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。本暗号を、乱数検定、差分攻撃、線形攻撃、高階差分攻撃、補間攻撃、鍵衝突攻撃、それぞれ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付くような深刻な問題点は導かれなかった。各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。

乱数検定 :

5 段以上では、今回用意した全ての検定項目で乱数と区別されない。

差分攻撃 :

自己評価書の記述にやや疑問点があるものの、差分攻撃に対する安全性に問題はない。

線形攻撃 :

自己評価書の記述にやや疑問点があるものの、線形攻撃に対する安全性に問題点はない。

高階差分攻撃 :

高階差分攻撃に対する問題点はない。

補間攻撃 :

補間攻撃に対する問題点はない。

鍵衝突攻撃 :

自己報告書の記述にやや難があるものの、暗号そのものの安全性については問題ない。

1 乱数検定

暗号の安全性評価法の一つとして、与えられた入力に対する暗号の出力を疑似乱数として見た場合に、その列が、真の乱数列との区別可能であるかどうかによって、その暗号が安全であるかどうかを判断するという報告例がいくつかみられる。そもそも、現代共通鍵ブロック暗号の代表格である差分攻撃法／線形攻撃法にしても、ある一定段数までに、入力差分と出力差分との関係、あるいは入出力ビットの線形式の値を調べることにより、それぞれ真の乱数とは著しく性質が異なることを利用して、最終段の鍵の値を推定する方法であるから、この「真の乱数列と区別可能かどうか」という基準は、暗号の安全性に密接に結び付いているといってよく、この基準をクリアしない暗号は、解読される危険があると考えられる。その意味から、提案者によって提出された安全性評価書に見られるようなビットアバランシュ性等の初等統計量調査による調査は、十分に意味があると思われる。

さて、安全性評価書によれば提案者らが行なった検定項目は次の 4 項目であるとされている。

- アバランシュ
- ビットバランス
- 入出力間関連
- 出力間関連

提案者らはこれらの項目について本暗号と DES, MISTY の一段の性質を検定した所、本暗号がいずれの項目でも相対的に低い相関性しか持たないこと実験的に調べている。

提案者が行なったこれらの検定を検証する意味を含め、本報告書では下記に示す統計量調査を行なった結果について報告する。

> AES 選考の際に NIST が行なった 189 種類の乱数検定法を用いて計算機による検定実験を行ない、何段以上であればこれら全ての乱数検定に合格するかを調査する。

行なった検定項目は次の通りである。

- Frequency,
- Block-Frequency,
- Cusum(2 種),
- Runs,
- Long-Run,
- Rank,
- FFT,
- Aperiodic-Template(148 種),
- Periodic-Template,
- Universal,

- Apen,
- Random-Excursion(8 種),
- Random-Excursion-V(18 種),
- Serial(2 種),
- Lempel-Ziv,
- Linear-Complexity,

なお、各々の乱数検定項目の詳細については [1] を参照して頂きたい。今回の検定で行なった検定実施方法ならびにデータサンプリング方法は以下の通りである。

検定実施方法：

Hamming weight が 2 以下の 64 bit データ 16648 Byte に対し、そのデータを入力値とし、相異なる拡大鍵 300 個によって生成された暗号文 (全体で約 5 MByte) のそれぞれの乱数性を調べ、その合格率を調査する。
合格率の閾値は NIST による検定と同じく 0.9633 以上、すなわち、300 個のデータの中で 96.33 % 以上が乱数と判定された場合、そのテストは合格であるとする。

実験の結果を、図 1 から 図 6 に示す。各々のグラフについて、横軸は各検定テスト項目 1 〜 189 番目に相当し、縦軸は、集められたデータの乱数性非棄却率である。非棄却率が 1 に近い程乱数性が高いことを示している。図 5 から 図 6 までは、見やすくする為に縦軸を [0.0,1.0] から [9.6,1.0] へ縮尺を変えているので注意して頂きたい。

実験の結果から、今回行なったこれらの乱数検定では、1, 2 段では暗号の出力を乱数と区別できる可能性が極めて大きいが、3,4 段目の出力ではほとんどの項目について乱数検定に合格し、さらには 5 段以上では (標準仕様である 16 段も含めて) その出力を乱数と区別することは難しいと判断される。

なお F 関数が十分ランダムであるような Feistel 暗号の場合、3 段以上で Random Permutation, 4 段以上で Strongly Random Permutation となるという性質が知られており [2]、本実験による 1, 2 段目の出力が乱数と区別可能であるという性質は、CIPHERUNICORN-E が Feistel 構造であるということに由来しているものと思われ、CIPHERUNICORN-E 独自が持つ性質ではないものと考えられる。

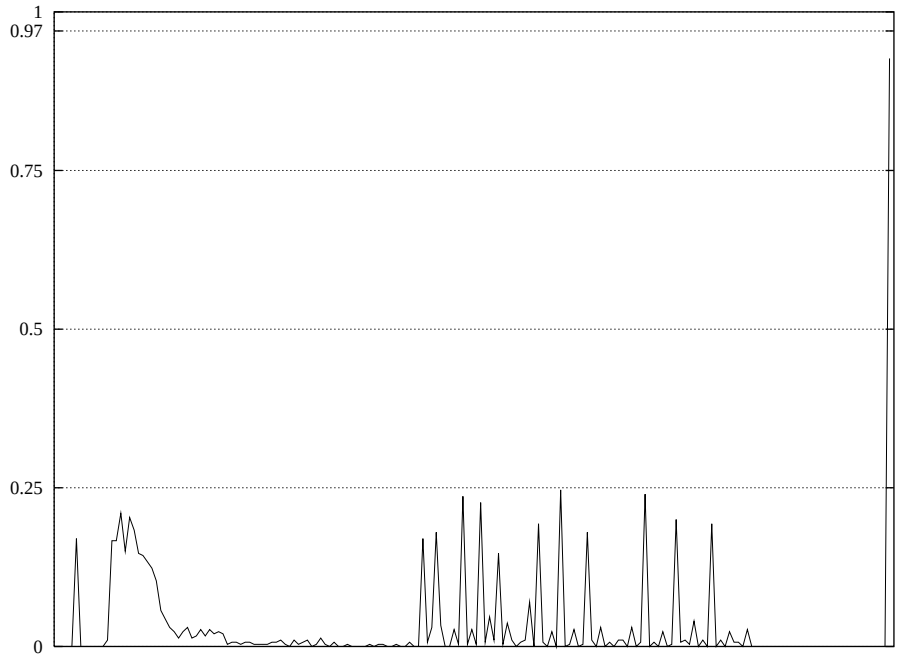

図 1: 1 段 [成功確率 0.0 ～ 1.0]

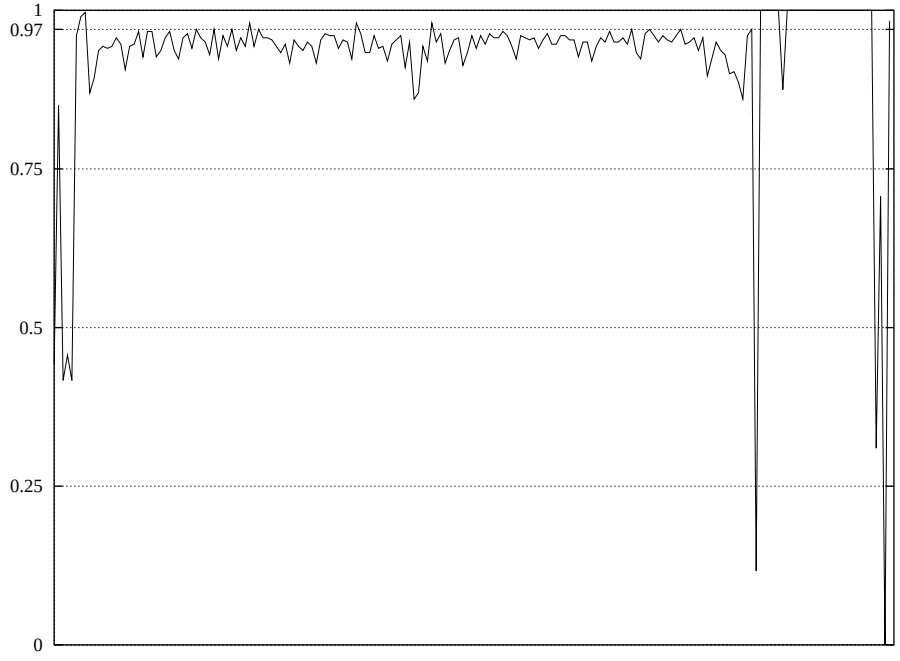

図 2: 2 段 [成功確率 0.0 ～ 1.0]

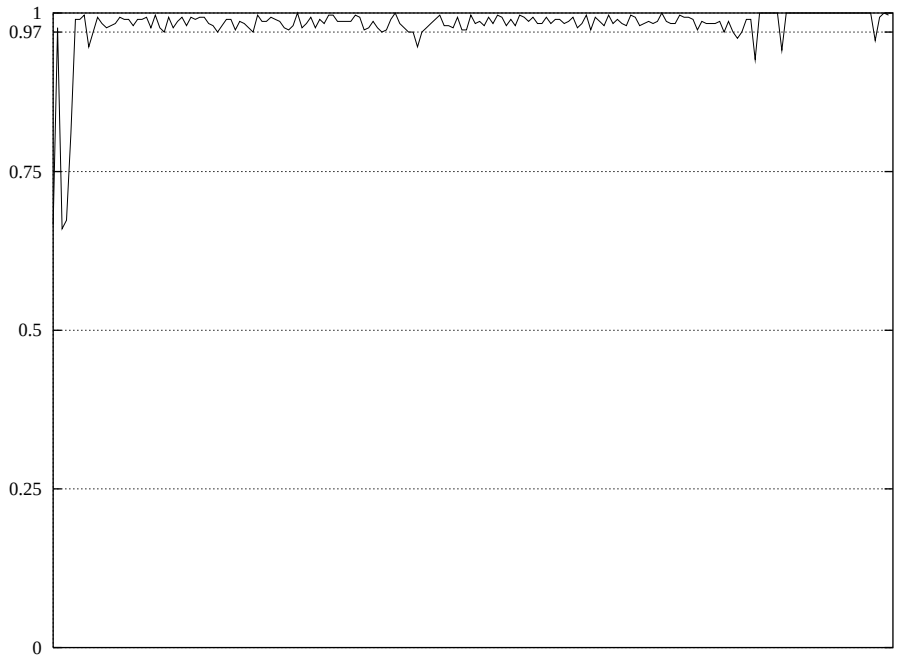

図 3: 3 段 [成功確率 0.0 ～ 1.0]

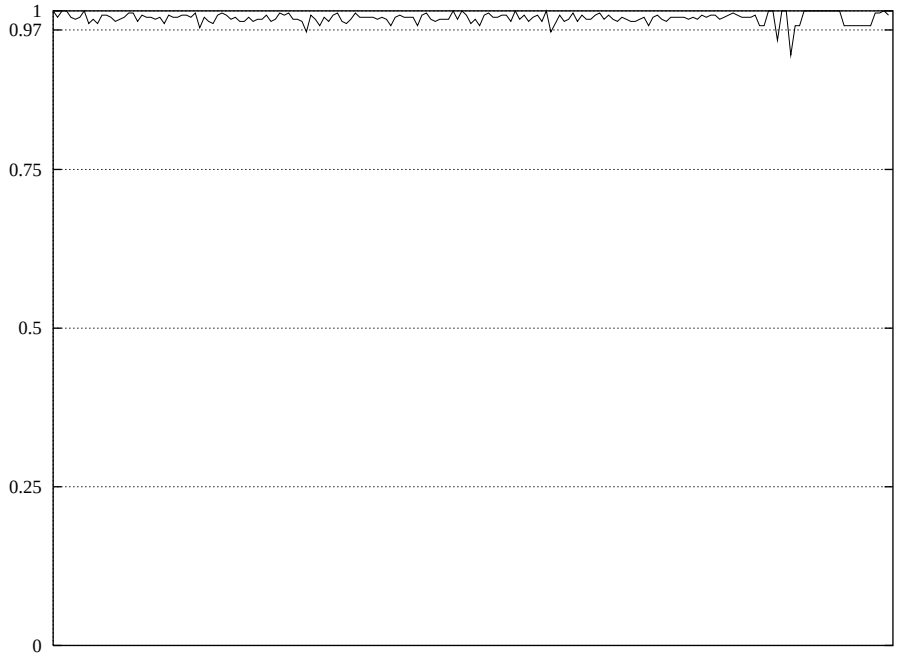

図 4: 4 段 [成功確率 0.0 ～ 1.0]

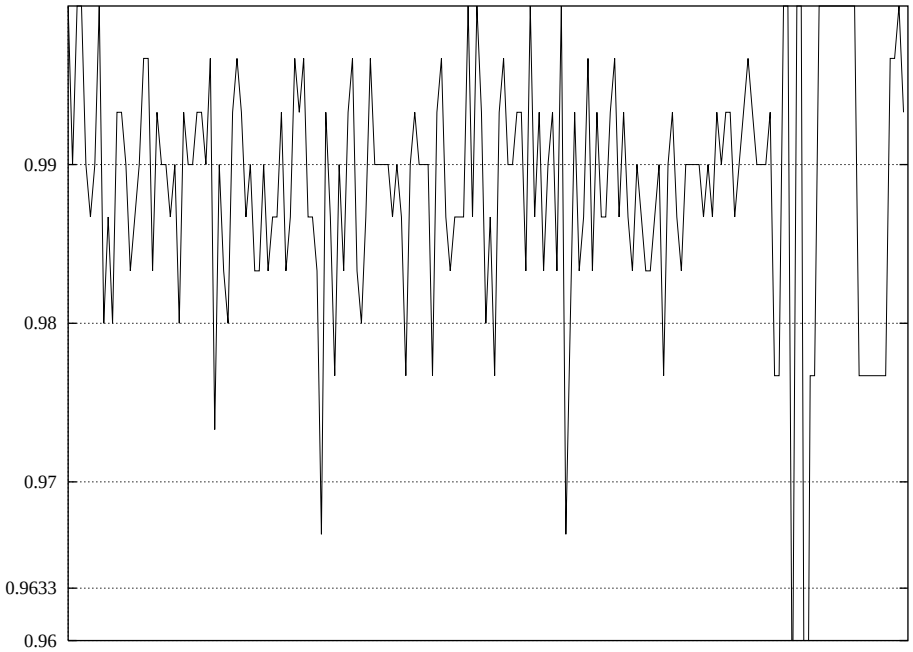

図 5: 4 段 [成功確率 0.96 ～ 1.0]

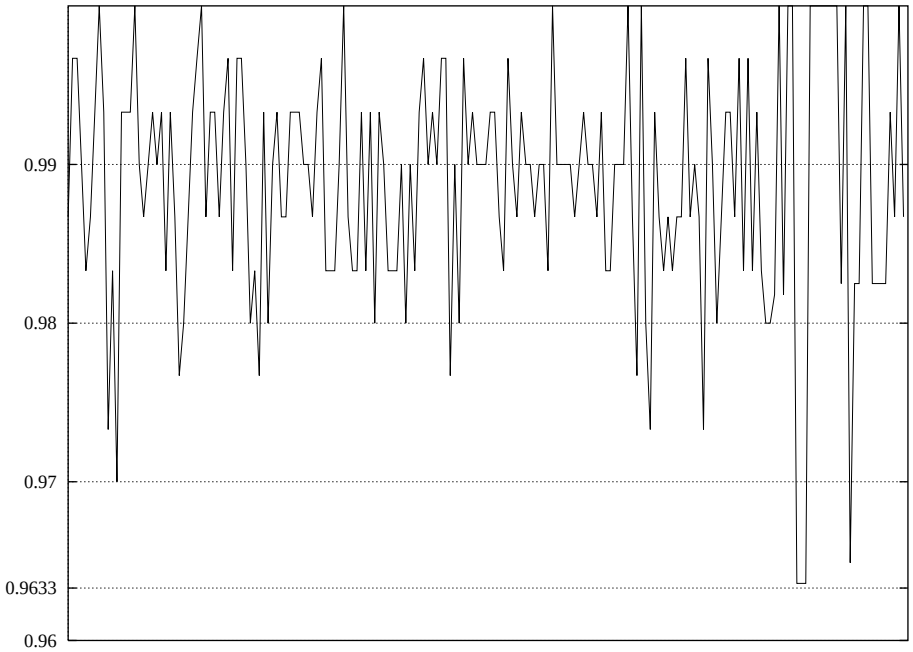

図 6: 5 段 [成功確率 0.96 ～ 1.0]

2 差分攻撃

本暗号は F 関数内部の演算において 32 ビット鍵算術加算および 32 ビットシフト加算 (Y 関数)、さらにデータ依存 S-box 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を求めることは、困難であると思われる。設計者による安全性解析では、F 関数に対して次のような単純化を行なった関数 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 bit 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。

上記の様に単純化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なものであってはならない。このような立場から、上記の単純化に関する正当性について、意見を述べておく。

- 1 については、排他的論理和に置き換えてもなお安全であることが示されれば、変換前の暗号の安全性についても保証されたと考えていいと思われる。ただし、本暗号のように算術加算が拡大鍵に対してなされている場合には、鍵の値によって差分確率に差が生じ、weak key となる場合があることに注意が必要である [3]。
- 2 については、Y 関数に用いるローテートシフト量の決め方からその性質を近似しようと考えてのことであると思われる。つまり入力 32 ビットの内、ハミングウェイトが 1,2 の場合には、出力上位 1 バイト中のビットそれぞれの差分の期待値が $1/2$ に近い値になるという定数の設計方針から、その性質のみをこの方法で抽出するための単純化であると考えられる。Y 関数は、本暗号独自の関数であり、これまでこの様な関数の差分確率について論じた文献は見当たらないため、Y 関数について何らかの近似が必要となるのは仕方が無い。本近似方法によって、安全性が増すような構造になっているとは思われないことから、本近似による安全性の検証は、安全性を検証するための一つの近似手段として、認められるものと思われる。なお、その他の方法としては、シフト加算をシフト排他的論理和で置き換えるか、あるいは完全に取り去ってしまうという単純化の仕方もあるものと思われる。いずれの単純化がより元の F 関数の性質を残しているかどうかは分からないが、今後検討する価値はあるだろう。

さて、上記の考察から、自己評価書による単純化された F 関数 mF の解析には妥当性があると考えられるので、本詳細評価においてもこの関数 mF について調べることにする。

S-box の設計法から各 $T(i)$ 関数の差分確率の最大値は、全て 2^{-6} となる。自己評価書では mF と単純化したラウンド関数について、バイト単位の差分探索を行なった結果、図 7 のようなケースが差分特性確率 DP_{mF} を最大にし、その値は

$$DP_{mF} = (2^{-6})^2 = 2^{-12}$$

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 の場合、その差分確率を q としたときの R 段の差分確率は、最大で $q^{R\times 1/2}$ となることから、16 段目の出力を推定するための最大差分確率 DCP は、

$$DCP = (DP_{mF})^{(15\times 1/2)} = 2^{-84}$$

表 1: 提案者による 15 段評価

段数	1	2	3	4	5	6	7	8	
差分確率	1	2^{-12}	1	2^{-12}		1	2^{-12}	1	2^{-12}
全体	2^{0}	2^{-12}	2^{-12}	2^{-24}	2^{-24}	2^{-36}	2^{-36}	2^{-48}	

段数	9	10	11	12	13	14	15
差分確率	1	2^{-12}	1	2^{-12}	1	2^{-12}	1
全体	2^{-48}	2^{-60}	2^{-60}	2^{-72}	2^{-72}	2^{-84}	2^{-84}

であると報告している。

この報告で述べられている攻撃法は、最良ではない。

提案者は 15 段における DCP の値は $2^{-84} = (2^{-12})^7$、つまり 7 段分の近似が必要であるとしている。おそらく 15 段の差分近似を、表 1 のように配分したものと思われる。

この近似式は差分が 0 でない入力ビット数はわずか 16 ビットであるから、この近似式を用いて 1 段目ならびに 15,16 段目の拡大鍵のうちそれぞれ $16 \times 2 = 32$ ビットを推定する、いわゆる (1+2)- 段消去型攻撃を用いることができる (図 8)。

本攻撃で推定する鍵ビット数は、 32 ビットであり、用いられる 13 段差分近似式 DCP_{13} の成立確率は、最高で

$$DCP_{13} = (2^{-12})^6 = 2^{-72}$$

となるから、攻撃者に対し最も有利な仮定を設定した場合には最低で 2^{72} 個の選択平文で解読できることになり、提案者が示す必要平文数より少ない値となった。ただし 2^{72} 個の選択平文数は、可能な全ての平文数 2^{64} を越えているため、 (2+1)- 消去型攻撃を用いても、攻撃は成功しない。同様のテクニックを用いれば 15 段までであれば、 (2+2)- 消去型攻撃法を用いて mF 関数を用いた Feistel 型暗号を攻撃が可能となる可能性がある。

3 線形攻撃

本暗号は F 関数内部の演算において 32 ビット鍵算術加算および 32 ビットシフト加算 (Y 関数)、さらにデータ依存 S-box 等を用いていることから、差分攻撃と同様、従来から知られている手法では厳密に線形確率を求めることは、困難であると思われる。提案者は、差分攻撃と同様、 F 関数を単純化した mF 関数を用いて、本暗号の線形攻撃に対する安全性を検証している。mF 関数への単純化については、差分攻撃と場合同様、安全性を評価する上での正当性があるものと思われる。自己評価書によれば、 mF 関数の線形近似特性をバイト単位のマスク値で探索した所、図 9 のパターンで線形特性確率が最も大きくなり、その確率 LP_{mF} は以下の値となったと報告している。

$$\begin{aligned} LP_{mF} &= (((S_0S_1S_2)\text{での入力マスク} \neq 0)^2 \times ((S_0S_1S_2)\text{での入力マスク} = 0)^1 \\ &\quad \times ((S_0S_2)\text{での入力マスク} = 0)^2 \times ((S_1S_2)\text{での入力マスク} \neq 0)^2 \\ &\quad \times ((S_1)\text{での入力マスク} \neq 0)^2 \times ((S_2)\text{での入力マスク} \neq 0)^1 \\ &\quad \times ((S_3)\text{での入力マスク} \neq 0)^4 \\ &= 2^{-2.60\times 2} \times 2^{-3.22\times 1} \times 2^{-3.66\times 2} \times 2^{-3.08\times 2} \times 2^{-6.00\times 2} \times 2^{-6.00\times 1} \times 2^{-6.00\times 4} \\ &= 2^{-63.90} \end{aligned}$$

一般に入力マスクが 0 で線形確率が q であるような線形パターンを用いた R 段の Feistel 型暗号の線形特性確率は $q^{R\times 1/2}$ で与えられることから、提案者らは本暗号 16 段目の F 関数の出力を推定するための線形特性確率 LCP の下界として、

$$(2^{-63.90})^{15\times 1/2} = 2^{-447.30}$$

が示されるため、 mF 関数を用いた暗号であっても線形攻撃に対し、安全であると結論づけている。

この自己評価については疑問点がある。

まず、 64 ビット入出力の関数について、最良線形確率の理論的な下限値は 2^{-64} であり、提案者が示す値 $2^{-63.90}$ は、矛盾はしていないとはいえ、現実にそぐわない値である。図 9 のパターンにおいて active となる各 T 関数の入力それぞれに対し、独立の拡大鍵値を加算しているわけではないため、入力に強い相関関係があるものと思われ、実際の線形確率は、より大きく異なることが予想される。例えば、 下段中央で S_3 が連続する所では、 $S_3(S_3(x))$ という一つの S-box と見る必要があり、その線形確率は、全単射性からせいぜい 2^{-6} である。ただし各 T 関数の入力値の従属性に関する解析が複雑であるため、これ以上詳細に求めることは非常に困難であると思われる。

さて、本暗号に対してこの線形パターンを用いて線形攻撃を行なう場合、鍵の全数探索より少ない計算量で解読する方法としては、差分攻撃の場合と異なり、 1- 段消去型攻撃法を用いるのが最良である。いずれにせよ、現時点で mF 関数をラウンド関数とする Feistel 型暗号への線形攻撃は成功していない。

今回、 F 関数を mF 関数で単純化した暗号について線形攻撃に対する安全性を再評価した結果、安全性に関する深刻な問題は発見できなかった。また、仕様通りの F 関数についての線形攻撃に対する安全性については、現時点では問題点は何も見付かっていない。ただし、より安全性を詳しく検証するために、今後はより F 関数に近い形で厳密な評価を行なった方がよいと思われる。

4　高階差分攻撃

提案者は自己評価書において、F 関数の低次項 (1 次〜 6 次) の項数を鍵値を変えて計算し、その項数の最大値、最小値、平均値を求め、ランダムな関数の場合、理論的に導かれる期待値から差がほとんどないことを導き、F 関数の代数次数は最低でも 6 次であり、5 段以上では解読に必要な平文を用意することは不可能であると導いている。

本結果は、F 関数を近似すること無く、低次の項数を計算した上で導いたものであり、本暗号を高階差分攻撃を用いて解読することは不可能であるとの結論には妥当性があると思われる。

5　補間攻撃

提案者は自己評価書において、F 関数で用いる 4 種類の S-box の入出力を $GF(2^8)$ の多項式で表現した時の項数を計算し、最低でも 252 項以上であったことから、暗号全体を多項式で表現するために必要な平文を用意することは不可能であり、補間攻撃に対して十分に安全であると期待していると述べている。

本暗号の S-box は、$GF(2^8)$ の冪乗演算を利用していることから、S-box 単体では、有理式表現を用いた攻撃に対する耐性を検討しなければならないところではあるが、F 関数全体としては、定数乗算や、拡大鍵の算術加算等、別の代数系が用いられていることによって、多項式表現が極めて難しくなっているものと思われる。よって補間攻撃に対しては、段数が少ない場合を除き攻撃が成功することはないとの考えは、妥当性があると思われる。

6　鍵衝突攻撃

提案者は自己評価書において、鍵衝突攻撃は暗号器の内部構造によらず、秘密鍵ビット長のみに依存する、と述べているが、これは、鍵スケジュール部が理論的にランダムな関数であることを仮定した場合に行なう考察であって、本件のように具体的な鍵スケジュール部が存在する場合は、解析が必要であり、記述として不十分であると感じられる。

さて、本暗号についていえば、仕様書 図 3.10 において、 ST 関数が Feistel 構造を利用した構造になっていることから、 ST 関数の入力 4×32 ビット X_0, X_1, X_2, X_3 から拡大鍵

$$SK^i[0], SK^i[1], SK^{i+1}[0], SK^{i+1}[1]$$

への 1 対 1 写像が導かれる。このような写像の存在より、異なる秘密鍵に対して、上記拡大鍵のいずれかが必ず異なるため、本暗号では、少なくとも拡大鍵に関しては鍵衝突が起こらないことが理論的に示される。

参考文献

[1] "Random Number Generation and Testing," National Institute of Standard Technology, URL`http://csrc.nist.gov/rng/rng2.html`

[2] M. Luby and C. Rackoff, "How to Construct Pseudorandom Permutations from Pseudorandom Functions," SIAM Journal on Computing, 17(2), pp.373–386, 1988.

[3] S. Moriai, K. Aoki, and K. Ohta "Key-Dependency of Linear Probability of RC5," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, E80-A(1), 1997.

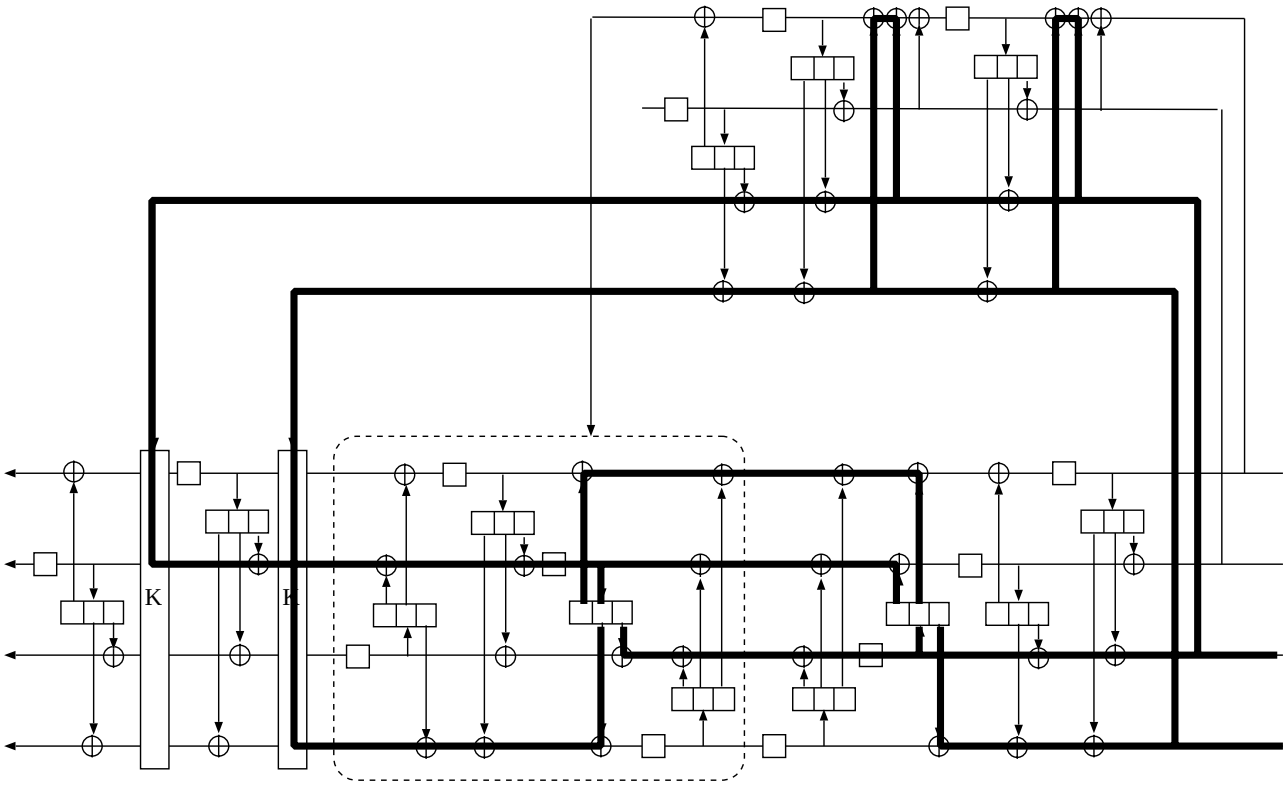

図 7: 提案者らによる最良差分近似

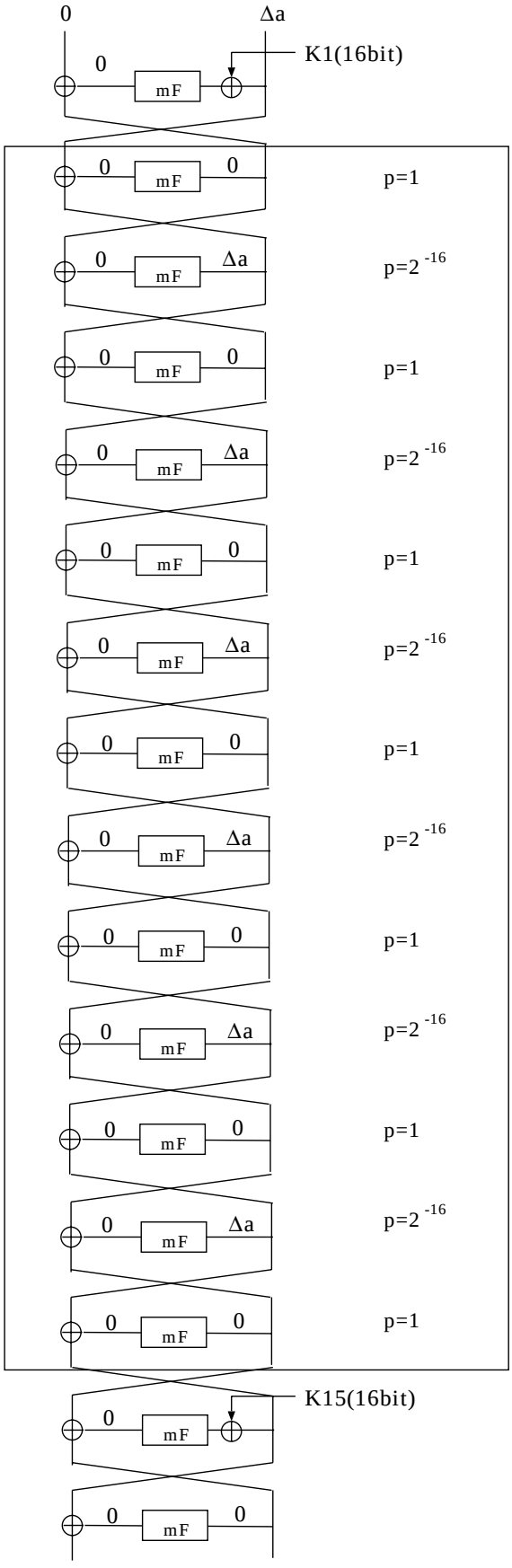

図 8: (1+2)- 段消去型差分攻撃

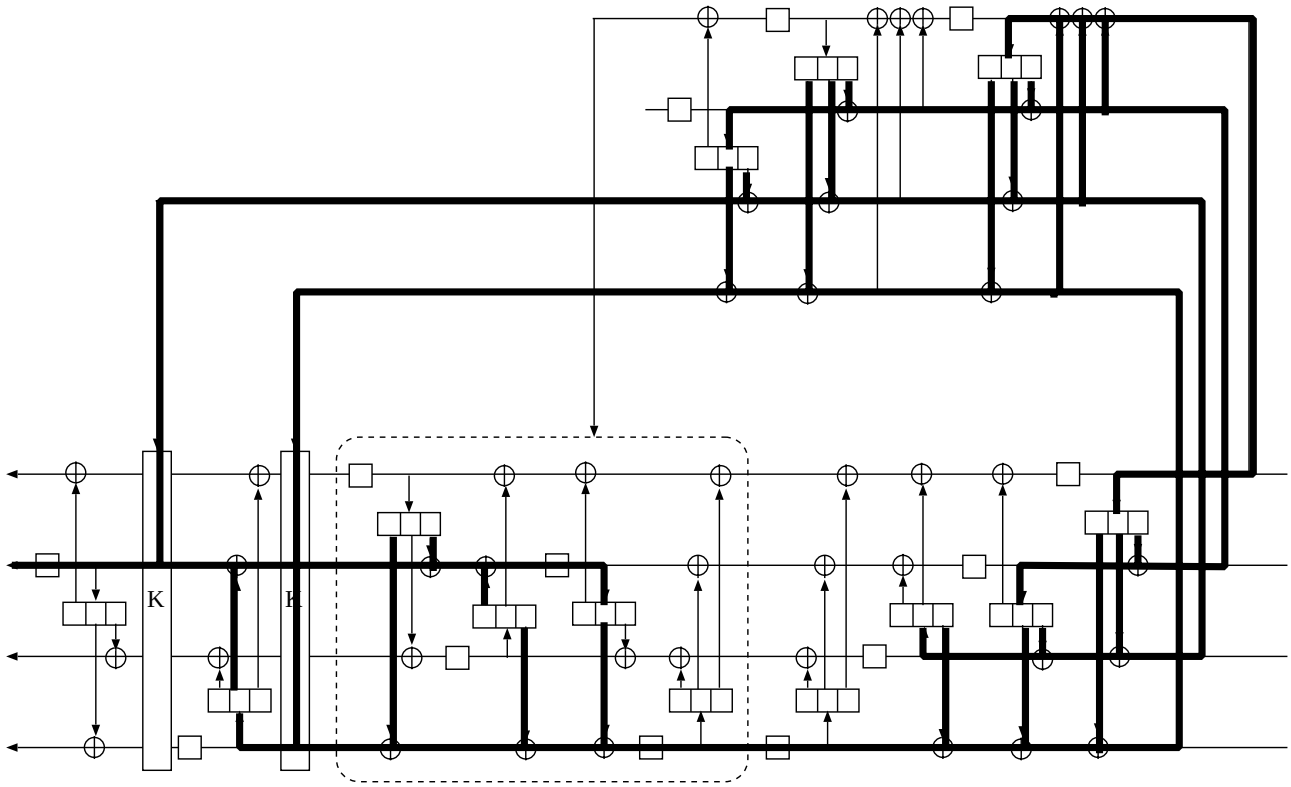

図 9: 提案者らによる最良線形近似