ から $2^{2m}$ 以下に減少する．

$F^{-1}$ の内部構造が図のように，より小さな非線形関数（ここでは，S-box) で構成されているならば，この mod 2 頻度分布法は繰り返し適用が可能である．mod 2 頻度分布 $P_2(x, y) = 1$ の $(x, y)$ 組に対し，$K_1, K_2$ を仮定して，変数 $u = S_1(x \oplus K_1) \oplus S_2(y \oplus K_2)$ の mod 2 頻度分布 $P_2(u)$ が得られる．$P_2(u) = 1$ の $u$ の値について，$H = S_3(u \oplus K_3)$ の総 XOR 和を計算すればよい．図の例であれば，mod 2 頻度分布 $P_2(u)$ を求める計算量は，仮定する鍵 $(K_1, K_2)$ 当り高々 $2 * 2^{2m}$ 回の S-box 計算である．mod 2 頻度分布 $P_2(u)$ に対し，仮定する鍵 $K_3$ の $2^m$ 種類に対し，各々$S_3$-box を高々$2^m$ 回呼び出し，$H$ の総 XOR 和を計算する．

計算量は，分布表 $P_2(u)$ 1 枚当り高々$2^m * 2^m$ の S-box 計算である．これを $K_1, K_2$ の種類数 $2^{2m}$ 回繰り返すので，全体で $2^{2m}(2 * 2^{2m} + 2^m * 2^m) = 3 * 2^{4m}$ の S-box 計算である．$F^{-1}$ 関数を $n$ 階差分のデータ $2^n$ に対し，$3m$ bit の拡大鍵に対し，総当りするならば，$3 * 2^{n+3m}$ の S-box 計算であり，$F^{-1}$ 関数が 2 個以上の並列 S-box 構造の場合 $(2m \leqq n)$ の場合，mod 2 頻度分布法の方が，明らかに計算量は少ない．

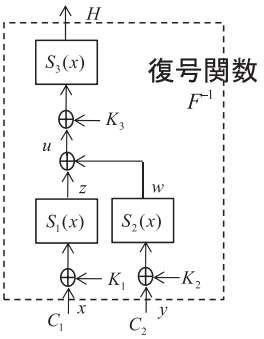



**図 10　攻撃方程式簡易モデル**

### 5.5.3 部 分 和 法

図 11 に AES に対し 4 段の 32 階差分特性を使い，6 段攻撃をする攻撃部分を示す．線は，8 bit データを表し，暗号文（一部)$(C_1, C_2, C_3, C_4)$ から変数 $H$ への復号過程を表す．6 段目 S-box の $S_1, S_2, S_3, S_4$ は，AES の InvSubByte と InvMixColumns の合成関数であり，5 段目の $S_5$ は，InvSubByte を表す．$K_1, \cdots, K_5$ は，段鍵である．攻撃方程式では，$2^{32}$ 組の暗号文に対し，$H$ を計算し，総 XOR 和が 0 であるか否かを調べることになる．この図のように 3 個以上の S-box の出力の和が，次段の入力となる場合，直接に次段入力の mod 2 頻度分布表を作成するのではなく，頻度分布表を順次縮小して作成すると効果的である．すなわち，$2^{32}$ 組の暗号文に対し，鍵 $K_1, K_2$ を仮定し，$(z, C_3, C_4)$ について 24 bit の mod 2 頻度分布表 $P_2(z, C_3, C_4)$ を作成する．それを使い，$K_3$ を仮定し $(w, C_4)$ について 16 bit の mod 2 頻度分布表 $P_2(w, C_4)$ を作成する．それを使い，$K_4$ を仮定し mod 2 頻度分布表 $P_2(u)$ を作成し，$K_5$ を仮定して，$H$ の総 XOR 和を計算する．S-box 出力の和を順次求めていくので Ferguson は部分和法[13]と呼んでいる．彼らは，この手法で 6 段 AES の攻撃において解法を従来比 $2^{28}$ 倍，高速化している．

この手順において，mod 2 頻度分布表を使い段鍵を仮定し，S-box を引いて，次の mod 2 頻度分布表を作る作業が繰り返される．S-box を引かずして，直接に mod 2 頻度分布表を操作して，次の mod 2 頻度分布表に変換した方が，攻撃計算は，高速化する．mod 2 頻度分布表の 1 エントリは，1 bit である．鍵を仮定し，S-box を引く場合，1 回の S-box 参照当り，1 エントリしか処理できない．近年の CPU は 64 bit CPU である．mod 2 頻度分布表のデータ並びを適切に配置することにより，64 エントリを一括に処理でき，CPU のビットサイズ倍の高速化を図ることができる[43](注8)

### 5.5.4 XSL 攻 撃

Courtois らは，暗号系全体を $GF(2)$ 上の多変数高次連立方

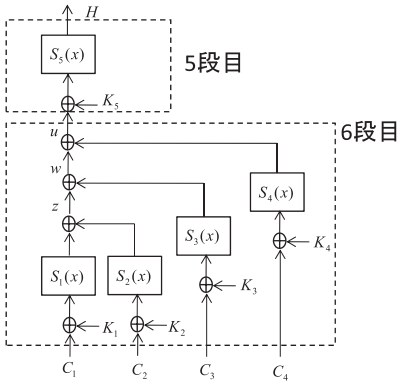



**図 11　6 段 AES の攻撃方程式**

(注8)：CPU ビットサイズが十分であれば，8 bit S-box の暗号のときは，256 倍まで．

程式で表現し，解読する手法として XSL 攻撃を提案した[44]．当初の，彼らの予想では AES を全数探索より少ない計算量で解読可能とのことであり，議論を引き起こした．結果として，XSL 法は，AES の場合，鍵の総当りより多い計算量になり有効でないことが分かっている[45]．

未知数の個数に比べ方程式の組数が多い連立方程式を overdefind な連立方程式という．AES の S-box において，入力 $X = (x_1, \cdots, x_8)$，出力 $Y = (y_1, \cdots, y_8)(x_i, y_j \in GF(2))$ とする．入出力に関し，$GF(2)$ 上で，陰関数 $g(X, Y) = 0$ 型の連立方程式を作るならば，S-box が，$GF(2^8)$ 上の逆数関数とアフィン変換の縦続接続であることを使い，23 本の二次方程式が得られる．ここで，未知数をまとめて $\mathbf{X} = (X, Y) = (x_1, \cdots, x_{16})$ と表せば，未知数 16 個の連立二次方程式 $\{g_i(\mathbf{X}) = 0 | i = 1, \cdots 23\}$ であり，未知数の数に比べ，方程式の数が多い overdefined な連立方程式である．任意の多項式 $h(\mathbf{X})$ に対し，この方程式の解は，$h(\mathbf{X})g_i(\mathbf{X}) = 0$ も満足するはずである．このように，方程式の数を増やし，式の中の単項の種類数より多くできれば，単項を独立未知数と考えた線形連立方程式として（線形化法で）解くことができる．Courtois らは，$GF(2)$ に置いて $x^2 = x$ であること及び，連立方程式 $\{g_i(\mathbf{X}) = 0\}$ を処理して得られる一部の式に，適切な単項式 $x_i$ を乗算することにより，新たな独立未知数の発生を抑制しつつ，方程式の数を増やす方法として XSL 法を提案している．しかしながら，その後の検討で，この手法は AES に対し，有効でないことが分かっている．

上述の考え方は，ストリーム暗号に対して，効果を上げており，algebraic atack と呼ばれ，LFSR と非線形フィルタで構成される filter generator 型擬似乱数生成器に対して適用されている．filter genarator において時刻 $t = 0$ の擬似乱数出力 $r_0$ は，LFSR の内部状態 $K_0$ をフィルタ関数 $f$ に通したもの

$$r_0 = f(K_0) \tag{47}$$

である．次の時刻では，内部状態は，LFSR の再帰関係式に従い更新され，$K_1 = L(K_0)$ となる．時刻 $t = 1$ の擬似乱数出力 $r_1$ は，

$$r_1 = f(L(K_0)) \tag{48}$$

となる．ここで，$L$ は，線形式であることに注意すると，これらの式の右辺の次数は，上昇しない．乱数を観測して得られる方程式を連立方程式として解いて，(等価) 鍵 $K_0$ を求めればよい．観測する時刻数を増やせば，任意の本数の overdefined な連立方程式を手にいれることができる．この連立方程式に適切な，多項式 $h(K_0)$ を乗算し，新たな方程式を導き，線形化法で解けばよい．filter generator に対するこの攻撃法や，それに対するフィルタ関数の強度指標と有限体上の DFT との関係は，論文(46)，(47) に詳しい．

## 6. AES に対する関連鍵攻撃

2009 年に Biryukov らは，AES の安全性に関し，鍵長が 192 及び 256 bit のもの（以下 AES-192 及び AES-256) に関し，関連鍵攻撃で full round 攻撃可能であるとの発表[14]をした．そこでは，選択平文攻撃に加え，攻撃者の指定した関数で，秘密鍵 $K$ を変換したものを $K^*$ として，これを使い平文を暗号化した平文・暗号文組を攻撃に利用することができるという攻撃条件（関連鍵攻撃）を仮定している(注9)．彼らが述べているように，この関連鍵攻撃は，理論的な興味の対象であり，現実世界のセキュリティ製品に対し，脅威となるものではない．しかしながら，AES を理想暗号と期待し，結果としてこのような関連鍵攻撃条件を成立させる使い方は避けるべきである．

この攻撃では，選択平文によるデータかくはん部の差分パスと，関連鍵条件による拡大鍵生成部における差分パスを巧妙に組み合わせるとともに，2 種類の差分パスを組み合わせて攻撃効率を上げるブーメラン攻撃の考え方を使用している．以下に概要を説明する．

### 6.1 AES の構造

#### 6.1.1 データランダム化部と差分攻撃

AES のデータランダム化部を図 12 に示す．基本構成要素は，拡大鍵の XOR 加算，S 層，そして Shift Row 及び Mix Column から成る線形変換 (P 層) を 1 段とする SPN(Substitution Permutation Network) 構造である．この段関数が，128 bit 鍵の場合は 10 段，192 bit 鍵では 12 段，256 bit 鍵では 14 段繰り返される．なお，最終段の P 層は省かれ，拡大鍵の XOR 加算が挿入される．入力された 128 bit = 16 Byte の平文は，図の左側に模式的に示したように，$4 \times 4$ の行列状に配置され，拡大鍵加算，16 個の 8 bit S-box による変換 (非線形変換)，Shift Row によるバイト単位の行シフト，Mix Column による 4 Byte 列の線形変換を，順次所定の段数回受け，暗号文となる．

差分攻撃では，$\Delta P = P \oplus P^* \neq 0$ を持つ選択平文対 $(P, P^*)$ をデータランダム化部に入力し，対応する暗号文対 $(C, C^*)$ における，暗号文差分 $\Delta C = C \oplus C^*$ の分布の偏りを利用する．攻撃者は，式 (12) の最大差分特性確率 $DCP_{Max}$ を与える差分パスを探して，攻撃を行う．AES の S-box の最大差分確率は，$2^{-6}$ であり，これは，知られている 8 bit 入出力の非線形関数の中で最も小さな値である．P 層の Mix Column 層は，分岐数 5 の MDS 行列であり，4 Byte の入力に入る差分を最も効果的に拡散する能力を持つ．図 12 の左側には，平文の 1 Byte に差分を与えた時 (図の青色部分)，1 段通過後 4 Byte に差分が発生し (赤色部分)，2 段通過後，全部の 16 Byte(黄色部分) に差分が拡散する様子が模式的に示してある．このような，段関数を持つ AES では，4 段で，最大差分特性確率が $2^{-150}$ を超えないことが示され，差分攻撃に対する AES の安全性の根拠となっている．

#### 6.1.2 鍵スケジュール部

データランダム化部で使用する拡大鍵を，ユーザの秘密鍵から生成する関数が鍵スケジュール部である．AES-256 の鍵スケ

(注9)：自明な攻撃を除外するため，関連鍵攻撃として，鍵 $K$ を変換する関数には，1 対 1 写像の条件を課している．

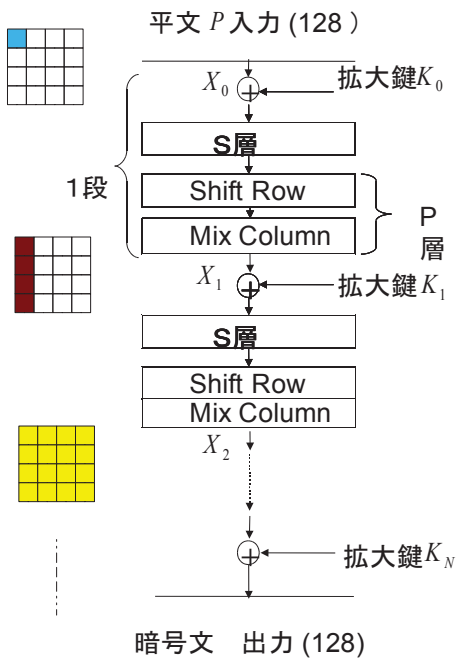



**図 12　AES　データランダム化部**

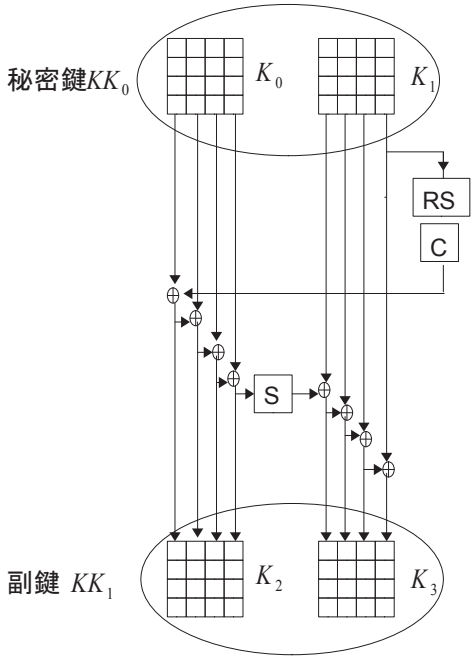



**図 13　AES-256 鍵スケジュール部**

ジュール部を，図 13 に示す．256 bit = 32 Byte の秘密鍵 $KK_0$ は，$4 \times 8$ の行列状に配置される．その左半分の $4 \times 4$ 部分が，データランダム化部 1 段目の拡大鍵 $K_0$ となり，右半分の $4 \times 4$ 部分が，2 段目の拡大鍵 $K_1$ となる．その後，$KK_0$ は，図に示す処理を受け，$4 \times 8 = 32$ Byte の副鍵 $KK_1$ となる．図の中で，S 及び RS と表された部分が，非線形関数であり，S では，データランダム化部と同じ S-box が，4 並列で並び，RS では，バイト巡回シフトの後，S と同じ処理が行われる．C では，段固有の定数を XOR 加算する．図中の $\oplus$ は，4 バイトデータの XOR 加算である．

副鍵 $KK_1$ の左半分及び右半分は，拡大鍵 $K_2$，$K_3$ として，データランダム化部で使用される．この図のように，$KK_0$ から $KK_1$ を作成する関数が，鍵スケジュール部の 1 段分であり，副鍵 $KK_1$ から，副鍵 $KK_2$ を作成するときも，$KK_1$ を図の $KK_0$ と考え，同じ関数で $KK_2$ が作られる．AES-256 は，データランダム化部が 14 段であり，必要な拡大鍵は，$K_0$ から，$K_{14}$ なので，この鍵スケジュールの 7 段分の処理が必要となる．

鍵スケジュールでは，256 bit の鍵データを，8 個の S-box で処理している．データランダム化部で，128 bit のデータを 16 個の S-box で処理しているのに比べ少ない S-box である．S-box の関与が少ないので，関連鍵攻撃の攻撃条件では，攻撃者の意図するような鍵差分を拡大鍵に与えることが比較的容易であり，論文(14) の攻撃が full round AES に対して成立する要因となっている．

## 6.2　ブーメラン攻撃

ブーメラン攻撃の概念図を，図 14 に示す．そこでは，暗号変換 $C = E(P)$ を，中間段で分けて，二つの変換 $E_0$，$E_1$ と考える．すなわち，$E(P) = E_1(E_0(P))$ である．中間段の変数を $X$ として，

$$X = E_0(P) \tag{49}$$

$$C = E_1(X) \tag{50}$$

である．平文入力差分 $\alpha$ に対し，中間変数差分 $\beta$ が，差分（特性）確率 $p$ で期待できるとする．同じく，暗号文差分 $\delta$ に対し，中間変数差分 $\gamma$ が，差分 (特性) 確率 $q$ で期待できるとする．このとき，次の手順を考察する．

（1） 差分 $\alpha$ を持つ平文組 $(P_1, P_2)$ を暗号化する．$P_1 \oplus P_2 = \alpha$ である．

（2） 中間変数組 $(X_1, X_2)$ の差分は，確率 $p$ で，$X_1 \oplus X_2 = \beta$ となる．

（3） 平文 $P_1$，$P_2$ に対応する暗号文を $C_1$，$C_2$ とする．それぞれに対し，差分 $\delta$ を持つ暗号文 $C_3 = C_1 \oplus \delta$，$C_4 = C_2 \oplus \delta$ を計算し，それを復号する．

（4） 中間変数組 $(X_1, X_3)$，$(X_2, X_4)$ の差分が両方とも $\gamma$ となる確率は，$q^2$ である．このとき $X_3 \oplus X_4 = \gamma \oplus \beta \oplus \gamma = \beta$ となっている．

（5） $X_3$，$X_4$ に対応する平文 $P_3$，$P_4$ の差分は，確率 $p$ で，$P_3 \oplus P_4 = \alpha$ となることが期待される．

上記の手順で得られる四つの平文組 $(P_1, P_2, P_3, P_4)$ を，四つ組（quartet）という(注10)．四つ組の中で，$P_3 \oplus P_4 = \alpha$ となっているものを，正しい四つ組 (right quartet) という．差分（特性）確率で解析すると，正しい四つ組が発生する確率は，$p^2q^2$ である．一方，理想的な暗号であれば，その確率は，$2^{-n}$ である．したがって，$(pq)^2 > 2^{-n}$ であれば，正しい四つ組を発見

(注10)：四つの暗号文組 $(C_1, C_2, C_3, C_4)$ も四つ組と言う．

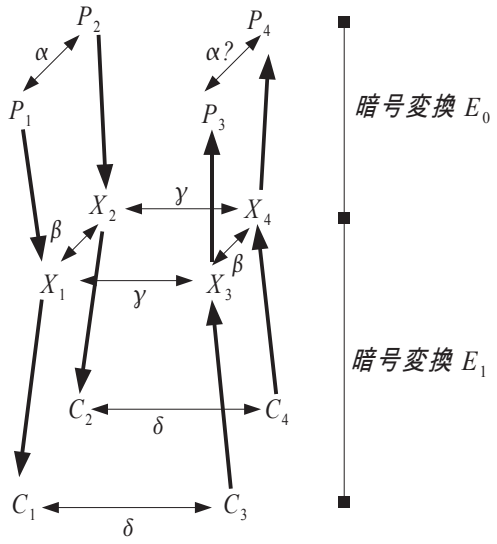



**図 14　ブーメラン攻撃**

することにより，理想暗号と区別することができる．

暗号が，$N$ 段の繰返し暗号であれば，平文側，または暗号文側の 1 段（状況によっては，2 段以上）を取り除いた，$N-1$ 段暗号化変換に対し，四つ組の考えを適用し，1 段目の拡大鍵を仮定して，正しい四つ組が，(理想暗号に比べて) 偏って出てくる鍵を，正しい鍵と判断することにより，鍵を復元することができる．

## 6.3　関連鍵ブーメラン攻撃

AES の場合，6.1.1 節で述べたように，平文に与えた差分は，段を経るごとに急速に拡散し，多数の S-box に非 0 の差分入力を与え，差分特性確率は，急速に減少する．しかし，各 S-box の手前に拡大鍵加算があるので，関連鍵攻撃においては，平文から伝わってきた差分を，拡大鍵の差分で打ち消してやれば，S-box の入力差分は 0 となり，確率 1 でその出力差分も 0 となる．

図 15 に Biryukov らの関連鍵攻撃における差分伝搬の基本戦略を示す．$4 \times 4$ の行列状に 16 Byte データを表し，着色部分の Byte に差分が入力され，白色部分は 0 差分を表す．鍵差分が 1 Byte に入り，S-box の一つに差分 (赤色) が入る．確率 $2^{-6}$ で，ある出力差分 (緑色) が期待される．Shift Row 及び Mix Column により，これは，4 Byte の差分 (灰色) に変換される．次段の拡大鍵加算において，同じ差分を拡大鍵に準備すれば，このデータの差分はキャンセルされ，次段の S 層入力は 0 差分となる．このように，データランダム化部の S-box 出力に発生した差分を拡大鍵差分で打ち消すような差分パスを想定することにより，高い差分特性確率が期待できる．この図 15 の差分パスは，local collision path と呼ばれ，同様の差分打ち消し構造を次の 2 段にも期待できる構造である．

鍵スケジュールの図 13 で明らかなように，AES-256 の場合，引き続く拡大鍵 32 Byte (= 2 段分) を指定すると，全ての拡大鍵は，一意に決定されてしまう．2 段分の local collision path となるように，鍵差分を設定しても，一般には次の 2 段分で，local collision path が期待できる訳ではない．しかしながら，この 2 段の local collision path を線形変換したものも，2 段で差分を打ち消す local collision path であるという性質がある．鍵スケジュールにおける非線形要素 S の入力差分を 0 とする鍵差分パスであれば，この性質を使って，次の 2 段にも差分確率の高い local collision path を作ることが可能である．

AES の 128 bit 鍵ではなく，より長い鍵長の 256 bit，192 bit のものが，full round 攻撃が可能であった理由の一つは，local collision path を次段以降も継続する鍵差分パスを構成することが，

（1） 鍵スケジュールが非線形部分の関与が薄い（弱い）構造であること

（2） 256 bit 鍵の方が，128 bit 鍵に比べ，鍵差分設定の自由度が高いこと

に起因すると推定される．文献(14)の著者は,「256 bit 鍵，192 bit 鍵の鍵スケジュールは，鍵差分に関し，ほとんど線形関数として取り扱うことができる」と述べている．

256 bit 鍵 AES の 14 段のうち，ブーメラン攻撃の平文側暗号変換 $E_0$ として 2 段目から 7 段目，暗号文側暗号変換 $E_1$ として 10 段目から 13 段目を選び，四つ組の差分パスを構成している．1 段目は，鍵を推定して鍵復元を行うために用い，8 段目，9 段目には Ladder Switch という手法を適用している(注11)最終段の 14 段目は，正しい四つ組の場合，S 層入力差分は 0 であり，$E_1$ に組み込んで考えても，除外して表現してもよい(注12)

このようにして，四つ組差分確率 $p^2q^2 = (2^{-30})^2(2^{-18})^2 =$

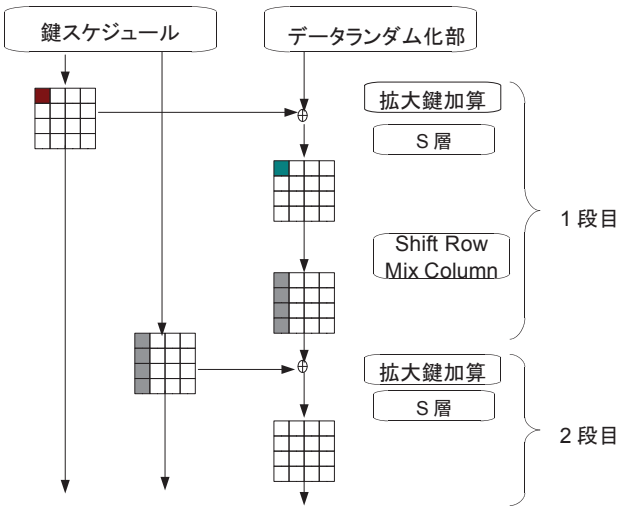



**図 15　関連鍵ブーメラン攻撃の差分伝搬**

(注11)：ブーメラン攻撃の接合部分（図 14 の変数 $X$ の位置する部分）は，段処理の境界で，128 bit 変数を一斉に切り替える必要はなく，並列処理可能な構造の範囲であれば，あるバイトは，S-box の前，他のバイトは，S-box の後ろで切り替え，正しい四つ組の確率 $p^2q^2$ を上げることができる．これを，Ladder Switch として提案している．

(注12)：論文の表記にしたがって，ここでは，$E_1$ から除外して説明している．

$2^{-96}$ のブーメラン差分パスを構成し，関連鍵攻撃により，AES-256 及び AES-192 は，full round を鍵の全数探索より少ない計算量で解読可能であると推定してる．具体的なブーメランパス及び，鍵推定アルゴリズムは，論文(14)を参照して頂くことにして，そこで，見積もられた攻撃コストを，表 2 に示す．表中のデータ数は，攻撃に必要な選択平文及び選択暗号文の個数であり，鍵数は，攻撃に必要な関連鍵の個数を表す．攻撃対象の鍵を $K_A$ とすれば，四つ組ブーメラン差分を保証する拡大鍵差分を持つ，鍵 $K_B$，$K_C$，$K_D$ の三つを被害者に計算させて，その鍵で，例えば，AES-256 であれば，$2^{95.5}$ 組の平文（若しくは暗号文）を暗号化（または復号) させるという攻撃条件である．

AES-256 では，関連鍵ブーメラン手法 (Related-key boomerang) を用いているが，AES-192 では，それを強化した，関連鍵ブーメラン増強型手法 (Related-key amplified boomerang) を用いる．これは，正しい四つ組として，図 14 の接合部分の差分を $(\beta, \gamma)$ のみではなく，平文差分 $\alpha$（及び暗号文差分 $\delta$ ）を与える複数の差分 $(\beta', \gamma')$ を想定し，マルチパスの考えで，正しい四つ組の発生確率の評価を増加させたものである．

**表 2　関連鍵攻撃の攻撃コスト**(14)

| 対象 | 段数 | 鍵数 | データ数 | 計算量 | メモリ |
|---|---|---|---|---|---|
| AES 192 bit 鍵 | 12 | 4 | $2^{123}$ | $2^{176}$ | $2^{152}$ |
| AES 256 bit 鍵 | 14 | 4 | $2^{95.5}$ | $2^{99.5}$ | $2^{77}$ |

## 7. AES に対する Biclique 攻撃

ASIACRYPT 2011 において，full round AES に対し，鍵の全数探索より少ない計算量で攻撃が可能との報告があった(15)．攻撃条件は，選択平文攻撃である．それによれば，計算量は，AES-128 に対し $2^{126.1}$ 回の暗号化計算量，同じく AES-192 に対し $2^{189.7}$，AES-256 に対し $2^{254.4}$ 回の暗号化計算量である．必要な選択平文数は，AES-128/AES-192/AES-256 に対し，それぞれ $2^{88}/2^{80}/2^{40}$ である．これら暗号の 10 段/12 段/14 段の全 round 中，2 段分に Biclique を適用し，残りラウンドで，中間一致攻撃の手法を適用している．

この攻撃法は，提案者も述べているように，実際の AES 使用に脅威となるものではない．また，SCIS 2012 において，この攻撃法の実効性に関し，議論した論文が発表されている(48)．そこでは，AES-128 において，Biclique を使わず，単に鍵総当りを中間一致の手法で行うならば，計算量は $2^{127.62}$ であり，同等であるとしている．Biclique 法で得られる攻撃計算量の削減効果は，$2^{126.1}/2^{127.62} \approx 1/2.8$ と，ごく僅かであり，より効果的な別の Biclique が存在する可能性について，懐疑的な意見(48)もあるが，ここでは，Biclique 法の原理を簡単に説明する．

### 7.1 中間一致法

共通鍵暗号において，平文 $P$ は，各段の処理が繰り返し適用され，暗号文 $C$ に変換される．その過程の中間段のデータを $S$ とする．暗号化関数を，この中間段で切って考えるならば，それは，$P$ から $S$ への変換 $S = g_K(P)$ と $S$ から $C$ への変換 $C = f_K(S)$ の合成 $E_K(P) = f_K(g_K(P))$ である．

$$P \xrightarrow{g_K} S \xrightarrow{f_K} C \tag{51}$$

中間段の選び方により，関数 $g_K(\cdot)$，$f_K(\cdot)$ に関わる鍵が，$K$ の全ビットではなく，一部のビットとし $g_K(\cdot) = g_{K1}(\cdot)$，$f_K(\cdot) = f_{K2}(\cdot)$ と書けたとする．このとき，全数探索法は，次のアルゴリズムで効率化できる．

Step.1　全ての鍵 $K1$ に対し，平文 $P$ を中間段データ $S = g_{K1}(P)$ に変換し，記録しておく．

Step.2　全ての鍵 $K2$ に対し，暗号文 $C$ を中間段データに逆変換 $S = f_{K2}^{-1}(C)$ する．Step.1 の記録に一致するものがあれば，それが正しい鍵（候補）である．

この攻撃法を中間一致攻撃という．なお，Step.1 と Step.2 は，逆順に行ってもよい．いずれの場合にも，Step.1 の結果を記録するメモリが必要である．暗号化計算量 1 回は，$g_K(\cdot)$，$f_K(\cdot)$ を 1 回づつ行う計算量であることに注意すれば，この攻撃計算量は，$2^{\max(|K1|,|K2|)}$ である．鍵 $K$ が，最も効率良く $K1$，$K2$ に分割できたとして(注13)攻撃計算量の下限は，$2^{|K|/2}$ であり，攻撃に必要なメモリ量も $2^{|K|/2}$ となる．すなわち，中間一致法を使う限り，128 bit 鍵の暗号において攻撃計算量は，$2^{64}$ を下回ることはない．

### 7.2 Biclique

暗号化関数を，前節と同じく $S = g_K(P)$ と $C = f_K(S)$ の合成とする．$2^d$ 種類の内部状態 $\{S_j\}$ が，$2^{2d}$ 種類の鍵 $\{K[i,j]\}$

$$\{K[i,j]\} = \begin{bmatrix} K[1,1] & K[1,2] & \dots & K[1,2^d] \\ \dots & & & \\ K[2^d,1] & K[2^d,2] & \dots & K[2^d,2^d] \end{bmatrix} \tag{52}$$

を使って，関数 $f$ により $2^d$ 種類の暗号文 $\{C_i\}$ に写像されているとする．三つ組 $[\{C_i\},\{S_j\},\{K[i,j]\}]$ が次式を満たすとき $d$ 次元 Biclique と言う．

$$C_i = f_{K[i,j]}(S_j)\ for\ all\ i,j \in \{1,\dots,2^d\} \tag{53}$$

言い換えれば，biclique において，鍵 $K[i,j]$ により，内部状態 $S_j$ が暗号文 $C_i$ に写像される．模式的に表現すれば，図 16 である．

### 7.3 Biclique 攻撃

暗号化関数 $E_K(\cdot)$ を，式 (51) のように，二つの関数 $g_K(\cdot)$ と $f_K(\cdot)$ の合成で表現する．攻撃の準備として，鍵空間を biclique を構成する鍵集合 $\{K[i,j]\}$ (式 (52)) の集合に分割する．鍵集合の中の鍵は，$2^d \times 2^d$ 行列の $i,j$ 要素であり，$2^{2d}$ 種類の鍵 $K[i,j]$ である．中間状態 $S_j$ が，鍵 $K[i,j]$ と関数 $f$ により，暗

(注13)：例えば，$K$ の前半分が $K1$，後半分が $K2$.

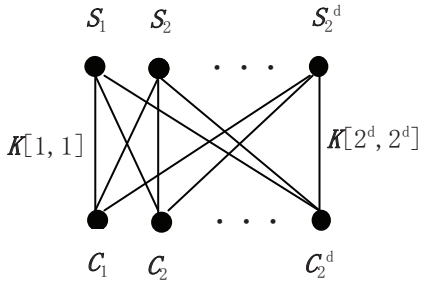



**図 16** $d$ **次元** biclique

号文 $C_i$ に写像されるとき，

$$\forall i,j : S_j \xrightarrow[f]{K[i,j]} C_i \tag{54}$$

と表す．各鍵 $K[i,j]$ に対し，上式の関係にある，三つ組 $[\{C_i\},\{S_j\},\{K[i,j]\}]$ データを用意する．

攻撃は，次の二つの Step である．

Step.1　攻撃対象の暗号器から，$C_i$ $(i=1,\ldots,2^d)$ に対応する平文 $P_i$ を手に入れる．

$$C_i \xrightarrow[E^{-1}(\cdot;K_{secret})]{decryption\ oracle} P_i \tag{55}$$

Step.2　鍵集合のどれかの鍵 $K[i,j]$ が，秘密鍵 $K_{secret}$ に等しいならば，それは中間状態 $S_j$ を平文 $P_i$ に写像するはずである．攻撃者は，次式を検査し

$$\exists i,j : P_i \xrightarrow[g]{K[i,j]} S_j \tag{56}$$

この関係を満たす鍵 $K[i,j]$ が秘密鍵の候補である．

この攻撃で，$2^{2d}$ 種類の鍵候補 $K[i,j]$ が検査できる．関数 $f$,$g$ 及び暗号関数 $E$ の 1 回の計算量をそれぞれ，$T_f$,$T_g$,$T_E$ とするならば，

$$T_E = T_f + T_g \tag{57}$$

であり，当然 $T_g < T_E$ である．共通鍵暗号では，暗号関数と復号関数の計算量は等しいので，この攻撃で，$2^{2d}$ 種類の鍵を検査する計算量は，

$$T = 2^d T_E + 2^{2d} T_g \approx 2^{2d} T_g < 2^{2d} T_E \tag{58}$$

と見積もれる．すなわち，総当りに比べ $T_g/T_E$ の計算量となる．

この論文[15]においては，AES-128 の 10 段に対し，8 段目から 10 段目にかけて Biclique を構成している．残りの 1 段目から 7 段目が関数 $g$ となるが，式 (56) の検査において，中間一致攻撃の手法を導入し，更に不要な S-box 計算を削除する等して，攻撃計算量を削減し，攻撃計算量は，$2^{126.1}$ 回の暗号化計算としている．

## 8. おわりに

本稿では，共通鍵ブロック暗号の 1990 年以降の代表的攻撃法として，差分攻撃，線形攻撃，高階差分攻撃の原理を紹介した．更に，AES に対する攻撃として，近年話題になった XSL 攻撃，関連鍵攻撃，Biclique 攻撃についてその概要を述べた．実用に供する共通鍵ブロック暗号の安全性は，各種の攻撃法の成果を基に総合的に判断される．攻撃法は，ここで紹介したものに限定されるわけではない．多くの学生が，この分野に興味を持ちここで紹介した攻撃法を発展させ，あるいは，新攻撃法を着想することを期待している．

## 文　献


(1) National Institute of Standards and Technology,“ Fips pub 46, data encryption standard (DES),” 1976.
(2) R. Sugarman, G. Davida, W. Tuchman, and D. Branstad,“ On foiling computer crime,” IEEE Spectr., vol.16, no.7, pp.31–41, 1979.
(3) E. Biham and A. Shamir,“ Differential cryptanalysis of the fu11 16-round DES,” Crypto’92, LNCS, vol.740, pp. 487–496, 1993.
(4) 松井　充,“ DES 暗号の線形解読法 (I),” SCIS 93-3C, 1993.
(5) M. Matsui,“ The first experimental cryptanalysis of DES,” Eurocrypt’93, LNCS, vol.765, pp. 386–397, 1994.
(6) K. Nyberg and L. R. Knudsen,“ Provable security against differential cryptanalysis,” Crypto’92, LNCS, vol.740, pp. 566–574, 1993.
(7) K. Nyberg,“ Differentially uniform mappings for cryptography,” Eurocrypt’93, LNCS, vol.765, pp. 55–64, 1994.
(8) T. Beth and C. Ding,“ On almost perfect nonlinear permutations,” Eurocrypt’93, LNCS, vol.765, pp. 65–76, 1993.
(9) L. R. Knudsen,“ Truncated and higher order differentials,” FSE’94, LNCS, vol.1008, pp.196–211, 1995.
(10) X. Lai,“ Higher order derivatives and differential cryptanalysis,” in Proceedings of symposium on communication, coding and cryptography,in honor of J. L. Massey on the occation of his 60th birthday, 1994.
(11) NIST,“ Announcing the Advance encryption standard(AES),” FIPS 197, Nov. 2001. http://csrc.nist.gov/publications/fips/fips197/fips197.pdf
(12) J. Daemen and V. Rijmen,“ The Rijndael block cipher,” AES Proposal, 1998.
(13) N.Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting,“ Improved cryptanalysis of rijndael,” FSE2000, LNCS, vol.1978, pp. 136–141, 2001.
(14) A. Biryukov and D. Khovratovich,“ Related-key cryptanalysis of the full AES-192 and AES-256,” Asiacrypt2009, LNCS, vol.5912, pp. 1–18, 2009.
(15) A. Bogdanov, D. Khovratovich and C. Rechberger,“ Biclique cryptanalysis of the full AES,” Asiacrypt2011, LNCS, vol.7073, pp.344–371, 2011.
(16) RSA Laboratories,“ DES challenge III,” `http://www.rsa.com/rsalabs/`
(17) RSA Laboratories,“ The RSA laboratories secret-key challenge,” http://www.rsa.com/rsalabs/
(18) E. Biham and A. Shamir,“ Differential cryptanalysis of DES-like cryptosystems,” Crypto’90, LNCS, vol.537, pp. 2–21, 1990.
(19) 宮川　洋, 岩垂好裕, 今井秀樹, 符号理論,16 章, 昭晃堂, 東京, 1973.
(20) CRYPTREC,“ CRYPTREC　技術報告書,”(2002〜) http://www.cryptrec.go.jp/estimation.html
(21) L. Knudsen,“ Block ciphers - a survey,” Proc. State of the Art in Applied Cryptography, LNCS, vol.1528, pp. 18–48, 1998.
(22) J. F. Dillon,“ APN polynomials: an update,” Fq9, International Conference on Finite Fields and their Applications, July 2009. http://mathsci.ucd.ie/ gmg/Fq9Talks/Dillon.pdf
(23) K. Nyberg and L. R. Knudsen,“ Provable security against a differential attack,” J. of Cryptology, 1995, vol.8, no.1, pp. 27–37, 1995.

(24) M. Matsui,“ New structure of block ciphers with provable security against differentialand linear cryptanalysis,” FSE’96, LNCS, vol.1039, pp. 205–218, 1996.
(25) T. Jakobsen and L. Knudsen,“ The interpolation attack on block ciphers,” FSE’97, LNCS, vol.1267, pp. 28–40, 1997.
(26) M. Matsui,“ New block encryption algorithm MISTY,” FSE’97, LNCS, vol.1267, pp. 54–68, 1997.
(27) 松井 充,“ ブロック暗号アルゴリズム MISTY,” 信学技報, ISEC 96-6, pp. 35–48, July 1996.
(28) L. R. Knudsen,“ Practically secure Feistel ciphers,” FSE’93, LNCS, vol.809, pp. 211–221, 1993.
(29) S. K. Langford and M. E. Hellman,“ Differential-linear cryptanalysis,” Crypto’94, LNCS, vol.839, pp. 17–25, 1994.
(30) K. Aoki and K. Ohta,“ Differential-linear cryptanalysis of FEAL-8,” IEICE Trans. Fundamentals, vol. E79-A, no.1, pp. 20–27, Jan. 1996.
(31) X. Lai, J. Massey, and S. Murphy,“ Markov ciphers and differential cryptanalysis,” Eurocrypt’91, LNCS, vol.547, pp. 17–38, 1991.
(32) B. Kaliski and M. Robshaw,“ Linear cryptanalysis using multiple approximations,” Crypto’94, LNCS, vol.839, pp.26–39, 1994.
(33) B. Kaliski and M. Robshaw,“ Linear cryptanalysis using multiple approximation and FEAL,” FSE’94, LNCS, vol.1008, pp. 249–264, 1994.
(34) T. Shimoyama and T. Kaneko,“ Quadratic relation of S-box and its application to the linear attack of full round DES,” LNCS, vol.1462, Crypto’98, pp. 200–211, 1998.
(35) E. Biham, A. Biryukov, and A. Shamir,“ Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials,” Eurocrypt’99, LNCS, vol.1592, pp. 12–23, 1999.
(36) L. Knudsen and D. Wagner,“ Integral cryptanalysis,” FSE 2002, LNCS, vol.2365, pp. 112–127, 2002.
(37) J. Daemen, L. Knudsen, and V. Rijmen,“ The block cipher square,” FSE’97, LNCS, vol.1267, pp. 149–171, 1997.
(38) T. Shimoyama, S. Moriai, T. Kaneko, and S. Tsujii,“ Improved higher order differential attack and its application to nyberg-knudsen’s designed block cipher,” IEICE Trans. Fundamentals, vol.E82-A, no.9, pp. 1971–1980, Sept. 1999.
(39) S. Moriai, T. Shimoyama, and T. Kaneko,“ Higher order differential attack of a cast cipher,” FSE’98, LNCS, vol.1372, pp. 17–31, 1998.
(40) K. Aoki,“ Practical evaluation of security against generalized interpolation attack,” IEICE Trans. Fundamentals, vol. E83-A, no.1, pp. 33–38, Jan. 2000.
(41) Y. Hatano, H. Tanaka, and T. Kaneko,“ Optimization for the algebraic method and its application to an attack of MISTY1,” IEICE Trans. Fundamentals, vol. E87-A, no.1, pp. 18–27, Jan. 2004.
(42) Y. Tsunoo, T. Saito, M. Shigeri, and T. Kawabata,“ Security analysis of 7-round MISTY1 against higher order differential attacks,” IEICE Trans. Fundamentals, vol. E93-A, no.1, pp. 144–152, Jan. 2010.
(43) 井上祐輔, 北川明伸, 金子敏信,“ AES に対する高階差分攻撃における攻撃方程式解法の高速化 (II),” 信学技報, ISEC 2012-31, SITG2013-27, ICSS2012-33, MM2012-23, pp. 159–166, July 2012.
(44) N. T. Courtois and J. Pieprzyk,“ Cryptanalysis of block ciphers with overdefined systems of equations,” IACR ePrint archive 2002/044, 2002.
(45) N. T. Courtois and J. Pieprzyk,“ Cryptanalysis of block ciphers with overdefned systems of equations,” Asiacrypt2002, LNCS, vol.2501, pp. 267–287, 2002.
(46) G. Gong,“ Sequences, DFT and resistance against fast algebraic attacks,” SETA 2008, LNCS, vol.5203, pp. 197–218, 2008.
(47) S. Ronjom, G. Gong, and T. Helleseth,“ A survey of recent attacks on the filter generator,” AAECC 2007, LNCS, vol.4851, pp. 7–17, 2007.
(48) 青木和麻呂,“ 改善された力まかせ攻撃法の実効性について-AES と Camellia の (再) 評価,” SCIS 2012, 1C2-5, 2012.
(49) D. Wagner,“ The boomerang attack,” FSE’99, LNCS, vol.1636, pp. 156–170, 1999.
(50) E. Biham, O. Dunkelman, and N. Keller,“ New results on boomerang and rectangle attacks,” FSE2002, LNCS, vol.2365, pp. 1–16, 2002.
(51) M. E. Hellman and S. K. Langford,“ Differential-linear cryptanalysis,” Crypto’94, LNCS, vol.839, pp. 26–39, 1994.

（幹事団提案，平成 25 年 3 月 18 日受付　5 月 1 日最終受付）

**金子敏信**（正員：フェロー）
昭 46 東大・工・電子卒，昭 51 同大学院博士課程了．工博．同年東京理科大・理工に奉職．平 5 同大学教授，現在に至る．誤り訂正符号，共通鍵暗号の研究に従事．平 13 CRYPTREC 共通鍵評価小委員会委員長．平 15 情報理論とその応用学会監事．平 13 本会基礎・境界ソサイエティ副会長．平 16 陸上自衛隊通信団表彰．平 25 情報セキュリティ文化賞．著書「誤り訂正符号とその応用」「情報セキュリティハンドブック」など．