コンピュータセキュリティ　18－30
(2002. 7. 19)

CIPHERUNICORN-A の差分解読/線形解読に対する安全性について

角尾幸保† 久保博靖‡ 山田真紀‡ 洲崎智保‡ 宮内宏†

†日本電気株式会社 〒216-8555 神奈川県川崎市宮前区宮崎四丁目1番1号
‡北陸日本電気ソフトウェア株式会社 〒920-2141 石川県石川郡鶴来町安養寺1番地
E-mail: †{tsunoo@BL, h-miyauchi@BC}.jp.nec.com, ‡{kubo, yamada, suzaki}@bd1pws.hnes.nec.co.jp

あらまし　本稿では，128ビットブロック暗号であるCIPHERUNICORN-Aの差分解読／線形解読に対する安全性について報告する．CIPHERUNICORN-Aのラウンド関数は複雑な構造をしているため，正確な差分／線形確率の計算が困難である．従来の評価では鍵加算と定数乗算を近似したmF関数を定義し，差分／線形特性確率を求めていた．しかし，この定数乗算の近似ではあり得る差分／線形経路を全て網羅していなかったため評価が十分ではなかった．

本稿では，定数乗算を近似しない mF'関数を新たに定義し，バイトオリエンテッドな差分／線形経路を再度全数探索した．また，定数乗算における確率を導入し，差分／線形特性確率を従来よりも厳密に求めた結果を報告する．

キーワード　ブロック暗号，CIPHERUNICORN-A，差分解読，線形解読

Differential and Linear cryptanalysis of CIPHERUNICORN-A

Yukiyasu TSUNOO† Hiroyasu KUBO‡ Maki YAMADA‡ Tomoyasu SUZAKI‡ Hiroshi MIYAUCHI†

†NEC Corporation 4-1-1, Miyazaki, Miyamae-ku, Kawasaki, Kanagawa 216-8555, Japan
‡NEC Software Hokuriku, Ltd. 1, Anyouji, Tsurugi, Ishikawa, Ishikawa 920-2141, Japan
E-mail: †{tsunoo@BL, h-miyauchi@BC}.jp.nec.com, ‡{kubo, yamada, suzaki}@bd1pws.hnes.nec.co.jp

Abstract In this paper, we describe an experimental result of safety against differential and linear cryptanalysis of CIPHERUNICORN-A. Because of the complex structure, it is difficult to calculate the probability of differential and linear characteristics of CIPHERUNICORN-A.

We used an mF function in our previous evaluation in order to be able to do the approximate calculation in short term. But, by using the mF function, the approximation of the constant multiplication did not have enough coverage with its possible influential bits relations in differential and linear cryptanalysis. The mF function has two changes from original F function. One is key additions and the other is constant multiplications modified to exclusive OR operations. In this paper, we used a newly defined the mF' function which omitted the change of constant multiplications, searched exhaustively byte-oriented differential and linear influential paths and investigated more strict differential and linear characteristic probabilities.

Keyword Block Cipher, CIPHERUNICORN-A, Differential Cryptanalysis, Linear Cryptanalysis

1. はじめに

CIPHERUNICORN-A[1]は，NEC が提案する共通鍵暗号ファミリ CIPHERUNICORN の 1 メンバであり，データブロック長 128 ビット，鍵長 128，192，256 ビットの何れかを利用できる DES 型ブロック暗号である．また，情報処理振興事業協会および通信・放送機構が公募した電子政府調達暗号候補として応募しており，現在も CRYPTREC 評価委員会において継続評価されている．

CIPHERUNICORN-A のラウンド関数は複雑な構造をしているため，正確な差分／線形確率の計算が困難である．自己評価書[2]では，F 関数の鍵加算と定数乗算を近似した mF 関数を定義し差分／線形特性確率を求めた．その結果，差分特性確率は 15 ラウンドで 2^{-120} 以下，線形特性確率は 15 ラウンドで 2^{-157} 以下となったが，経路の探索が十分ではなかったためこれより大きな確率になり得るとの指摘[3]がある．また，CRYPTREC 評価委員会が 2002 年 3 月に公表した評価報告[4]によると，mF 関数で近似した場合の差分特性確率は 13 ラウンドで 2^{-100} 以下，同様に線形特性確率

は 13 ラウンドで 2^{-128} 以下と報告されている．このように，mF 関数を用いた評価では確率の上界が十分な安全性を保証出来ておらず，より厳密に確率を調査する必要がある．

本稿では，近似の方法を変更した mF'関数を新たに定義する．バイトオリエンテッドな差分／線形経路を全数探索し，定数乗算による確率も考慮し詳細に評価する．結果として，一部予想値を含むが 13 ラウンドでの差分／線形特性確率がともに 2^{-128} を下回ることを確認し，差分解読／線形解読に対して安全であろうという結果を得たので報告する．

2 章では，まず CIPHERUNICORN-A の構造と自己評価書での評価の問題点を述べ，本稿での評価の概要を説明する．3 章では，mF'関数を用いた差分特性確率の導出方法と結果を，同様に 4 章では線形特性確率について説明する．最後に 5 章でまとめと考察を述べる．

2. 評価の概要

本章では，CIPHERUNICORN-A の F 関数，自己評価書で使用した mF 関数，および，本稿の評価で使用する mF'関数について説明する．また，自己評価書における評価と本稿の評価の違いを示しながら，本稿の評価の概要について述べる．

2.1. CIPHERUNICORN-A の構造

CIPHERUNICORN-A は F 関数（図 1）を 16 ラウンド繰り返す DES 型暗号である．F 関数は，本流部と一時鍵生成部（以後，TKG と呼ぶ）から構成され，本流部では入力 64 ビットと拡大鍵 FKa，FKb を加算し，A3 関数，定数乗算，T_n 関数により攪拌する．TKG では，拡大鍵 SKa，SKb と入力 64 ビットとを加算し，定数乗算，T_n 関数を通過後，一時鍵を取り出す．最後に，本流部と TKG を合流し，出力 64 ビットを生成する．

鍵加算と定数乗算は，GF(2^{32})上の演算を行う．A3 関数（64 ビット入出力）は，入力データ，および入力データを 23, 41 ビット左ローテイトシフトした値を排他的論理和する．T_n 関数（32 ビット入出力）は，n で指定した番号の入力バイトを 4 個の換字テーブルを通して出力とする．T_k 関数は，T_n 関数の n を一時鍵で決定する関数である．

2.2. 従来の評価

自己評価書では差分／線形特性確率を求めるにあたって，F 関数を近似した mF 関数（図 2）を定義した．mF 関数の定数乗算は下位 3 バイトを最上位 1 バイトに排他的論理和する処理に置き換えている．経路探索では，下位 3 バイトに差分が入ったとき必ず最上位バイトに差分が出るものとして扱っていたが，実際の定数乗算では最上位バイトに差分が出ない場合も存在するため，全てのパタンについて評価されていなかった．同様に線形確率についても全てのパタンは網羅されていなかった．

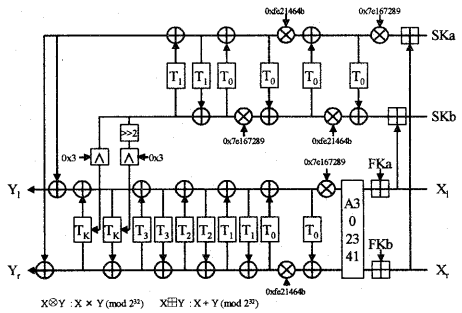

図 1　F 関数

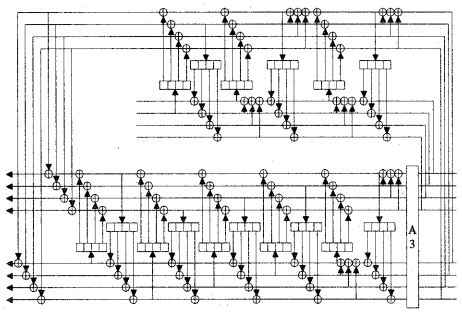

図 2 mF 関数

2.3. 本稿の評価方法

本稿の評価では，新たに mF'関数（図 3）を定義する．

mF'関数について，経路を全数探索し最大もしくは上界となる確率を検討する．ここで，mF'関数は全単射でないことから，mF'関数の出力差分（あるいは入力マスク）が 0 の場合と非 0 の場合に分けて計算する．

学術的な観点から 3R-attack を考慮し，13 ラウンドでの特性確率が 2^{-128} 以下になることを確認する．つまり，mF'関数あたりでは出力差分（あるいは入力マスク）が 0 の場合で $2^{-21.334}$ 以下，出力差分（あるいは入力マスク）が非 0 の場合で $2^{-16.000}$ 以下となることを確認していくことにする．

従来の評価との主な違いは以下の点である．

- 定数乗算はバイトオリエンテッドで起こり得る経路全てを探索し，確率は実際に測定した値，もしくは予想値を用いる．

• 差分特性の経路において排他的論理和演算部分での経路探索は，2 入力ともに差分が存在する場合に出力に差分が出る場合と出ない場合の両方を調査する．

• 線形特性の経路において分岐部分での経路探索は，2 入力ともにマスクが存在する場合に出力にマスクが出る場合と出ない場合の両方を調査する．

本稿では，バイトオリエンテッドで表現した差分やマスクを 101x のように表記する．例えば 101x は，32 ビットの差分（あるいはマスク）を 4 バイトの連結 b0 ‖ b1 ‖ b2 ‖ b3 とすると，b0≠0，b1＝0，b2≠0，b3 は 0 あるいは非 0 であることを意味する．

2.3.1. mF'関数

mF'関数は，定数乗算の近似を行わない点が mF 関数とは異なる．以降の説明のために各部品関数の名称を定義する．定数乗算については，本流部の入力側から順に m1，m2 とする．TKG の定数乗算についても同様に m3，m4，m5，m6 とする．T_n 関数については，本流部の入力側から順に Ta，Tb，...，Th とし，TKG の T_n 関数も同様に Tu，Tv，...，Tz とする．なお，T_k 関数については入力側から Tka，Tkb とする．また，拡大鍵の挿入については排他的論理和で近似することとし，本稿では省略する．

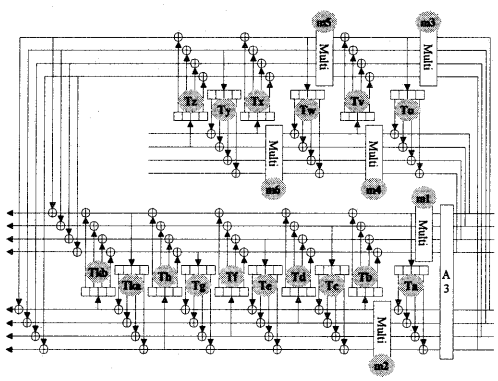

図 3 mF'関数

2.3.2. 拡大鍵の移動

拡大鍵は本流部，TKG へそれぞれ 64 ビットずつ挿入されている．本流部へは FKa(32 ビット)および FKb（32 ビット）が，TKG へは SKa（32 ビット）および SKb（32 ビット）が挿入されている．これらの鍵は，図 4に示すように変形して移動させることができる．移動させた鍵を FKa，FKb，SKa，SKb に対して，それぞれ FK'a，FK'b，SK'a，SK'b と呼ぶことにし，部品関数の入力の独立性を確認する際に使用する．

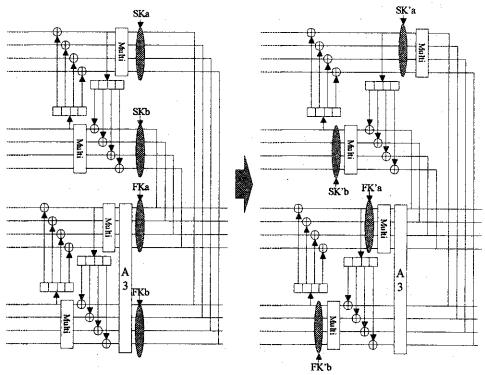

図 4 拡大鍵の変形移動

3. 差分特性確率

まず，mF'関数についてバイトオリエンテッドな経路を全数探索し，確率が最大となる経路を求め，その確率を用いて暗号全体の確率を計算する．しかしながら，T_n 関数のアクティブ数のみで安全性の条件を満たさない経路を出力しようとすると，3.1節の条件では，A3 関数と定数乗算の部分でパタン数が増加し，組み合わせが膨大になってしまうという問題がある．そこで，本流部と TKG は拡大鍵によって入力が独立であると考えられることから，それぞれ独立に確率を求め探索の手間を削減する．求めた確率から，

mF'関数の特性確率

=本流部での特性確率×TKG での特性確率

と計算する．

3.1. 差分経路探索における部品関数の扱い

経路探索と確率計算を行うにあたって部品関数の扱いを検討する．

3.1.1. T_n 関数

T_n 関数の差分確率は，換字テーブル単体では 2^{-6} となることを確認しているが，換字テーブルを連結した場合の差分確率も調査した．その結果を表 2に示す．

3.1.2. T_k 関数

T_k 関数については，入力となるバイト位置が変化する構造のため，T_k 関数がアクティブにならない場合が一番弱くなるものと考えることにする．

3.1.3. A3 関数

A3 関数については，入力側と出力側でバイトオリエンテッドな差分経路全ての組み合わせについて経路を探索する．調査しきれなかった部分については全ての経路が存在するものとする．このことから実際に存在しない組み合わせも含まれるが，差分特性確率の上界を求めるという意味では問題ない．A3 関数は，どのよ

うな入出力差分の場合も確率1として計算する．

3.1.4. 定数乗算

定数乗算については，バイトオリエンテッドであり得る差分経路全てを考慮する．経路によっては差分確率を詳細に調査し，mF'関数の確率をより厳密な値へ近似する．しかし，厳密な確率を求めるのは計算量的に困難なことがあるため，必要に応じて計算量の効率化を行い，確率の上界を求めることにする（表 3）．

- 定数乗算は全単射であることから，正方向，逆方向（逆関数を用いる）のうち計算量が少ない方を選択して求める．
- 差分の出現頻度を調べる表は最大で 2^{32} のテーブルが必要であり，計算機上に全てを保持することは困難である．従って，出力側の差分値を一部のビットについてのみ調査する．例えば出力側の上位24ビットに注目して差分の出現頻度を調べた場合，0x12345678 という差分値と 0x123456ab という差分値を同じ差分値として扱う．差分確率としては弱く見積もることになり，設計者に有利な結果になることはない．
- 定数乗算の出力差分が T_n 関数の出力差分と消しあう経路になっている場合，T_n 関数がとり得る出力差分についてのみ確率を計算する（図 5）．
- 上記効率化を施しても，あるいは施すことができずに計算量が大きくなるパタンもある．これらについては少量の乱数データを与え予想する．一例として，表3の通番2の実験を乱数データ 2^{20} で調査したところ $2^{-4.983}$ となった．全数で求めた結果が $2^{-4.994}$ であったことから，予想値を用いてもおおよその確率を見積もることが可能であると判断した．

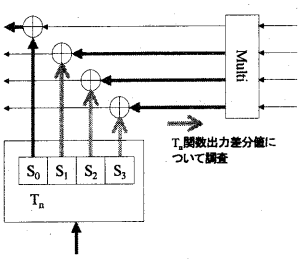

図 5 定数乗算と T_n 関数の出力差分が消しあう例

3.2. 本流部の差分特性確率

本流部の差分特性確率は，拡大鍵 FK によって独立であることが保証できる部品関数（T_n 関数，定数乗算）の確率の積で求めることにする．

以下の実験と考察より，本流部の差分特性確率は最大でも以下の値になると考えられる．

- 出力差分が0のとき $2^{-14.000}$ 以下
- 出力差分が非0のとき $2^{-7.000}$ 以下

3.2.1. 出力差分が 0 の場合

mF'関数の出力差分が 0 となる可能性があるのは，本流部の上位4バイトと下位4バイトの出力差分が等しいときである．本流部の出力側からバイトオリエンテッドで上位4バイトと下位4バイトが等しくなる16パタンの丸め差分を試行しアクティブな T_n 関数が1個以下になる場合を探索したところ，Tb のみがアクティブになるパタンただ一つであった（図 6）．この場合，m1 で入力丸め差分 xxx1 が出力丸め差分 0111 になって，かつ，Tb 出力差分と消える差分値でなければならない．m1 の確率については Tb が出力し得る差分値に限定して計算を行い $2^{-7.181}$ となった．従って，このときの本流部の確率は最大でも $2^{-7.181} \times 2^{-7.000} = 2^{-14.181}$ 以下であると考えられる．

本流部でアクティブな T_n 関数が2個以上の場合，それぞれの T_n 関数の入力は独立であるとみなすことができることから，最大でも $2^{-14.000}$ 以下であると考えられる．従って，出力差分が0の場合，本流部の確率は最大でも $2^{-14.000}$ 以下であると言える．

3.2.2. 出力差分が非 0 の場合

本流部の上位4バイトと下位4バイトの出力差分が等しいときを除いて本流部で確率が最大となる経路を求めた．その結果，Ta のみアクティブになるパタンが最大となり，このときの本流部の確率は $2^{-7.000}$ であった．

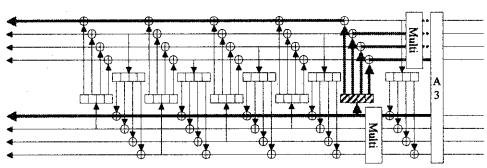

図 6 本流部において Tb のみアクティブになる場合

3.3. TKG の差分特性確率

ここで，mF'関数あたりの差分特性確率として，出力差分が0の場合で $2^{-21.334}$ 以下，出力差分が非0の場合で $2^{-16.000}$ 以下となることを確認したいので，TKG の

確率については以下の値になることを検証する.

- 出力差分が 0 のとき

$2^{(-21.334)-(-14.000)} = 2^{-7.334}$ 以下

- 出力差分が非 0 のとき

$2^{(-16.000)-(-7.000)} = 2^{-9.000}$ 以下

TKG の差分特性確率は，拡大鍵 SK によって独立であることが保証できる部品関数（T_n関数，定数乗算）の確率の積で求めることにする．独立ではない部品関数については，本稿では確率を 1 とみなすことにする．本節では，TKG におけるアクティブな T_n関数の個数によってそれぞれの確率の上界を求め，最大となる確率を TKG の確率として採用する．

以下の実験と考察より，TKG の差分特性確率は最大でも $2^{-11.994}$ であると考えられる．

- アクティブな T_n関数が 0 個のとき

$2^{-12.304}$ 以下

- アクティブな T_n関数が 1 個のとき

$2^{-11.994}$ 以下（予想値含む）

- アクティブな T_n関数が 2 個以上のとき

$2^{-14.000}$ 以下

3.3.1. アクティブな T_n関数が 0 個の場合

アクティブな T_n関数が 0 個となるのは，以下に示す条件 1 または条件 2 の少なくともどちらか一方が成立するときのみである．

条件 1）m3 出力丸め差分=0xxx，かつ，
m5 出力丸め差分=00xx

条件 2）m4 出力丸め差分=0xxx，かつ，
m6 出力丸め差分=00xx

各条件について3.1.4節の効率化を適用して確率を求めた．具体的には，例えば条件 1 の場合，m5 逆関数について入力丸め差分値が 00xx である差分値全てについて出力差分値の上位 1 バイトが 0 となるペアを抽出する．次に，そのペアに対して Tv がとり得る出力値を排他的論理和し，m3 逆関数への入力ペアとする．m3 逆関数の出力丸め差分値上位 2 バイトに注目して出現頻度を調査する．以下にアルゴリズムを示す．

step1)m5 逆関数に入力丸め差分 00xx を全数与える(2^{16}-1 通り)
step1-1)m5 逆関数にデータを全数与える(2^{31} ペア)
step1-1-1)m5 逆関数の出力丸め差分が 0xxx となるペア(X とする)は step1-1-2 へ
step1-1-2) Tv 出力を全数与える(256 通り:Y とする)
step1-1-2-1)ペア X の 2 文それぞれに Y を排他的論理和する(Z とする)
step1-1-2-2)ペア Z を m3 逆関数に与える
step1-1-2-3)m3 逆関数の出力差分を上位 16 ビットでカウントする
step1-2)step1-1-2-3 でカウントした中から最大値を探す
(step1 で与えた差分における最大値)
step1-3)step1-2 の最大値が過去の最大値より大きければ新たに最大値 max とする
(条件 1 における最大値)
step2)max から確率を求める
(max÷m5 逆関数に与えたペア数(2^{31})
÷T 関数出力数(2^8))

3.3.2. アクティブな T_n関数が 1 個の場合

アクティブな T_n関数が 1 個となるのは，表 4に示す 6 パタンである．表 4の通番 1 を図示した例が図 7である．図中の太線は差分が通過する経路を表し，点線は差分が通過する場合としない場合があることを表している．

各パタンにおいて表 4の項目"独立な部品関数"に記載の部品関数はそれぞれ独立とみなすことができると考える．通番 1（図 7）については，m5 の入力下位 3 バイトは Tu の入力とは独立であると考える．最上位 1 バイトは SKb が作用している Tv 出力が影響しており，Tu の入力とは独立であると考える．これらのことから，Tu と m5 は独立であると考える．通番 2～5 については T_n関数と定数乗算の入力はそれぞれ SKa, SKb により独立であると考える．通番 6 については，Tz の入力は SKa が作用している Ty の出力によって m6 と独立であると考える．

これらの部品関数の確率を求め，TKG の確率を表したものが表 4の項目"TKG の確率"である．この結果から，アクティブな T_n関数が 1 個の場合の確率は最大でも $2^{-11.994}$ 以下（予想値含む）であると考えられる．

3.3.3. アクティブな T_n関数が 2 個以上の場合

アクティブな T 関数が 2 個以上になる場合，独立ではない部品関数を確率 1 とみなしても，少なくとも 2 以上の T_n関数は独立であると考えられる．従って，最大でも $2^{-14.000}$ 以下であると言える．

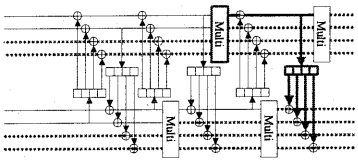

図 7 TKG において Tu のみアクティブになる場合

3.4. CIPHERUNICORN-A の差分特性確率

これまでの結果をまとめたものを表 1に示す．この結果から mF'関数の差分特性確率は，最大でも次の値であると考えられる．ただし，上界を示しているだけであって，本流部で確率が最大となった経路と，TKG で確率が最大となった経路が必ずしも繋がるわけではない．

- 出力差分が 0 のとき

$2^{-(14.000+11.994)} = 2^{-25.994}$ 以下

- 出力差分が非 0 のとき

$2^{-(7.000+11.994)} = 2^{-18.994}$ 以下

従って，13 ラウンドでの確率は最大でも次の値であると考えられる．

- 出力差分が 0 のとき

$2^{-25.994 \times \lfloor 13 \times 1/2 \rfloor} = 2^{-155.96}$ 以下

- 出力差分が非 0 のとき

$2^{-18.994 \times \lfloor 13 \times 2/3 \rfloor} = 2^{-151.95}$ 以下

表 1 差分特性確率評価結果

mF'関数 出力差分	調査対象	T_n関数の ｱｸﾃｨﾌﾞ数	確率 上界	参照 節
0	本流部	1	$2^{-14.171}$	3.2.1
		2 以上	$2^{-14.000}$	3.2.1
	TKG	0	$2^{-12.304}$	3.3.1
		1(*1)	$2^{-11.994}$	3.3.2
		2 以上	$2^{-14.000}$	3.3.3
非 0	本流部	1 以上	$2^{-7.000}$	3.2.2
	TKG	0	$2^{-12.304}$	3.3.1
		1(*1)	$2^{-11.994}$	3.3.2
		2 以上	$2^{-14.000}$	3.3.3

(*1)予想値を含む

4. 線形特性確率

まず，mF'関数についてバイトオリエンテッドな経路を全数探索し，確率が最大となる経路を求め，その確率を用いて暗号全体の確率を計算する．

4.1. 線形経路探索における部品関数の扱い

経路探索と確率計算を行うにあたって部品関数の扱いを検討する．

4.1.1. T_n 関数

T_n 関数の線形確率は，アクティブな換字テーブルによって確率が異なることを考慮する必要がある．換字テーブルを連結した場合の確率を表 2に示す．

4.1.2. T_k 関数

T_k 関数については，変化する入力場所を全パタン（Tka，Tkb それぞれ 4 パタン）試行する．

4.1.3. A3 関数

A3 関数については，入力側と出力側でバイトオリエンテッドな線形マスクが非 0 の全ての組み合わせについて経路を探索する．中には実際に存在しない組み合わせも含まれるが，線形特性確率の上界を求めるという意味では問題ない．A3 関数は，どのような入出力マスクの場合も確率 1 として計算する．

4.1.4. 定数乗算

定数乗算については，バイトオリエンテッドであり得る線形マスク全てを考慮する．定数乗算は，どのような入出力マスクの場合も確率 1 として計算する．

4.2. mF'関数の線形特性確率

バイトオリエンテッドな線形マスクの経路を本流部，TKG とも，あり得る全ての経路について調べる．各経路においてアクティブな換字テーブルから mF'関数の線形特性確率が最大となるものを探索する．

以下の考察より，mF'関数の線形特性確率は最大でも以下の値になると考えられる．

- 入力マスクが 0 のとき $2^{-21.369}$ 以下
- 入力マスクが非 0 のとき $2^{-21.036}$ 以下

4.2.1. 入力マスクが 0 の場合

入力マスクが 0 の場合に確率が最大となった経路の一例を図 8に示す．図 8において，FK，SK が一様にランダムであるとすると，変形移動させることで，アクティブとなっている換字テーブルの入力は独立であると考えられる．Ta，Tc，Te，Tg については，入力に FK'a が作用し，Tka の入力には FK'b が作用した Th の出力が作用している．また，Tv の入力には SK'b が作用し Tx，Tz の入力には SK'a が作用した Tw の出力が作用している．従って，mF'関数あたりの線形特性確率は以下の式で求めることができる．

$\{(S_0 \| S_1 \| S_2 \| S_3)$で入力マスク$\neq 0\}$
$\times \{(S_0 \| S_1 \| S_2 \| S_3)$で入力マスク$=0\}^7$

$= 2^{-2.385} \times 2^{(-2.712\times 7)} = 2^{-21.369}$

4.2.2. 入力マスクが非 0 の場合

入力マスクが非 0 の場合に最大になった経路を図 9 に示す．図 9においても図 8と同様に，FK，SK が一様にランダムであるとすると，変形移動させることで，アクティブとなっている換字テーブルの入力は独立であると考えられる．Tb，Td，Tf，Th については，入力に FK'b が作用し，Tka の入力には FK'a が作用している．Tkb の入力には FK'a が作用した Tg の出力が作用している．従って，mF'関数あたりの線形特性確率は以下の式で求めることができる．

$\{(S_1 \| S_3)$で入力マスク$\neq 0\} \times \{S_3\}$
$\times \{(S_1 \| S_2 \| S_3)$で入力マスク$\neq 0\}$
$\times \{(S_1 \| S_2 \| S_3)$で入力マスク$=0\}^3$
$= 2^{-3.081} \times 2^{-6.000} \times 2^{-2.712} \times 2^{(-3.081\times 3)} = 2^{-21.036}$

4.3. CIPHERUNICORN-A の線形特性確率

mF'関数の線形特性確率から，13 ラウンドでの確率は最大でも次の値であると考えられる．

- 入力マスクが 0 のとき

$2^{-21.369\times\lfloor 13\times 1/2\rfloor} = 2^{-128.214}$ 以下

- 入力マスクが非 0 のとき

$2^{-21.036\times\lfloor 13\times 2/3\rfloor} = 2^{-168.288}$ 以下

5. まとめ

本稿では，mF'関数を新たに定義して経路探索を実施し，CIPHERUNICORN-A の差分解読／線形解読に対する安全性を検討した．その結果，定数乗算の差分確率は一部予想値を含むが，差分／線形特性確率ともに 13 ラウンドで 2^{-128} 以下であると予想できた．

本稿では，計算量の都合から定数乗算については一部予想値を用いているが，調査を継続し予想値の正当性を確認する必要がある．

また，独立ではないと思われる部品関数については確率を 1 としたが，それらの部品関数も同時に考慮し，より正確な確率を調査する必要があると考える．同様に，T_k 関数が及ぼす影響についても考慮した調査が必要であると考える．

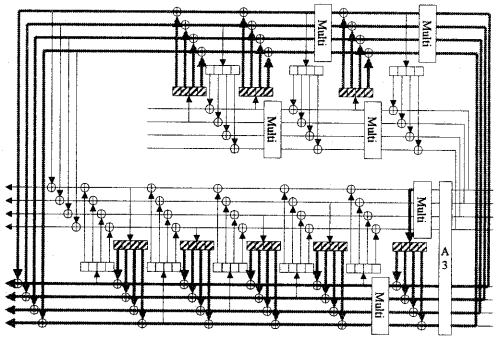

図 8 線形特性確率が最大となる場合
（入力マスク=0）

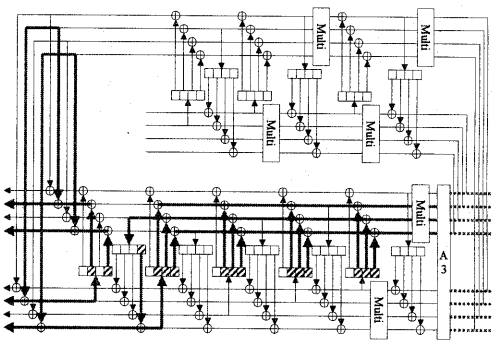

図 9 線形特性確率が最大となる場合
（入力マスク≠0）

文　献

[1] 日本電気株式会社，“暗号技術仕様書 CIPHERUNICORN-A,” CRYPTREC 応募書類, 2001.

[2] 日本電気株式会社，“自己評価書 CIPHERUNICORN-A,” CRYPTREC 応募書類, 2001.

[3] 関根泰樹，金子敏信，“CIPHERUNICORN-A の Truncated 差分攻撃に関する一考察，” ISEC2001-120，2002.

[4] 情報処理振興事業協会，通信・放送機構，“暗号技術評価報告書（2001 年度版）CRYPTREC Report 2001，” 2002.

表 2 換字テーブルの確率

換字テーブルの組み合わせ	差分確率	線形確率	
		入力ﾏｽｸ =0	入力ﾏｽｸ ≠0
S0	$2^{-6.000}$	$2^{-6.000}$	—
S1	$2^{-6.000}$	$2^{-6.000}$	—
S2	$2^{-6.000}$	$2^{-6.000}$	—
S3	$2^{-6.000}$	$2^{-6.000}$	—
S0 ‖ S1	$2^{-7.000}$	$2^{-3.081}$	$2^{-3.825}$
S0 ‖ S2	$2^{-7.000}$	$2^{-3.081}$	$2^{-3.660}$
S0 ‖ S3	$2^{-7.000}$	$2^{-3.081}$	$2^{-3.504}$
S1 ‖ S2	$2^{-7.000}$	$2^{-3.081}$	$2^{-3.504}$
S1 ‖ S3	$2^{-7.000}$	$2^{-3.081}$	$2^{-3.825}$
S2 ‖ S3	$2^{-7.000}$	$2^{-3.215}$	$2^{-3.660}$
S0 ‖ S1 ‖ S2	$2^{-7.000}$	$2^{-2.599}$	$2^{-3.215}$
S0 ‖ S1 ‖ S3	$2^{-7.000}$	$2^{-2.599}$	$2^{-3.215}$
S0 ‖ S2 ‖ S3	$2^{-7.000}$	$2^{-2.712}$	$2^{-3.215}$
S1 ‖ S2 ‖ S3	$2^{-7.000}$	$2^{-2.712}$	$2^{-3.081}$
S0 ‖ S1 ‖ S2 ‖ S3	$2^{-7.000}$	$2^{-2.385}$	$2^{-2.712}$

表 3 調査した定数乗算の最大差分確率

通番	定数	入力丸め差分値	出力丸め差分値	最大確率
1	0x7e167289	xxx1	0111(*1)	$2^{-7.181}$
2	(m1,m3,m6)	1xxx	00xx	$2^{-4.994}$
3		0xxx	01xx	$2^{-4.995}$(*2)
4	0xfe21464b	1xxx	00xx	$2^{-5.710}$
5	(m2,m4,m5)	0xxx	01xx	$2^{-5.371}$

- xは0,1どちらでも可とする.
- 何れの項目も定数乗算の逆関数を使用し，入力丸め差分値上位24ビットのみに注目して出現頻度を調査した.

(*1)T_n関数の出力差分と消える場合のみを調査
(*2)乱数データ 2^{20} で調査した予想値

表 4 TKG のアクティブな T_n 関数が 1 個の場合

通番	丸め差分値					独立な部品関数	TKG の確率
	Tu 後	Tv 後	Tw 後	Tx 後	Tz 後		
1	1xxx xxxx	1xxx 0xxx	00xx 0xxx	00xx 00xx	00xx 00xx	Tu, m5(1xxx→00xx)	$2^{-7.000} \times 2^{-5.710}$
2	0xxx xxxx	1xxx 1xxx	00xx 1xxx	00xx 00xx	00xx 00xx	Tv, m5(1xxx→00xx)	$2^{-7.000} \times 2^{-5.710}$
3	0xxx xxxx	0xxx 0xxx	10xx 1xxx	10xx 00xx	10xx 00xx	Tw, m6(1xxx→00xx)	$2^{-7.000} \times 2^{-4.994}$
4	0xxx xxxx	0xxx 0xxx	01xx 0xxx	10xx 10xx	10xx 10xx	Tx, m5(0xxx→01xx)	$2^{-7.000} \times 2^{-5.371}$
5	0xxx xxxx	0xxx 0xxx	01xx 0xxx	01xx 01xx	01xx 10xx	Ty, m6(0xxx→01xx)	$2^{-7.000} \times 2^{-4.995}$
6	0xxx xxxx	0xxx 0xxx	00xx 0xxx	00xx 01xx	11xx 01xx	Tz, m6(0xxx→01xx)	$2^{-7.000} \times 2^{-4.995}$