CIPHERUNICORN-E に対する
安全性について

2001 年 12 月 14 日

日本電信電話株式会社

神田 雅透

CIPHERUNICORN-Eに対する安全性について

日本電信電話株式会社

December 14, 2001

Abstract

本稿では，CIPHERUNICORN-E に対する安全性，特に差分特性確率および線形特性確率について，設計者の立場から評価を実施した。その結果，差分解読法，線形解読法のどちらにおいても，仕様である 16 段について，攻撃が成功することはほぼありえないとの結論に達した。

1 安全性検証に関する考え方

本稿では，CIPHERUNICORN-E に対する差分解読法および線形解読法に対する安全性を検証する。今回は設計者の立場より評価を行うものとし，仕様である 16 段が攻撃可能かどうかについてのみ検討した。つまり，攻撃可能段数を検討したものではないことに注意されたい。

CIPHERUNICORN-E の検討すべき特徴点としては，

- 副鍵が作用しない連続する 4 つの T 関数の効果
- 一時鍵生成部の効果
- L 関数の効果

が挙げられる。もしも攻撃可能段数を求めようとするならば，これらの効果について厳密な調査を実施する必要がある。しかし，暗号仕様が安全であるか否かだけを検証するのであれば，必ずしも厳密に評価する必要はなく，適切な考察の下での安全性上界を調べればよい。この方針の下，安全性評価上，有効だと考える以下のような考察を行った。

副鍵が作用しない連続する 4 つの T 関数の効果

T 関数は 4 つの 8×8 ビット s-box を使っているものの，入力は 8 ビットだけであるため，8×32 ビット s-box と考えるほうが適当である。また，副鍵が作用しない連続する T 関数ではそれぞれの関数での差分確率（線形確率）の単純な積として表現することは適当ではなく，32×32 ビットの大きな s-box 一つとして考えるほうが望ましい。なぜならば，副鍵が作用しないと，T 関数間でのデータ従属性が強くなり，いわゆる “active s-box による評価” が前提とするような確率的な動作を起こさなくなるためである。

これを傍証するために，以下のような一つの簡単な実験を行った。

実験内容 16 ビットを入力サイズとするミニ・ラウンド関数を考え，その中の T(0) 関数から T(3) 関数までの部分を評価対象とする。まず，4 ビット s-box を 4 つ用意し，オリジナルの T 関数と同じ順序の配置にしたがったミニ T 関数（T(0) - T(3)) を構成する。そして，ミニ T 関数をオリジナルの配置と同様におき，平文全数探索により T(0) 関数への入力差分と T(3) 関数の出力差分の差分分布（最大差分確率）を調べる。同様に，最大線形確率についても調査する。

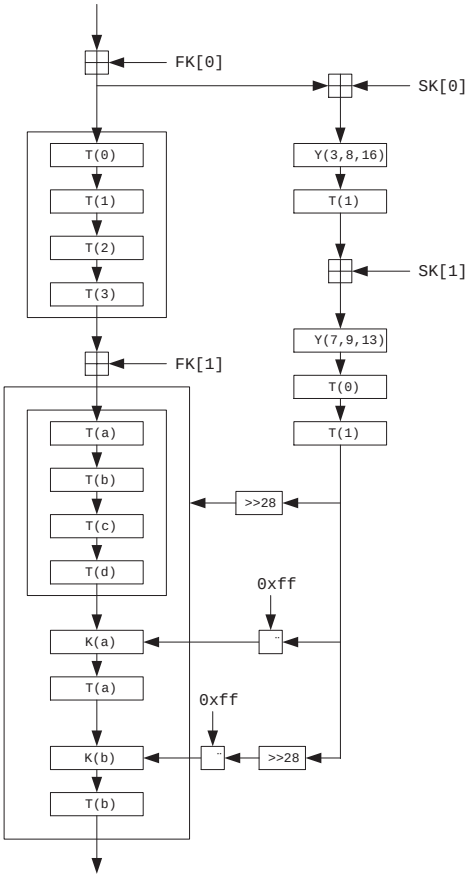

Figure 1: CIPHERUNICORN-E のラウンド関数

s-box s-box の構成では，$S_i(x) = \{(x+c)^{-1} \bmod g\} + d$ とし，最大差分確率が 2^{-2} となるように選んだ。オリジナルの s-box では最大差分確率，最大線形確率のほかにも考慮している点があるが，今回は副鍵が作用しない複数の T 関数をどのように評価すべきであるかの基礎データを得ることが目的であるので，c と d に関してはランダムに決めた。なお，$g = 0x19$ は既約多項式 $x^4 + x^3 + 1$ を表す。

s-box	g	c	d	備考
S0	0x19	0xb	0xf	
S1	0x13	0x7	0xc	
S2	0x19	0x5	0x6	出力 2 ビットローテーション
S3	0x1f	0xd	0x1	

本実験の結果は以下のとおりである。

- T(0) 関数から T(3) 関数までを 16×16 ビットの s-box として考えた場合，最大差分確率が 2^{-3} となるもの最大であった。ちなみに，全入力差分のパターン（2^{16}-1 通り）ごとの最大差分確率を調べた場合，以下のような分布が見られた。

確率	パターン数	確率	パターン数	確率	パターン数
2^{-9}	7072	2^{-6}	26990	2^{-5}	46
$2^{-8.83}$	21621	$2^{-5.98}$	473	2^{-3}	360
$2^{-8.68}$	1648	$2^{-5.96}$	7		
$2^{-8.54}$	40	$2^{-5.83}$	175		
2^{-8}	6976	$2^{-5.81}$	2		
$2^{-7.91}$	104	$2^{-5.68}$	1		
$2^{-7.83}$	3				
$2^{-7.42}$	17				

- T(0) 関数から T(3) 関数までを 16×16 ビットの s-box として考えた場合，最大線形確率が $2^{-3.66}$ となるものが見つかった。（実験途中）

本実験での結果は，s-box の構成を変えればパターン数（分布割合）などに若干の変動がおきる可能性が高いものの，大きな “傾向” としては変わらないものと考えられる。特に，最大差分確率や線形確率の最大値に関していえば，8×8 ビット s-box 単体での最大差分確率や最大線形確率とそれほど大きくは変わらないものが存在することはほぼ間違いがないと考える。

また，自己評価書図 3.3 の場合と同じ入出力パターンとなるケース（T(0) 関数から T(3) 関数のうち T(2) のみが active となっている状態）での最大差分確率の最大値は 2^{-3} ($\leq 2^{-2}$) となる。一方，図 3.2 の場合と同じ入出力パターンとなるケース（T(0) 関数から T(3) 関数のすべてが active となっている状態）での最大線形確率の最大値は $2^{-5.66}$ ($\geq (2^{-2})^4$) となる。

以上の結果から類推するに，副鍵が作用しない連続する 4 つの T 関数の効果はいくつの s-box (T 関数) が active s-box (active T-function) になっているかという評価からでは簡単に確率を見積もることはできないといえよう。むしろ，4 つの T 関数を一まとめとして，8×8 ビット s-box 単体での最大差分確率や最大線形確率並であると評価することが適当と判断する。つまり，2^{-6} を利用するということである。ちなみに，自己評価書による結果では，連続する 4 つの T 関数において，active T-function が 1 つである最大差分確率については 2^{-6}，active T-function が 4 つである最大線形確率については $2^{-17.68}$ で評価している。

なお，T(a) から T(d) までの連続する 4 つの T 関数についても同様のことがいえることにも注意されたい。

一時鍵生成部の効果

差分解読法や線形解読法において攻撃に有効なパス探索を行う場合，一時鍵生成部の効果をどのように見積もるかを検討する必要があるが，厳密に評価をすることはかなり難しい作業を伴うものと考えられる。そこで，本稿では，一時鍵生成部のもっとも簡単な近似として，以下のような近似を行うものとした。

- 一時鍵生成部で作られるデータは一様なランダムデータとなる。
- K 関数での一時鍵挿入による差分確率，線形確率への影響はない（確率 1 で成立する）ものとする。
- K 関数以降の T 関数（T(a) と T(b)) は non-active になっているものと仮定する。

言い換えれば，一時鍵生成部のデータが差分確率や線形確率に影響を与えるのは構造決定の部分だけであるということができる。この仮定により，一時鍵生成部に関する部分のデータの流れは考慮対象外とすることができ，今後は本流部のみについて検討すればよくなる。なお，この仮定は，設計者側に不利な（安全サイドに倒した）評価を与えることになる可能性が高いと思われる。

L 関数の効果

L 関数は副鍵依存の線形変換であり，ビット単位の演算として行われる。特に，ビット論理積のみを利用しているため，次のような性質がある。このため，L^8 関数の入力データ（同じビット位置の X_L と X_R のデータ）が高い確率で予測できるような攻撃が見つかった場合，L 関数の特性から副鍵 2 ビットが一意に求まる。

LK[0]	LK[1]	Z_L	Z_R
0	0	X_L	X_R
0	1	$X_L \oplus X_R$	X_R
1	0	X_L	$X_L \oplus X_R$
1	1	X_R	X_L

また，L 関数は二分割された左右のデータをまたがる演算であるため，段数を減少させる方向へ作用するような弱鍵の存在も理論的には考えられる。だが，L 関数がビット演算であることを考えれば，段数を劇的に減少をさせるような弱鍵が発生するのは，自己評価書でも述べているように，極めて低い確率であると考えてよい。それよりは，本来であれば高い確率での 2 段繰り返し表現にならないような差分特性や線形近似にもかかわらず，弱鍵の L 関数の影響を受けることによって高い確率での 2 段繰り返し表現になってしまう可能性のほうが現実的な脅威といえよう。

つまり，CIPHERUNICORN-E での考えるべき差分特性や線形近似とは，基本的に高い確率を有する 2 段表現（必ずしも繰り返し表現である必要はない）ということになる。

2 差分特性確率について

前章での考察で示したとおり，CIPHERUNICORN-E の差分解読法に対する安全性評価では 2 段表現における差分特性確率が重要な指標になると考えられる。

ここで，ラウンド関数の本流部に着目してみると，T(0) 関数から T(d) 関数（K(a) 関数の前）までは全単射の構成をしている。このことは，T(0) 関数から T(3) 関数の中に active T-function が存在するのであれば，かならず T(a) 関数から T(d) 関数の中にも active T-function が存在することを意味する。したがって，前章での考察で示したように 4 つの連続する T 関数での最大差分確率の上界を 2^{-6} とおくと，T(0) 関数から T(d) 関数までの最大差分確率の上界は少なくとも $(2^{-6})^2 = 2^{-12}$ で与えられることになる。

この他に，差分解読法を効果的に作用させることを考慮すれば，現実的には 2 つのデータに関してラウンド関数の構造を一致させる必要がある。したがって，一時鍵生成部からの影響を一様なランダムデータによるものと仮定すると，少なくとも 2^{-4} の確率変動要因があると考えられる。

これらの考察結果を合わせると，ラウンド関数での最大差分 (特性) 確率の上界値は 2^{-16} とするのが相当であると判断する。したがって，CIPHERUNICORN-E での最大差分特性確率の上界値は，2 段表現で表されることを考慮すると，以下のように示される。

Table 1: CIPERUNICORN-E の差分特性確率の上界

ラウンド数	1	2	3	4	5	6	7	8
上界値	1	2^{-16}	2^{-16}	2^{-32}	2^{-32}	2^{-48}	2^{-48}	2^{-64}

ラウンド数	9	10	11	12	13	14	15	16
上界値	2^{-64}	2^{-80}	2^{-80}	2^{-96}	2^{-96}	2^{-112}	2^{-112}	2^{-128}

安全性閾値を 2^{-64} とすると，10 段あれば差分解読法に有効な差分特性は存在しないということがいえる。また，実際に 9 段の差分特性が存在したとしても，CIPHERUNICORN-E の仕様である 16 段を解読するためには，さらに 7 段のラウンド関数と 4 つの L 関数における副鍵（の一部）

を推定する，すなわち 7 段消去型攻撃に相当する解読を行う必要がある。しかしながら，n 段消去型攻撃が一般に想定されるのは,（ラウンド関数の構成にもよるが）せいぜい 4 (=2+2) 段程度までであることを考えれば，7 段消去型攻撃というのは非常に考えにくい。特に，CIPHERUNICORN-E のラウンド関数の構成を見れば，そのような攻撃はほとんど不可能であるといってもいいであろう。

以上の結果，CIPHERUNICORN-E について，仕様である 16 段において差分解読法が成功することはほぼありえないと考える。なお，提案者は，ラウンド関数での最大差分 (特性) 確率の上界値を 2^{-12} として安全性評価を行っている。この自己評価は，安全性評価の上界という立場からは，何ら今回の結果と矛盾するものではない。もし，提案者の自己評価を採用したとしても，12 段以上の有効な差分特性がないことを示すことができるので，同様に，16 段の CIPEHRUNICORN-E が差分解読法に対して事実上安全であることが導かれる。

最後に，今回の結果，自己評価とも，安全性評価の上界によるものであるので，実際にはこれらの評価結果よりも安全である可能性もあることを付け加えておく。

3 線形特性確率について

線形解読法に対する安全性についても，前章の差分解読法のケースと全く同様の議論が行える。すなわち，線形マスク値の伝播に関して，ラウンド関数の本流部に着目してみると，ラウンド関数の入力側の分岐点（FK[0] の加算直後に一時鍵生成部への分岐がおきる所）まで，T 関数で構成される部分は全単射の構成をしている。つまり，差分解読法のときと同様，T(0) 関数から T(3) 関数の中に active T-function が存在するのであれば，かならず T(a) 関数から T(d) 関数の中にも active T-function が存在することを意味する。したがって，1 章での考察で示したように 4 つの連続する T 関数での最大線形確率の上界を 2^{-6} とおくと，T(0) 関数から最後の T(b) 関数までの最大線形確率の上界は少なくとも $(2^{-6})^2 = 2^{-12}$ で与えられることになる。

この他に，線形解読法を効果的に作用させることを考慮すれば，現実的にはラウンド関数の構造を決定しておく必要があり，一時鍵生成部からの影響を一様なランダムデータによるものと仮定すると，少なくとも 2^{-4} の確率変動要因があると考えられる。

これらの考察結果を合わせると，ラウンド関数での最大線形 (特性) 確率の上界値は，自己評価書での $2^{-63.90}$ ではなく，2^{-16} とするのが相当であると判断する。

これ以降の議論は，全く差分解読法の場合と同様であり，その結果，16 段の CIPEHRUNICORN-E が線形解読法に対して安全であることが導かれる。

4 おわりに

本稿では，CIPHERUNICORN-E に対する安全性，特に差分特性確率および線形特性確率について，設計者の立場から評価を実施した。その結果，ラウンド関数における最大差分（特性）確率および最大線形（特性）確率の上界を 2^{-16} と見積もることが適当であることを示した。

また，この見積もりを根拠に，10 段あれば差分解読法に有効な差分特性，線形解読法に有効な線形近似とも存在しないことが導かれる。したがって，最終的に CIPHERUNICORN-E の仕様である 16 段について，差分解読法や線形解読法によって攻撃が成功することはほぼありえず，それらの解読法に対して安全であるとの結論に達した。

以上