共通ブロック暗号 CIPHERUNICORN-E の
安全性に関する詳細調査報告書

2001 年度

東京理科大学

金子 敏信

共通鍵ブロック暗号CIPHERUNICORN-Eの安全性に関する詳細調査報告

概要

本資料は共通鍵ブロック暗号 CIPHERUNICORN-E の安全性に関する詳細報告書である。本暗号の差分攻撃及び線形攻撃に対する耐性について詳細に検討した結果、CIPHERUNICORN-E の安全性について解読に結びつくような問題点は導かれなかった。それぞれの攻撃法に対する安全性に関する結果は、以下の様にまとめられる。

差分攻撃 :
提案者による Y 関数近似よりもより攻撃者に有利な近似を施した Y' 関数を用いて探索した。その結果、最大差分確率は 2^{-98} となり、自己評価書とは異なる値を得たが 64 ビットブロック暗号に期待される確率を下回っているため差分攻撃に対する安全性という面では問題はない。

線形攻撃 :
提案者による Y 関数近似よりもより攻撃者に有利な近似を施した Y' 関数を用いて探索した。その結果、最大差分確率は $2^{-191.163}$ となり、自己評価書とは異なる値を得たが 64 ビットブロック暗号に期待される確率を下回っているため差分攻撃に対する安全性という面では問題はない。

1　はじめに

CRYPTREC Report2000 において CIPHERUNICORN-E は

> 「安全性について、今のところ問題は見つかっていない。複雑な構造のため、正確な評価が難しく、継続的な評価が必要である。」

とされている [3]。そこで特に問題とされている差分解読および線形解読に対する耐性を検討した。第 2 節では自己評価書の記述に対して指摘された問題点を列挙し、その問題点に対する対処について述べる。第 3 節では差分解読についての再検討を行う。第 4 節では線形解読についての再検討を行う。第 5 節ではそれぞれの検討の結果をまとめ結論として示す。

2　自己評価書の問題点と本報告書の評価手法

2.1　自己評価書における問題点

CIPHERUNICORN-E は F 関数内部において 32bit 算術加算を用いており、従来の方法で差分確率及び線形確率を導出することは困難であることから、自己評価書において提案者が F 関数を近似したラウンド関数、mF 関数を定義し安全性評価を行っている。しかしながらその近似について

- F 関数の近似の妥当性
- T 関数の最大差分確率あるいは最大線形確率
- 連続した T 関数の独立性
- L 関数を考慮した評価

が評価上の問題点として指摘されている [4]。ここでは各問題点について考察を行う。

2.2　解析に当たっての近似とその妥当性

本暗号は F 関数内部の演算において 32 ビット鍵算術加算及び 32 ビットシフト加算 (Y 関数)、さらにデータ依存の換字テーブル等を用いていることから、従来から知られている手法では厳密に差分確率や線形確率を求めることは、計算量的に困難である。設計者による安全性解析では、F 関数に対して次の様な変更を行った関数 mF を定義し、mF 関数を用いた Feistel 型ブロック暗号の差分攻撃に対する安全性を評価している。

1. 算術加算は排他的論理和に置き換える。
2. Y 関数については、32 ビットデータの上位 1 バイトへ入力ビットを集める処理、すなわち下位 3 バイトの排他的論理和を上位 1 バイトへ排他的論理和する処理とする。

上記の様に変更された暗号の強度評価結果を根拠として、もとの暗号の安全性を示そうとする場合、暗号の安全性が増す様な近似操作や、攻撃者に不利となる仮定が必要となってはならない。

2.2.1 算術加算の近似の妥当性

算術加算における最大差分確率、及び最大線形確率は 1 である。また排他的論理和における最大差分確率及び最大線形確率は 1 である。従って少なくともこの近似は差分確率及び線形確率を減少させる変形ではない。以上から提案者の用いた近似は妥当であると考える。

2.2.2 Y 関数の近似の妥当性

Y 関数の近似には疑問点が残る。自己評価書には Y 関数の近似をどのように選んでだのかと言う点には触れられていない。提案者の用いた Y 関数近似は入力差分値及びマスク値に対し、出力差分値及びマスク値が限定性を持ったものとなっている。したがって実際の Y 関数においては近似した Y 関数では示せない差分値もしくはマスク値が存在する可能性を捨てきれない。

2.3 本報告所の Y 関数の取り扱い

前項における疑問点を解決するために本報告所のパス探索においては mF 関数内の Y 関数を以下のように取り扱う。

1. Y 関数は任意の入力差分値及びマスク値に対し、攻撃者に有利となる任意の出力差分値及びマスク値が存在する関数であるとする。

この取り扱いはもっとも攻撃者に有利な仮定であることを根拠とする。

この Y' 関数で近似して Truncated vector 探索で最大差分特性確率および最大線形特性確率を求め評価する。

2.4 T 関数における連結した換字テーブル

2.4.1 最大差分確率の妥当性

自己評価書において、提案者は連結した換字テーブルの最大差分確率を一つの換字テーブルの差分確率と等しく 2^{-6} としている。しかし、実際は T 関数は 4 つの S 関数の並列関数であるため、8bit 入力、32bit 出力の関数とみなした場合必ずしも差分確率は 2^{-6} とならない。差分確率の定義

$$DP_f(\Delta x, \Delta y) = \frac{\#\{x \in \{0,1\}^n | f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n}$$

に対して $f(x) = (s_0(x)||s_1(x)||s_2(x)||s_3(x))$ として差分確率を計算したならば、最大差分確率は 2^{-7} となる。本稿における Truncated vector 探索における差分特性確率の評価はこの最大差分確率を用いて行う。

2.4.2 最大線形確率の妥当性

自己評価書において、提案者は連結した換字テーブルの最大線形確率を求めているが、S_0 から S_3 までの全ての換字テーブルに等しい値が入力されているにもかかわらず、S_3 は独立しているものと考え、連結した換字テーブルの最大線形確率を求めている。しかし、全ての換字テーブルを並列であると見なして、S_0 から S_3 までの全ての連結パターンの最大線形確率を求めると違う結果となる。自己評価書との対比を表 1,2 に示す。例えば、図 2 のように入力マスク $\neq 0$ で、S_0、S_2、S_3 にマスクが入力した場合、自己評価書における T 関数の最大線形確率 MP_T は、

$$\begin{aligned} MP_T &= \{(S_0 \parallel S_2) \text{で入力マスク} \neq 0\} \times \{S_3 \text{で入力マスク} \neq 0\} \\ &= 2^{-3.66} \times 2^{-6} \\ &= 2^{-9.66} \end{aligned}$$

となるが、我々が求めた T 関数の最大線形確率 MP'_T は、

$$\begin{aligned} MP'_T &= \{(S_0 \parallel S_2 \parallel S_3) \text{で入力マスク} \neq 0\} \\ &= 2^{-2.712} \end{aligned}$$

となり、T 関数ひとつでも異なる。本稿における Truncated vector 探索における線形特性確率の評価はこの最大線形確率を用いて行う。

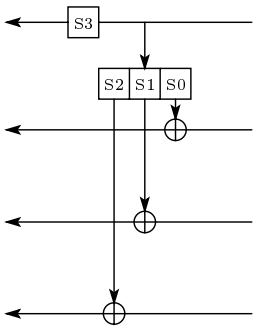

図 1: T(0) 関数

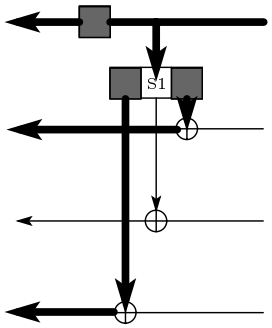

図 2: マスクが S_0,S_2,S_3 に入力した場合

	入力マスク $= 0$ の場合	入力マスク $\neq 0$ の場合
$S_0 \| S_1$	$2^{-3.83}$	$2^{-3.08}$
$S_0 \| S_2$	$2^{-3.66}$	$2^{-3.08}$
$S_1 \| S_2$	$2^{-3.50}$	$2^{-3.08}$
$S_0 \| S_1 \| S_2$	$2^{-3.22}$	$2^{-2.60}$

表 1: 連結した換字テーブルの最大線形確率（自己評価書）

	入力マスク $= 0$ の場合	入力マスク $\neq 0$ の場合
$S_0 \| S_1$	$2^{-3.825}$	$2^{-3.081}$
$S_0 \| S_2$	$2^{-3.660}$	$2^{-3.081}$
$S_0 \| S_3$	$2^{-3.504}$	$2^{-3.081}$
$S_1 \| S_2$	$2^{-3.504}$	$2^{-3.081}$
$S_1 \| S_3$	$2^{-3.825}$	$2^{-3.081}$
$S_2 \| S_3$	$2^{-3.660}$	$2^{-3.215}$
$S_0 \| S_1 \| S_2$	$2^{-3.215}$	$2^{-2.599}$
$S_0 \| S_1 \| S_3$	$2^{-3.215}$	$2^{-2.599}$
$S_0 \| S_2 \| S_3$	$2^{-3.215}$	$2^{-2.712}$
$S_1 \| S_2 \| S_3$	$2^{-3.081}$	$2^{-2.712}$
$S_0 \| S_1 \| S_2 \| S_3$	$2^{-2.712}$	$2^{-2.385}$

表 2: 連結した換字テーブルの最大線形確率（新たに算出）

2.5　mF 関数中の T 関数の独立性に関する考察

提案者は最大差分特性確率または最大線形特性確率を求める際に、mF 関数中のアクティブな T 関数をカウントし、最大差分確率または最大線形確率の乗算によって mF 関数の最大差分特性確率または最大線形特性確率を導出している。しかし、アクティブな T 関数が独立であるかという議論が必要である。

この疑問点の考察のため mF 関数を図 3 のように等価変形する。図中の BLOCK1 の部分について、T 関数はそれぞれバイトごとに独立な拡大鍵 FK[0] が入力されるため、すべての T 関数は独立となる。BLOCK2 の部分については BLOCK1 と同様に拡大鍵 FK[1] によって、T 関数はすべて独立となる。BLOCK3 の部分は k 関数の直前に拡大鍵 SK[0],SK[1] の下位 2 バイトを移動できる。K 関数は T 関数の内で換字テーブルを通過するバイトへ、一次鍵生成部のデータを排他的論理和する関数であることから、BLOCK3 の T 関数はすべて独立であることがわかる。また、BLOCK4 の T 関数は独立な拡大鍵 SK[0]、SK[1] の上位 2 バイトが排他的倫理和されていることから、すべて独立であることがわかる。

以上の考察から mF 関数中のすべての T 関数は独立となることがわかる。よって、少なくとも mF 関数の差分特性確率の導出法については、提案者の用いた評価法は妥当であると考える。

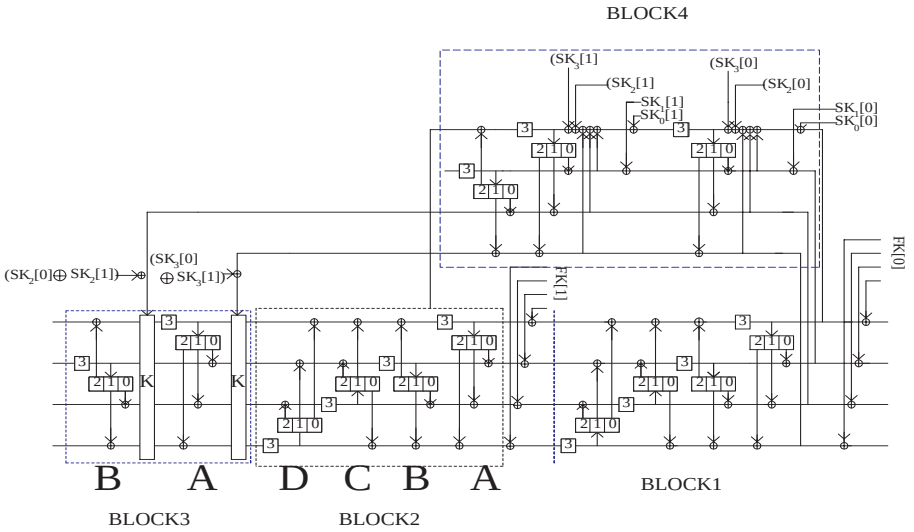

図 3: 拡大鍵を移動した mF 関数

2.6　L 関数を考慮した場合の最大差分特性確率、最大線形特性確率

自己評価書においてラウンド数 R における最大差分特性確率、最大線形特性確率の計算方法は、

(1) ラウンド関数の出力差分 $\Delta y = 0$、ラウンド関数の入力マスク $\Gamma x = 0$ の時、ラウンド関数最大差分確率を dp とし、ラウンド関数最大線形確率を lp とすると、

$$DCP_{max} \leq dp^{R/2} \tag{1}$$
$$LCP_{max} \leq lp^{R/2} \tag{2}$$

となる。
(2) ラウンド関数の出力差分 $\Delta y \neq 0$、ラウンド関数の入力マスク $\Gamma x \neq 0$ の時、ラウンド関数最大差分確率を dq とし、ラウンド関数最大線形確率を lq とすると、

$$DCP_{max} \leq dq^{2R/3} \tag{3}$$
$$LCP_{max} \leq lq^{2R/3} \tag{4}$$

となる。

しかし、L 関数を考慮した場合、図 4 のような差分値およびマスク値の伝搬が考えられる。この場合、ラウンド関数の出力差分 $\Delta y \neq 0$、ラウンド関数の入力マスク $\Gamma x \neq 0$ の時、ラウンド関数最大差分確率を dq とし、ラウンド関数最大線形確率を lq とすると、

$$DCP_{max} \leq dq^{R/2} \tag{5}$$
$$LCP_{max} \leq lq^{R/2} \tag{6}$$

と計算できる。L 関数の内部で図 4 のようなパスが存在することは確認済みである。

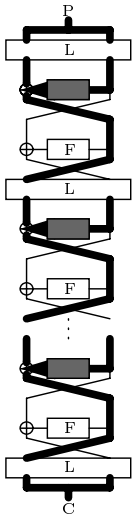

図 4: 最大差分特性確率、最大線形特性確率をあたえる差分値および、マスク値の通り方

3　差分攻撃

3.1　Truncated vector 探索による、mF 関数の差分特性確率

上記の考察より Y 関数をブラックボックスとして見なした F 関数を採用する。mF 関数はすべての処理がバイト単位となるため、差分値をバイト単位の 0,1 ですべてのパターンを代入して通過した S-box を調べ、mF 関数の最大差分特性確率を見積もった。Sh テーブルによって構造が変化する部分については全てのパターンを場合分けして調査した。結果、提案者が主張するパス以外にも T 関数を 2 回通過するパスが複数存在した。図 5 に提案者が主張するパスと同じパスを、図 6 に探索の結果判明したパスを示す。いずれの場合も出力差分は 0 である。出力差分値が 0 の場合、ラウンド関数の差分特性確率を p とした時、R 段での差分特性確率は式 (1) と計算できる。したがって 16 段での mF 関数の最大差分特性確率 DCP は、

$$DCP = 2^{-14\times 15/2} = 2^{-98} \tag{7}$$

となり、2.3.1 小節で述べた T 関数 1 つの最大差分確率の分だけ確率は下がっている。

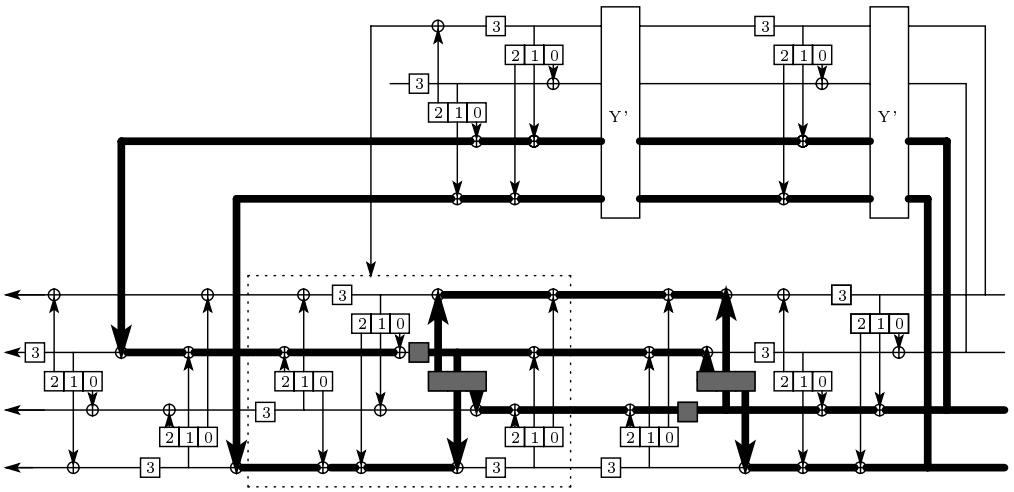

図 5: ラウンド数 R における最大差分特性確率が最大になるケース（自己評価書と同じパス）

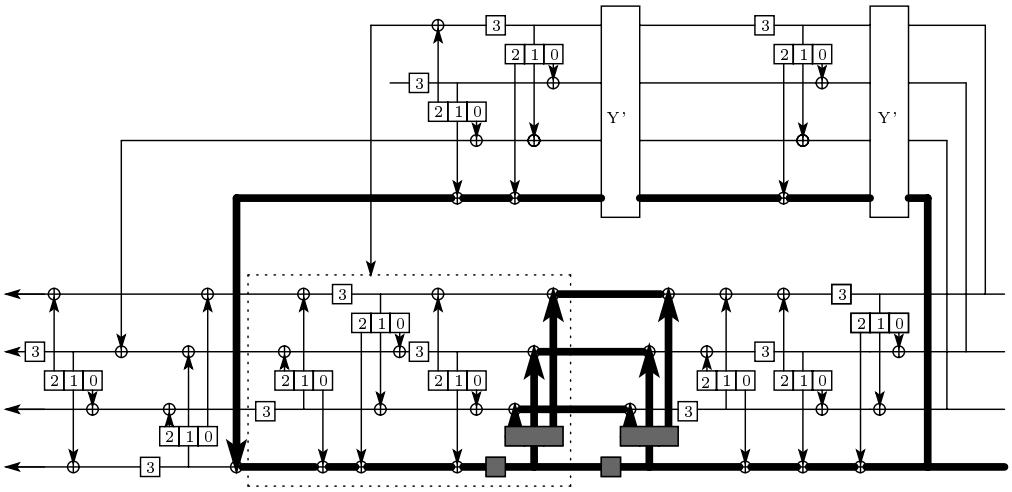

図 6: ラウンド数 R における最大差分特性確率が最大になるケース（新たに発見）

3.2 耐差分攻撃についてのまとめ

探索結果により自己評価書と異なる最大差分特性確率を得たが、CIPHERUNICORN-E の段数が 16 段であることを考慮すれば、差分解読法に対して安全であると考えてよい。

4 線形攻撃

4.1 Truncated vector 探索による mF 関数の最大線形特性確率

差分解読法と同様に、自己評価書では mF 関数において Truncated vector 探索を利用して、ラウンド関数の最大線形特性確率が $2^{-63.90}$、15 段での最大線形特性確率の上界が $2^{-447.30}$ であると評価している。自己評価書におけるラウンド数が R である場合の、最大線形特性確率が最大になるケースを図 7 に示す。

今回我々は、2.6 節で述べた L 関数の効果を考慮した上で自己評価書と同じ Truncated vector 探索を利用して最大線形特性確率が最も大きくなるパスを探した。その際、T 関数における換字テーブルに入力されるマスク値が 0 であるか否かで、表 2 の様に確率が変わることを配慮している。mF 関数は全ての処理がバイト単位になるので、線形マスク値をバイトごとの 0,1 で全てのパターンを代入して、通過した換字テーブルを調べ、Sh テーブルで構造が変化する処理については全てのパターンを場合わけして調査した。ラウンド数 R における最大線形特性確率が最も大きくなるケースを図 8 に示す。ラウンド関数最大特性線形確率を求めると、

$$\begin{aligned} LP_{mF} &= 2^{-3.081\times 1} \times 2^{-3.081\times 2} \times 2^{-3.215\times 1} \times 2^{-2.599\times 1} \times 2^{2.712\times 1} \times 2^{-2.385\times 4} \\ &= 2^{-27.309} \end{aligned}$$

となる。図 8 では入力マスク値 $\neq 0$ であるが 2.6 節で述べた L 関数の効果を考えると、16 段構成において最終段 F 関数出力を推定するための最大線形特性確率 LCP は、

$$\begin{aligned} LCP &= {LP_{mF}}^{(15/2)} \\ &= 2^{-191.163} \end{aligned}$$

となる。なお，図 8 のマスクパターンが図 4 の様に L 関数を通過することは確認ずみである。自己評価書との比較を表 3 に示す。

	自己評価書	本報告書
ラウンド関数の最大特性線形確率	$2^{-63.90}$	$2^{-27.309}$
15 段での最大線形特性確率	$2^{-447.30}$	$2^{-191.163}$

表 3: 自己評価書との最大線形特性確率の比較

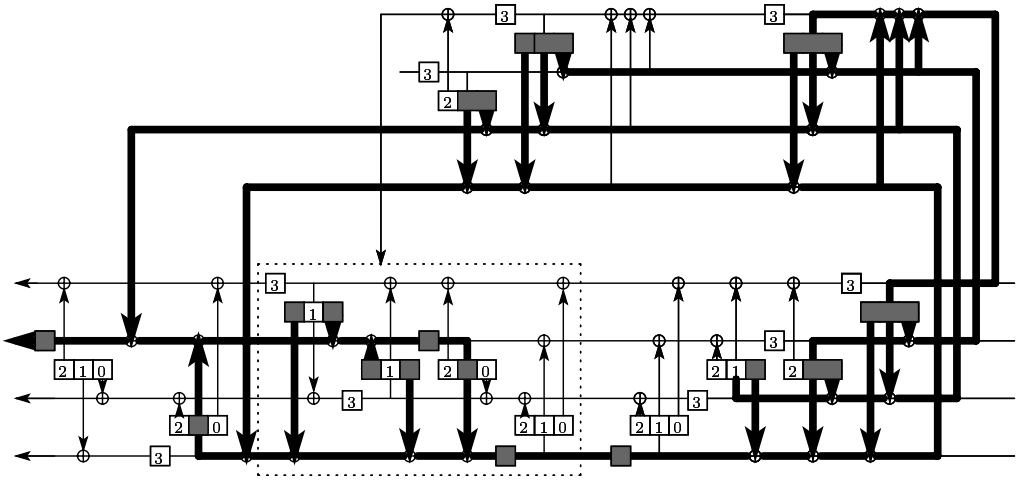

図 7: ラウンド数 R における最大線形特性確率が最大になるケース（自己評価書）

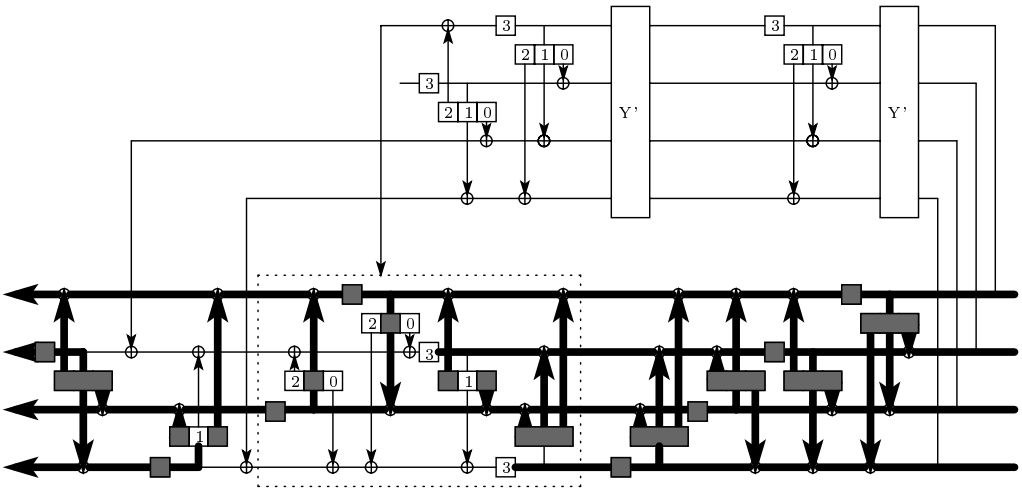

図 8: ラウンド数 R における最大線形特性確率が最大になるケース（新たに発見）

4.2 耐線形攻撃についてのまとめ

探索結果により自己評価書よりも大きい最大線形確率を得ることができたが、CIPHERUNICORN-E の段数が 16 段であることを考慮すれば、線形解読法に対して安全であると考えてよい。また、提案者による変形は線形攻撃に対して弱くなるような変形であり適切であるという結論に至った。

5　結論

適切な近似を施した CIPHERUNICORN-E は差分攻撃及び線形攻撃に対して耐性があった。提案された CIPHERUNICORN-E は差分攻撃及び線形攻撃に対して耐性があるという結論に至った。

参考文献

[1] 日本電気株式会社, ”暗号技術応募書/暗号技術仕様書 CIPHERUNICORN-E’

[2] 日本電気株式会社, ”暗号技術応募書/自己評価書 CIPHERUNICORN-E’

[3] ”暗号技術評価報告書 CRYPTREC Report 2000”, 情報処理振興事業協会セキュリティセンター

[4] ”共通鍵ブロック暗号 CIPHERUNICORN-E の安全性に関する詳細調査報告”, NTT コミュニケーションズ 供給