共通ブロック暗号 CIPHERUNICORN-A 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-A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-A 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。それぞれの攻撃法に対する安全性に関する結果は、以下のようにまとめられる。

差分攻撃　:
提案者による mF 関数近似は、安全側への評価であるという意味で、適切な近似であることを確認した。しかし、トランケート差分探索による最大差分特性確率は、$2^{-70.00}$ となり、128 ビットブロック暗号に期待される確率を上回る。よって、mF 関数を用いたトランケート差分評価では CIPHERUNICORN-A の差分攻撃に対する安全性を示すことはできなかった。

線形攻撃　:
提案者による mF 関数近似は、安全側への評価であるという意味で、適切な近似であることを確認した。また、最大線形特性確率は $2^{-149.52}$ となり、自己評価書とは異なる値を得たが、128 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線形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 Report 2000[3] において、CIPHERUNICORN-A 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。そのため本稿では、mF 関数近似の妥当性に着目し、CIPHERUNICORN-A の差分攻撃及び線形攻撃に対する再評価を実施した。

第 2 章では、自己評価書の問題点と本報告書の評価手法について述べる。第 3 章では、差分攻撃に対する耐性について述べ、第 4 章では線形攻撃に対する耐性について述べる。そして第 5 章で、上記の結果をまとめ結論として示す。

2　問題点の指摘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-A は F 関数内部において 32 ビット鍵加算、32 ビット定数乗算等の算術演算を用いていることから、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ため、自己評価書において提案者は F 関数を近似した mF 関数を定義し、それを用いて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の妥当性
- 連接する T 関数の独立性

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い、本稿での評価手法を述べる。

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（図 1）内部の演算において 32 ビット鍵加算、32 ビット定数乗算等の算術演算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。提案者による安全性解析では、F 関数に対して次のような近似を行った関数 mF（図 2）を定義し、mF 関数を用いた Feistel 型ブロック暗号の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。

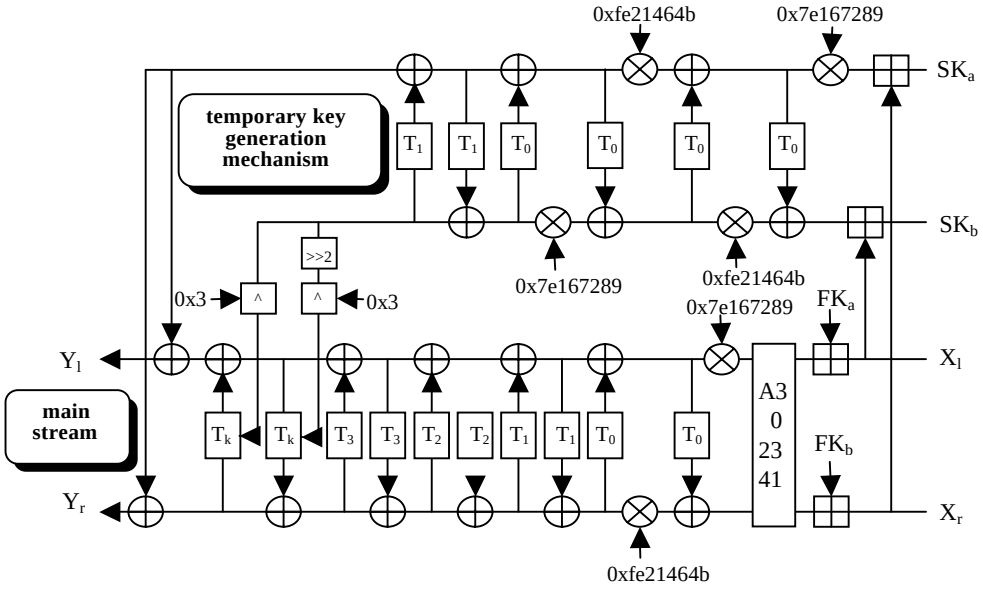


図 1: F 関数

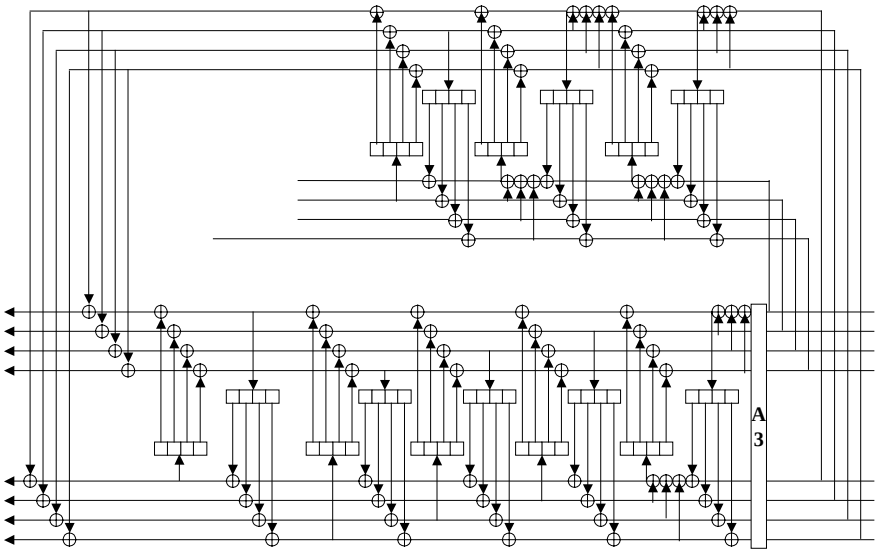


図 2: mF 関数

2. 定数乗算は、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バイトを上位１バイトへ排他的論理和する処理とする。
3. A3 関数は、ローテイトシフト数を考慮し、バイト全体に差分値が入る場合とそうでない場合の場合分けを行う。(差分攻撃時)
4. A3 関数は、A3 関数以降の本流処理と一時鍵生成部処理においてどちらも入力マスク値が $\neq 0$ の場合には、mF 関数への入力マスク値を 0 とする。(線形攻撃時)

さらに、変形した mF 関数ついて Truncated vector 探索を用いてアクティブとなる T 関数をカウントし、T 関数の各確率の乗算により最大差分特性確率、及び最大線形特性確率を求めている。

上記のように近似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ような変形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。このような立場から、上記の近似に関する正当性について考察する。

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。よって、本稿でも同じ近似を使用する。

2.2.2 定数乗算の近似の妥当性

定数乗算の出力は、実際には 4 バイトの経路を伝って 4ヶ所の T 関数入力に影響を及ぼす。これに対し、上位バイトへ入力ビットを集めるというこの近似は、処理直後の T 関数に値を波及させる効果を表している。この近似は排他的論理和の線形回路で表され、確率 1 で差分パス (線形パス) が伝わる形に評価しており、安全側の近似と考える。よって、本稿でも同じ近似を使用する。

2.2.3 差分攻撃時の A3 関数近似の妥当性

自己評価書の記述だけでは正確に意味を読みとることができなかったため、その妥当性は議論できない。本稿では、A3 関数の差分伝搬をビット単位で解析し、その差分伝播をトランケート差分で表現することとした。なお、A3 関数に繋がる暗号系の各部分においてはトランケート差分で接続を考えているため、全体として攻撃者にとって有利な仮定であると考える。

2.2.4 線形攻撃時の A3 関数近似の妥当性

A3 関数以降の本流処理と一時鍵生成部処理においてどちらも入力マスク値が $\neq 0$ の場合には、mF 関数への入力マスク値を 0 とするというのは、暗号系全体の特性確率を高めるという点で攻撃者にとって有利な仮定であると考える。本稿においては、A3 関数のトランケートパスの接続条件は、任意の接続が在り得るという条件設定で探索を行った。

2.3 T 関数における連結した換字テーブル

2.3.1 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、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 $f(x) = (s_0(x) \parallel s_1(x) \parallel s_2(x) \parallel s_3(x))$、つまり 8 ビット入力、32 ビット出力と見なして差分確率を計算したところ、最大差分確率は 2^{-7} となる。本稿における最大差分特性確率の計算は、この最大差分確率を用いて導出する。

2.3.2 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。本稿において再度計算を試みたところ、表 1 に示すとおり自己評価書と同様の値を得た。よって本稿における最大線形特性確率の計算は、この最大線形確率を用いて導出する。

2.4 T 関数の独立性

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欠けているため、これらの導出法には疑問が残る。この T 関数の独立性に関しては、後述する。

表 1: 換字テーブルの最大線形確率

連結状態	入力マスク＝0 の場合	入力マスク $\neq 0$ の場合
S_0	$2^{-6.000}$	$2^{-6.000}$
S_1	$2^{-6.000}$	$2^{-6.000}$
S_2	$2^{-6.000}$	$2^{-6.000}$
S_3	$2^{-6.000}$	$2^{-6.000}$
$S_0 \parallel S_1$	$2^{-3.825}$	$2^{-3.081}$
$S_0 \parallel S_2$	$2^{-3.660}$	$2^{-3.081}$
$S_0 \parallel S_3$	$2^{-3.504}$	$2^{-3.081}$
$S_1 \parallel S_2$	$2^{-3.504}$	$2^{-3.081}$
$S_1 \parallel S_3$	$2^{-3.825}$	$2^{-3.081}$
$S_2 \parallel S_3$	$2^{-3.660}$	$2^{-3.215}$
$S_0 \parallel S_1 \parallel S_2$	$2^{-3.215}$	$2^{-2.599}$
$S_0 \parallel S_1 \parallel S_3$	$2^{-3.215}$	$2^{-2.599}$
$S_0 \parallel S_2 \parallel S_3$	$2^{-3.215}$	$2^{-2.712}$
$S_1 \parallel S_2 \parallel S_3$	$2^{-3.081}$	$2^{-2.712}$
$S_0 \parallel S_1 \parallel S_2 \parallel S_3$	$2^{-2.712}$	$2^{-2.385}$

3 差分攻撃

3.1 Truncated vector 探索による mF 関数の最大差分特性確率

3.1.1 提案者による自己評価

提案者は、自己評価書において mF 関数に対し入力差分値をバイト単位の 0,1 として全パターンを代入し、通過した換字テーブルを調べた結果、図 3 のケースが差分特性確率 DP_{mF} を最大にし、その値は

$$DP_{mF} = (2^{-6.00})^2 = 2^{-12.00}$$

であると報告している。一般に、F 関数の差分近似の出力差分値が 0 でない場合、その差分確率を p としたときの R 段の差分確率は最大で $p^{2R/3}$ となることから、16 段において最終段の F 関数出力を推定するための最大差分特性確率 DCP は、

$$DCP = {DP_{mF}}^{15\times 2/3} = 2^{-120.00}$$

であると報告している。

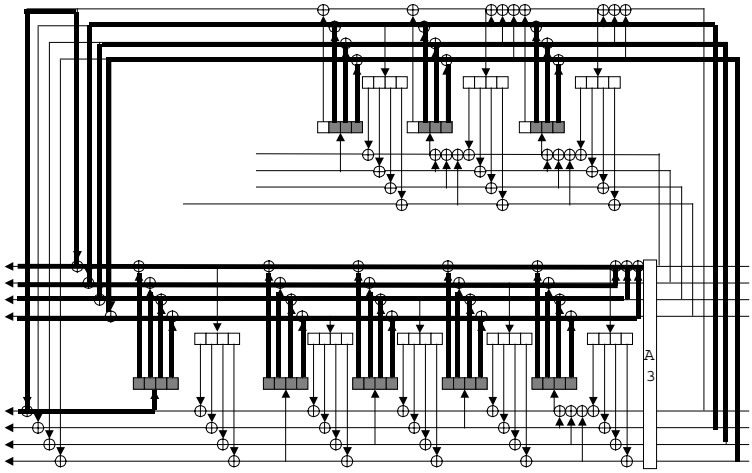


図 3: 差分特性確率が最大になるケース（自己評価書）

3.1.2 本報告での評価

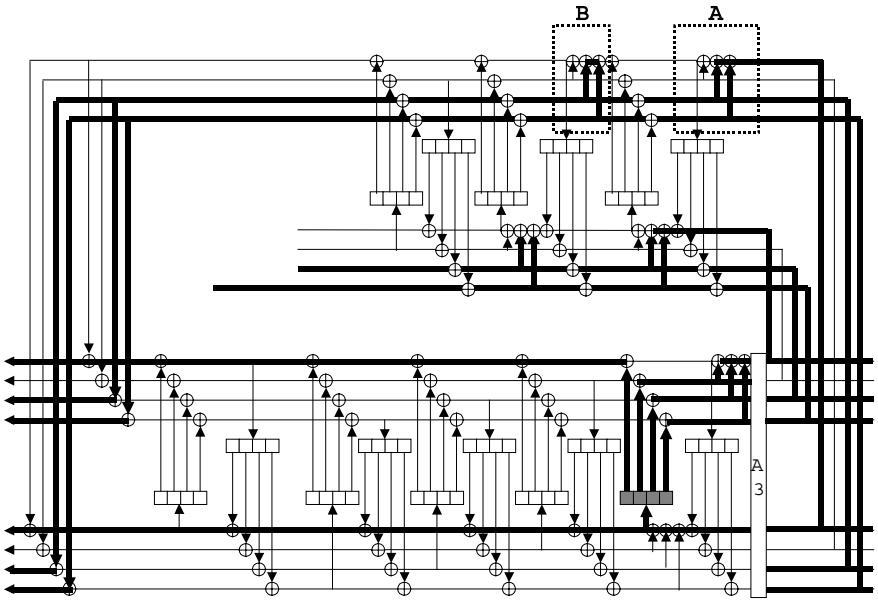
本稿では、mF 関数の入力側にバイト単位の 0,1 ですべてのパターンを代入し、その時 A3 関数の出力となりうるすべてのパターンを本流部 (下半分) に代入することにより通過した換字テーブルが最小となる入力パターンを探索した。この際、A3 関数は、差分伝搬をビット単位で解析し、その出力値をトランケート差分に置き換えることとした。ただし、ここでは通過した T 関数はそれぞれ独立であると仮定した。その結果、図 3 とは異なる最大差分特性確率が最大となるケースが存在した。新たに発見したケースを図 4(a) 及び図 5(a) に示す。また、A3 関数での入出力において、この差分伝播が存在し得ることを確認した。そのようなビット列の一例を図 4(b) 及び図 5(b) に示す。いずれのケースにおいても通過した T 関数は 1 つとなり、同様のトランケート入出力差分 (0xbb) が存在した。

このケースが新たに発見されたのは、排他的論理和演算の取扱いに起因することが一つの要因と考えられる。図 4(a) における 2 カ所の排他的論理和演算（A 及び B 部分）に着目し、抽出したものを図 6 に示す。A 及び B における入出力は、

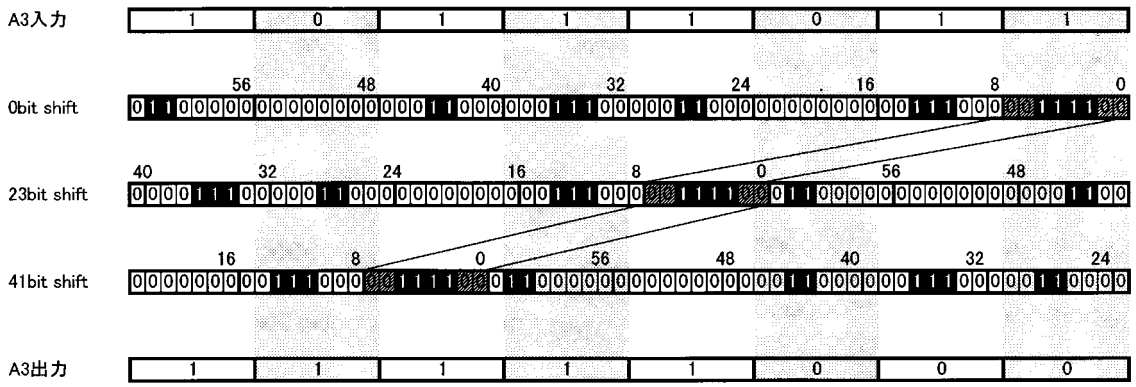
$$\begin{aligned} y_A &= x_3 \oplus x_1 \oplus x_0 \\ y_B &= x_1 \oplus x_0 \end{aligned}$$

と表せる。提案者は、どちらも単純な排他的論理和演算ととらえているため、$x_3 = x_1 = x_0 = 1$ のときには $y_A = y_B = 0$ はあり得ないとしている[1]。しかし、A においては定数乗算を近似した処理であるため、本稿では安全側への評価として $y_A = 0$ を満足する x_3 が存在するものとした。本近似で使われている定数乗算におけるパターンの伝播は図 7 である。これら全てのパターンに対し、実際に繋がることを

[1]提案者との議論により確認。

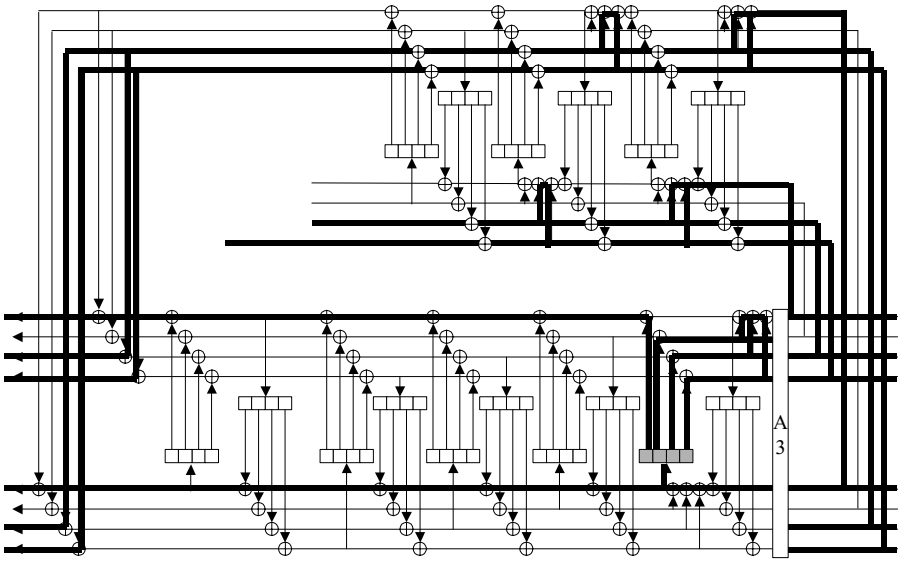


(a) ルート

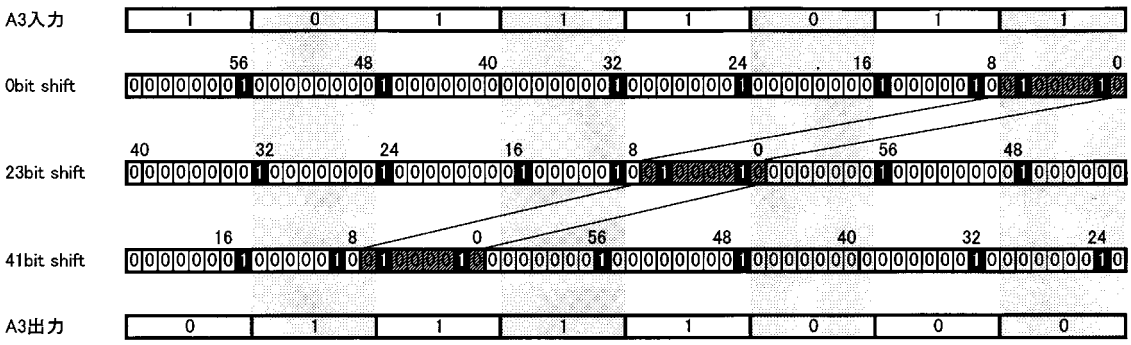


(b) A3 関数における入出力の例

図 4: 差分特性確率が最大になるケース１（新たに見出したもの）



(a) ルート



(b) A3 関数における入出力の例

図 5: 差分特性確率が最大になるケース２（新たに見出したもの）

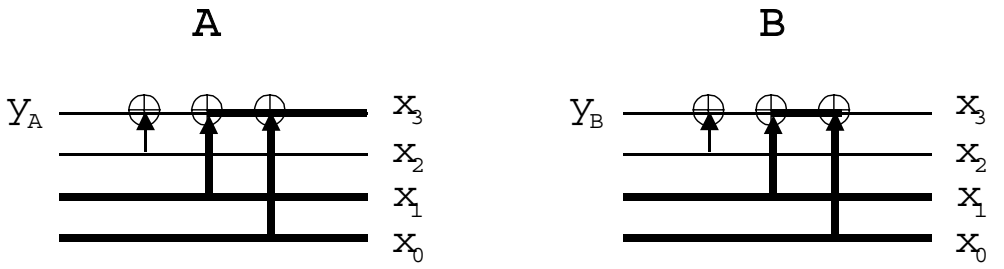


図 6: 排他的論理和演算

確認している。しかし、残念ながら計算量の関係で繋がる確率を見出すまでにはいたっていない。

図 4、5 のケースにおける mF 関数の最大差分特性確率は、４並列換字テーブルの差分確率の最大値が $2^{-7.00}$ であることから

$$DP_{mF} = (2^{-7.00})^1 = 2^{-7.00}$$

となる[2]。また、16 段構成において最終段の F 関数出力を推定するための最大差分特性確率は、出力差分値が 0 でないため

$$DCP = {DP_{mF}}^{15\times 2/3} = 2^{-70.00}$$

となる。これは提案者による自己評価書の結果と大きく異なる。

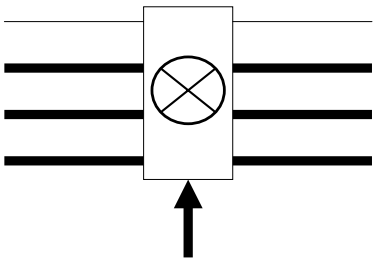
3.2 新たに見出した経路における T 関数の独立性

新たに見出した差分特性確率が最大になるケースにおいて、アクティブとなる T 関数は 1 つである。よって、この T 関数は独立である。

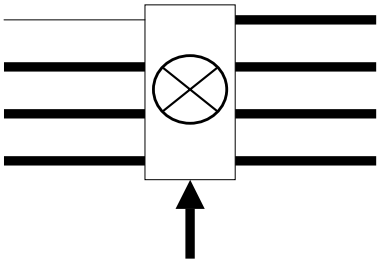
3.3 耐差分攻撃についてのまとめ

再探索の結果、トランケート差分の立場で自己評価書で報告されているよりも高い最大差分特性確率を得た。これは 128 ビットブロック暗号に期待される確率を上回っているため、mF 関数を用いたトランケート差分評価では CIPHERUNICORN-A の差分攻撃に対する安全性を示すことはできなかった。

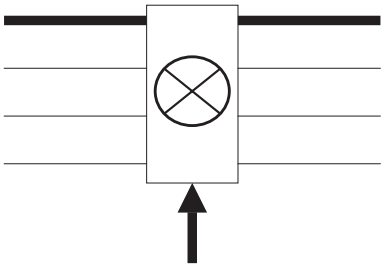
[2]なお、トランケート差分について、どのような経路も定数乗算に対し認めた場合、図 4,5 以外で、$2^{-7.00}$ の最大差分パスが多数見出された。



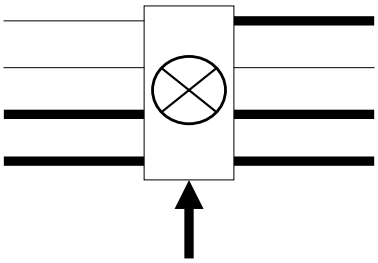
(a) パターン 1



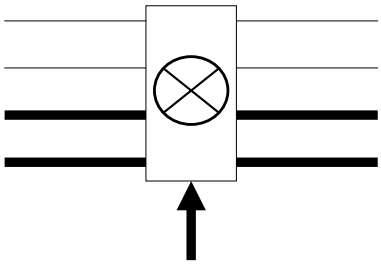
(b) パターン 2



(c) パターン 3



(d) パターン 4



(e) パターン 5

図 7: 定数乗算のパターン

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

4.1.1 提案者による自己評価

提案者は、自己評価書において mF 関数に対し線形マスク値をバイト単位の 0,1 として全パターンを代入し、通過した換字テーブルを調べた結果、図 8 のケースが線形特性確率 LP_{mF} を最大にし、その値は

$$\begin{aligned} LP_{mF} &= ((S_0 \parallel S_1 \parallel S_2 \parallel S_3) \text{で入力マスク} = 0)^4 \\ &\quad \times ((S_0 \parallel S_1 \parallel S_2 \parallel S_3) \text{で入力マスク} \neq 0)^1 \\ &\quad \times ((S_1 \parallel S_2 \parallel S_3) \text{で入力マスク} = 0)^3 \\ &= 2^{-2.71\times 4} \times 2^{-2.39\times 1} \times 2^{-3.08\times 3} \\ &= 2^{-22.47} \end{aligned}$$

であると報告している。一般に、F 関数の入力マスク値が 0 の場合、その最大線形特性確率を q としたときの R 段の線形特性確率は最大で $q^{R/2}$ となることから、16 段において最終段の F 関数出力を推定するための最大線形特性確率 LCP は、

$$LCP = {LP_{mF}}^{15\times 1/2} = 2^{-157.29}$$

であると報告している。

4.1.2 本報告での評価

本稿では、mF 関数に対し線形マスク値をバイト単位の 0,1 として全パターンを代入し、通過した換字テーブルを再度探索した。その際、すべての T 関数は独立であると仮定した. この仮定に関する考察は後述する。その結果、図 8 とは異なる最大線形特性確率が最大となるケースが存在した。新たに発見したケースの一例を図 9 及び図 10 に示す。これらのケースが新たに発見されたのは、自己評価書の分岐におけるマスク値の流れを適切に評価していない可能性が一つの要因として考えられる。図 8 と図 9 及び図 10 の違いは、1 次鍵生成部におけるアクティブな T 関数における換字テーブルの連接数であり、3 並列から 4 並列になった分、最大線形特性確率が上昇している。

図 9 のケースにおける mF 関数の最大線形特性確率は、

$$\begin{aligned} LP_{mF} &= ((S_0 \parallel S_1 \parallel S_2 \parallel S_3) \text{で入力マスク} = 0)^7 \\ &\quad \times ((S_0 \parallel S_1 \parallel S_2 \parallel S_3) \text{で入力マスク} \neq 0)^1 \\ &= 2^{-2.712\times 7} \times 2^{-2.385\times 1} \\ &= 2^{-21.369} \end{aligned}$$

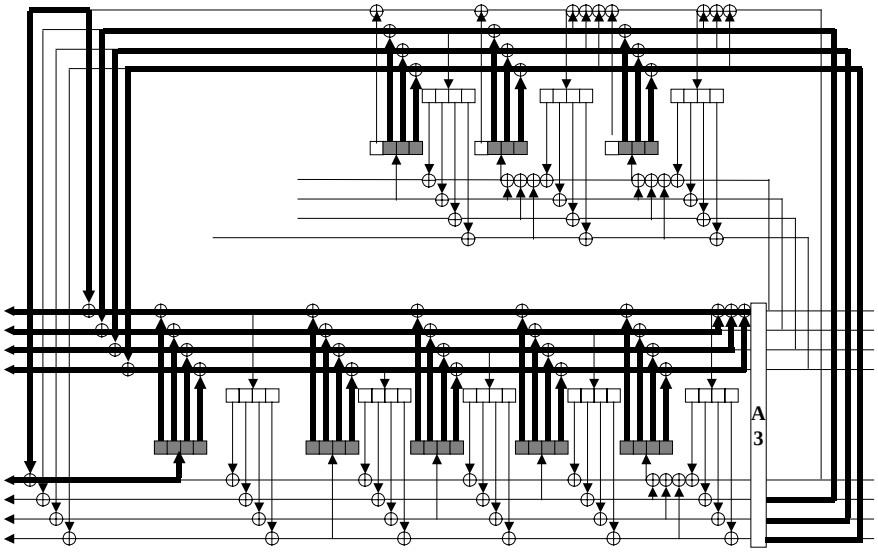


図 8: 線形特性確率が最大になるケース（自己評価書）

となる。また、16 段構成における最終段の F 関数出力を推定するための最大線形特性確率は、入力マスク値が 0 なので

$$LCP = {LP_{mF}}^{15\times 1/2} = 2^{-149.52}$$

となる。

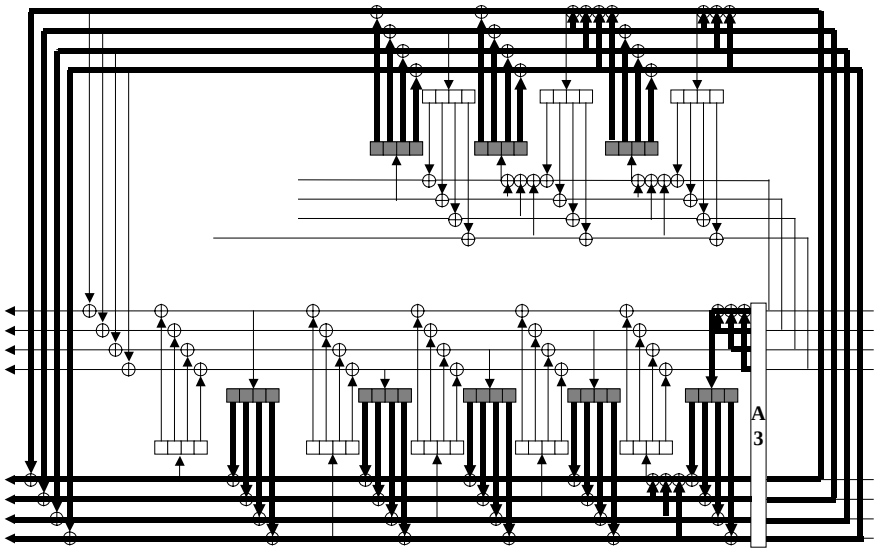


図 9: 線形特性確率が最大になるケース１（新たに見出したもの）

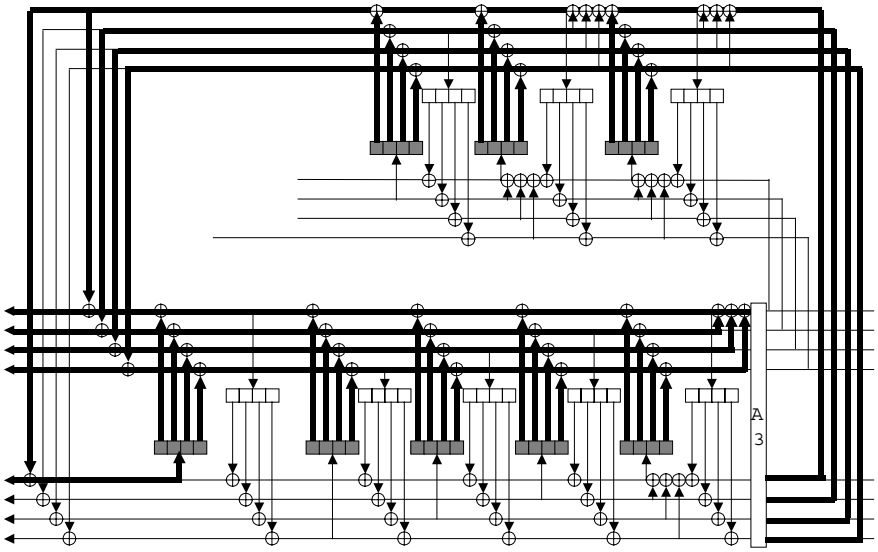


図 10: 線形特性確率が最大になるケース２（新たに見出したもの）

4.2　新たに見出した経路における T 関数の独立性

新たに見出した線形特性確率が最大になるケースにおいて、アクティブな T 関数はいずれも 8 つである。ケース 1 及びケース 2 において、図 11 及び図 12 の A、B、C 及び D で示した T 関数の独立性は明らかではない。ケース 1 におけるこれらの T 関数について考察を行う。また、ケース 2 でも同様である。

本流部　:　ここでは、Fk_a,Fk_b, の算術加算は排他的論理和で近似する。A3 関数は排他的論理和加算に対し線形性を有し、図 13 に示す等価鍵変形を行うことができる。図 11 の本流部について A と B の独立性にかかわる部分を抜粋し、このような等価鍵変形を行ったものが図 14 である。$F\tilde{K}_a$ の最上位バイトを k1、$F\tilde{K}_b$ の最下位バイトを k2 とする。換字テーブルは全単射であることから、鍵 k1,k2 が全通り均等に発生したとき、A における T 関数と B における T 関数の入力は独立な値をとる。

一時鍵生成部　:　図 15 のように、算術加算鍵は等価変形で定数乗算の後に移動可能である。移動後の等価鍵加算を排他的論理和加算で近似する。図 11 の一時鍵生成部について、このような等価鍵変形を行ったものが図 16 である。等価鍵 $S\tilde{K}_a$ の上位から 2 バイト目を k3 とする。拡大鍵 SK_b の最上位バイトを k4 とする。換字テーブルは全単射であることから、鍵 k3,k4 が全通り均等に発生した時、C における T 関数と D における T 関数の入力は独立な値をとる。

以上の考察から、ケース 1 及びケース 2 のいずれの経路においてもアクティブな T 関数は独立であることから、前節における導出法で線形特性確率を見積もることができる。

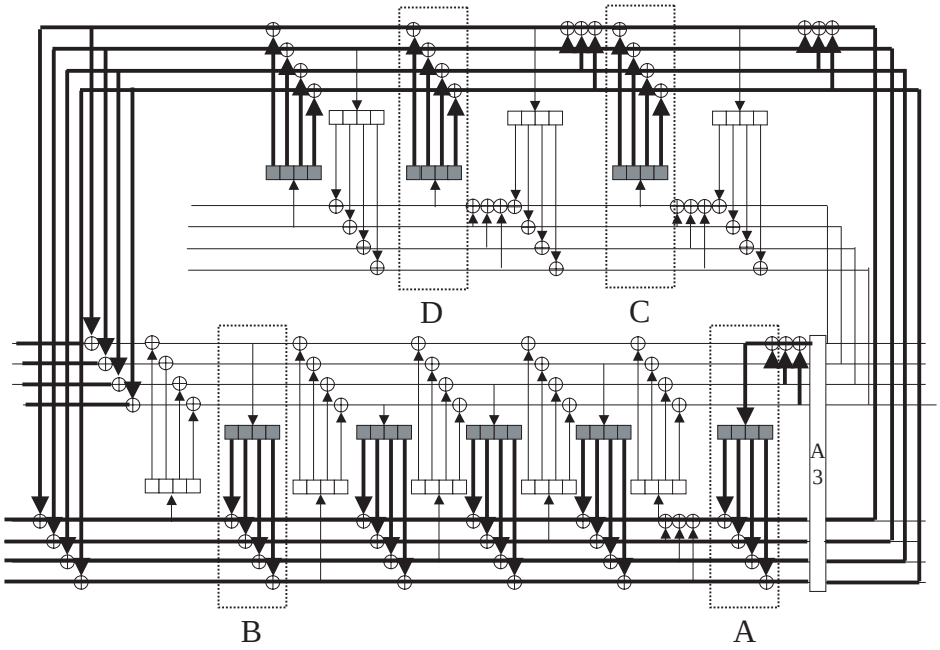


図 11: 考察する T 関数部 (ケース 1)

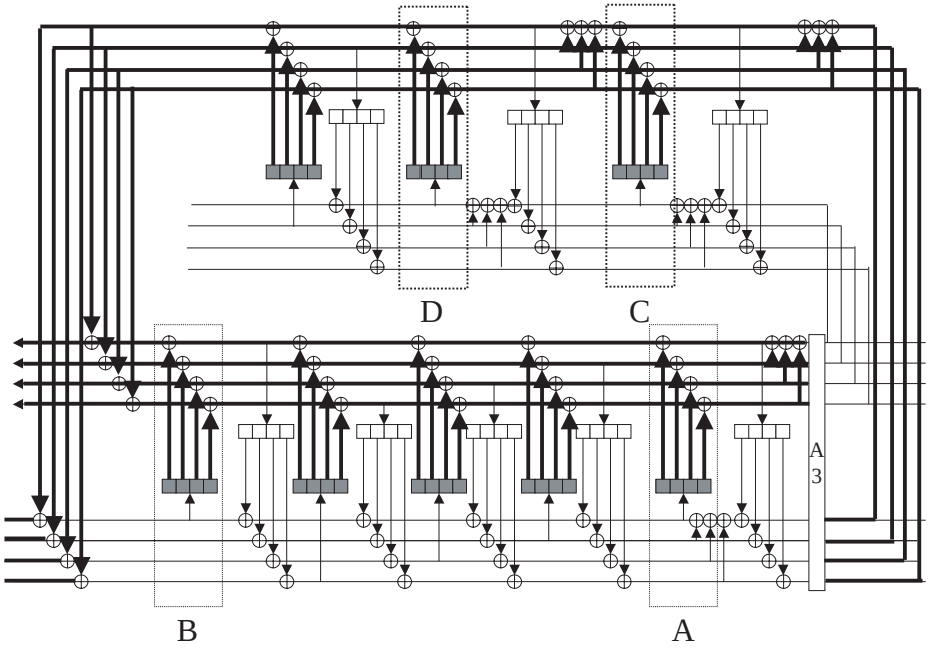


図 12: 考察する T 関数部 (ケース 2)

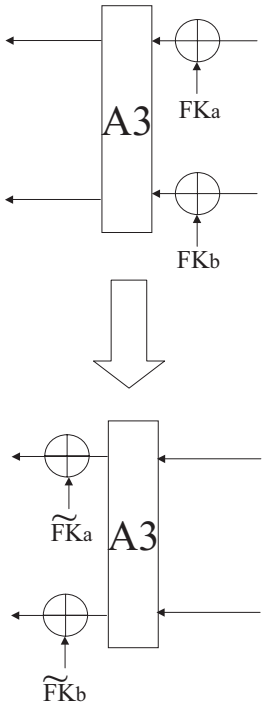


図 13: 本流部におけるの等価鍵変形

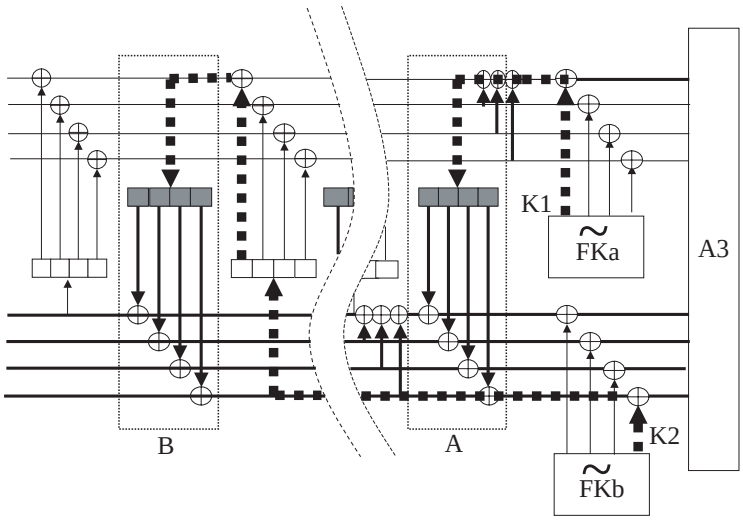


図 14: 等価鍵変形を行ったケース 1 の本流部 (抜粋)

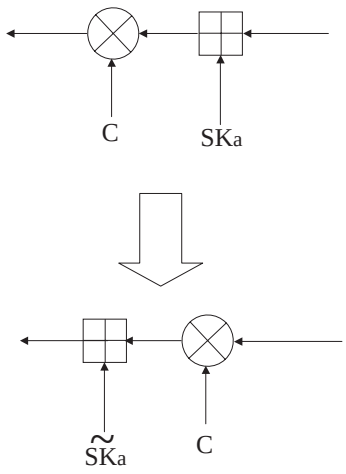


図 15: 一時鍵生成部における等価鍵変形

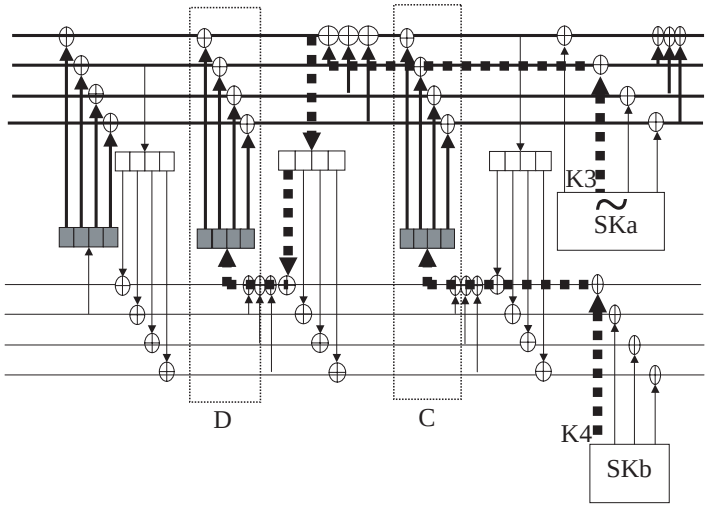


図 16: 等価鍵変形を行ったケース 1 の一時鍵生成部

4.3 耐線形攻撃についてのまとめ

mF 関数における再探索の結果、自己評価書よりも大きい線形特性確率を与えるケースを得ることができたが、CIPHERUNICORN-A 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。

5 結 論

提案者による mF 関数近似は、安全側への評価であるという意味で、適切な近似であることを確認した。しかし、トランケート差分探索による最大差分特性確率は、$2^{-70.00}$ となり、128 ビットブロック暗号に期待される確率を上回る。よって、mF 関数を用いたトランケート差分評価では CIPHERUNICORN-A の差分攻撃に対する安全性を示すことはできなかった。そのため、可能な計算量で安全性を評価できるような別の F 関数近似を提案者が示すことを望む。

一方、最大線形特性確率は $2^{-149.52}$ となり、自己評価書とは異なる値を得たが、128 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線形攻撃に対する安全性という面では問題はないと言える。

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-A”

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

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

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