ＣＲＹＰＴＲＥＣ応募暗号の高階差分及び補間攻撃耐性について

（Ver.1）

平成１３年１月

１．　はじめに

これは、電子政府用暗号として、応募された６４ビット／１２８ビットブロック暗号に対する高階差分及び補間攻撃の立場の検証評価である。対象暗号は６４ビットブロック暗号として、CIPHERUNICORN-E、MISTY1、FEAL-NX、Hierocrypt-L1 の４暗号、１２８ビットブロック暗号として CIPHERUNICORN-A、Camellia、RC6、SC2000、MARS、Hierocrypt-3 の６暗号である。ここでは、自己評価書及び、関連論文の調査並びに計算機探索により、高階差分及び補間攻撃耐性に関し、各暗号に対し考察を行った。

２．　評価項目

多くの暗号は、その構成部品として、S-box、F 関数を持つ。暗号に非線形特性を与える最小の構成部品を S-box と呼ぶ。平文は、暗号化関数を通る間に、非線形処理と線形処理の繰り返しを受けるが、S-box より大きなブロック単位で、繰り返し構造の基本単位を構成する部分をＦ関数と呼ぶ。各暗号の S-box 及び F 関数相当部品に対する以下の評価を基に、暗号の高階差分及び補間攻撃耐性を考察する。

（１）S-box $S(X)$の評価

（１－１）ブール多項式次数、項数

$S(X)$をブール多項式で表現し、その次数及び項数を評価する。

（１－２）拡大体上の補間多項式表現の項数

テーブルとして与えられる $S(X)$について、全ての拡大体 GF(2^m）上で補間多項式表現し、その項数を評価する。ここで $m=|X|$。

（２）Ｆ関数 $F(X)$の評価

（２－１）S-box 以外の F 関数構成要素のブール多項式項数、次数

（２－２）$F(X)$のブール多項式次数

$F(X)$のブール多項式表現を（１－１）及び（２－１）の結果を用い $F(X)$のブール多項式表現を求め次数評価を行う。計算量的に不可能な場合は、形式的代数次数評価で代用。

（２－３）$F(X)$ブール多項式における低次項の出現頻度の評価

関数 $F(X)$の低次項係数で非零の個数を評価する。これは、（２－１）が形式的代数次数評価で行われた場合の補足データ。

（３） 高階差分攻撃及び補間攻撃の評価

ここでは主として、暗号化関数のコアに着目し段数に対する強度評価を行う。

（３－１）代数次数評価

適切な高階差分を選び、段数に対する暗号系の形式的代数次数の上昇を評価する。

（３－２）１－８高階差分特性の評価

平文８ビット以下を選ぶ任意の組み合わせに対し、１－８階差分値を計算し、段数に対する高階差分攻撃可能性を調査する。

（３－３）３１及び３２階高階差分特性の評価

平文ブロック３２ビットを選び、３１階及び３２階差分値を計算し、段数に対する高階差分攻撃可能性を調査する。

（３－４）ＳＱＵＡＲＥ型攻撃評価

F関数構成部品の１対１写像性を利用した高階差分攻撃の可能性を、段数に対し評価する。

（３－５）線形和攻撃耐性の評価

線形和攻撃の観点から、補間多項式の項数を調査し、段数に対する線形和攻撃耐性を評価する。

（３－６）

以上の評価をもとに、高階差分攻撃又は線形和攻撃（補間攻撃）耐性の評価を行う。

３．　高階差分攻撃

３．１ 高階差分

$E(X;K)$を、入力 $X=(x_1,x_2,\cdots,x_n)\in GF(2)^n$ と鍵 $K\in GF(2)^s$ から、$Y=(y_1,y_2,\cdots,y_m)\in GF(2)^m$ を出力する暗号化関数とする。高階差分攻撃は、ブール関数の高階差分特性[L94]を利用した攻撃である。

定義１．高階差分

$\{a_1,a_2,\cdots,a_i\}$ を $GF(2)^n$ 上で１次独立な i 個のベクトル、これらによって張られる $GF(2)^n$の部分空間を $V^{(i)}$で表し、入力差分と呼ぶ。関数 $E(X;K)$の $V^{(i)}$に関する i 階差分 $\Delta^{(i)}E(X;K)$ は次式で定義される。

$$\Delta^{(i)}_{V^{(i)}}E(X;K)=\bigoplus_{A\in V^{(i)}}E(X\oplus A;K) \qquad (3.1)$$

この下付添え字 $V^{(i)}$は、誤解のおそれが無い省略する。高階差分は、次の性質を持つ。

性質１．

関数 $E(X;K)$の X に関するブール代数次数が N ならば、X と K に依存せず、次式が成立する。

$$\Delta^{(N+1)}E(X\oplus A;K)=0 \qquad (3.2)$$

この性質１を使用した高階差分攻撃が基本的高階差分攻撃である[JK97]。その攻撃能力は、以下の性質でさらに改良する事が可能である。

性質２．

関数 $E(X;K)$の X に関するブール代数次数が N で且つ、Ｎ次項の係数にＫが含まれていないならば、Ｎ階差分は、X と K に依存せず、関数 E固有の定数となる。

$$\Delta^{(N)}E(X\oplus A;K)=const \qquad (3.3)$$

ｎビットの入力 $\{x_1,x_2,\cdots,x_n\}$ から取り出したｋビット $\{x_{i1},x_{i2},\cdots,x_{ik}\}$ 組の積であるｋ

次項 $x_{i1}x_{i2}\cdots x_{ik}$ を考える。このｋビットを含むｋ'（≧ｋ）ビットのビット組のｋ'次項にｋ次項 $x_{i1}x_{i2}\cdots x_{ik}$ は含まれるというとする。このとき、次の性質が成り立つ。

性質３．

関数 $E(X;K)$のブール展開式にｋ次項 $x_{i1}x_{i2}\cdots x_{ik}$ が含まれていないならば、$\{x_{i1},x_{i2},\cdots,x_{ik}\}$ に対応するｋ個の単位ベクトルの組 $\{e_{i1},e_{i2},\cdots,e_{ik}\}$ で張られるｋ次元空間 $V^{(k)}(e_{i1},e_{i2},\cdots,e_{ik})$に関するｋ階差分は、$X$ と K に依存せず、次式が成立する。

$$\Delta_{V^{(k)}}^{(k)} E(X \oplus \mathrm{A};K) = 0 \qquad (3.4)$$

性質２及び３は、高階差分攻撃で必要な差分階数をＮ＋１から減らす性質であり、改良型高階差分攻撃で使用される[SMK97][MSK98]。さらに、関数 $E(X;K)$の入力Ｘを線形変換したもの $Z = T(X)$で置き換え、変数Ｚに関し、高階差分を取る事で高階差分攻撃の効率を上げる事も可能であり、これは定義１における、GF(2)^{n}の部分空間 $V^{(n)}$の選択のしかたに内包されている。また、$E(X;K)$が全単射関数の場合、次の性質が成り立つ。

性質４.

$E(X;K)$が全単射関数の場合、ブール代数次数はｎ－１であり、次式が成立する。

$$\Delta^{(n)} E(X \oplus \mathrm{A};K) = 0 \qquad (3.5)$$

この性質と、高階差分の線形性

性質５．

高階差分は⊕演算に関し、線形性を持つ。

$$\Delta^{(i)}(E(X;K) \oplus F(X;K')) = \Delta^{(i)}E(X;K) \oplus \Delta^{(i)}F(X;K') \quad (3.6)$$

を使い、高階差分攻撃を行う手法がある。ＳＰＮ構造の暗号に対する SQUARE 攻撃は、多くの場合 S-box の全単射性と性質４，５を使用して行われる[DKR97]。

３．２　攻撃方程式

図１に繰り返し型暗号の模式図を示す。$F(X)$は段関数であり、入力 Xを段鍵 K_i の制御のもと変換し、次段に出力する。高階差分攻撃では、暗号系の中間段の変数 H に関し、線形空間 $V^{(N)}$に関するＮ階差分が０(又は *const*)となる H及び $V^{(N)}$を何らかの方法で求める。その $V^{(N)}$の元を選択平文 P として入力するならば、H のＮ階差分が０(又は *const*)であることが保証されている。H を暗号文Ｃ側から、計算する関数を $G(C;K)$とするならば、次の攻撃方程式が成立する。

$$0 = \Delta^{(N)} H = \bigoplus_{C \leftarrow P \in V^{(N)}} G(C;K) \qquad (3.7)$$

この方程式を K に対し解くことで解読は行われる。この方程式に係わる鍵 K は、C から H を計算する時に関係する段鍵 K_i の全部又は一部である。この方程式は、高次代数方程式であり、解析的に解くことは困難である。以下、代表的な解法を３つ示す。

＜攻撃方程式総当たり攻撃＞変数 H 及び K の未知ビット数をそれぞれ$|H|$及び$|K|$と表すな

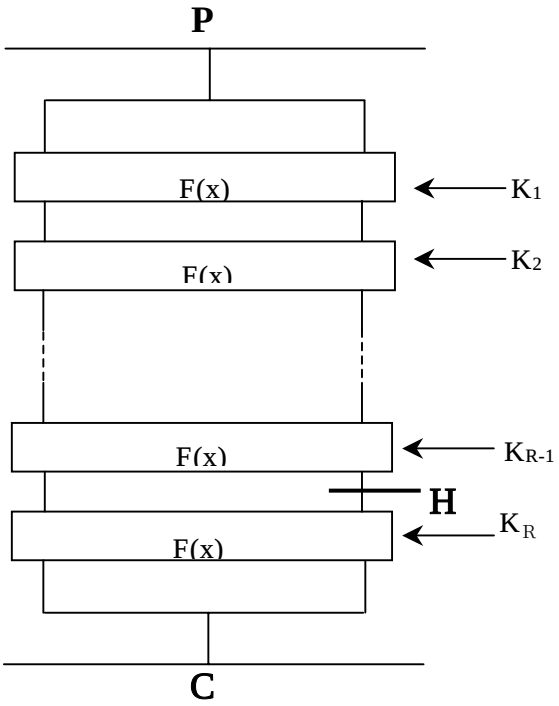

図１.暗号系模式図

らば、一つの偽鍵 K に対し式(3.7)が成立する確率は $2^{-|H|}$ であることから $M_1 = \left\lfloor (|K|+1) / |H| \right\rfloor$ 組[1]の高階差分に対し、式(3.7)をふるい式として検査する事により、真の鍵 K が定まる。この計算量 T_1 は、K を総当たりするならば、

$$T_1 = 2^{|K|} 2^N \sum_{i=0}^{M_1-1} 2^{-|H|i} \le 2^{N+|K|+1} \qquad (3.8)$$

回の G 関数計算である。必要な選択平文の最大組数は、M_1 組の線形部分空間 $V^{(N)}$ を共通部分無く取る場合であり、$M_1 2^N$ 組である。部分空間 $V^{(N)}$ の取り方に自由度があり、共通部分が許される場合は、線形部分空間 $V^{(N_1)}$ から $V^{(N)}$ を取り出す組み合わせは $\binom{N_1}{N}$ 通りあり、必要な選択平文の最小組数は、$\binom{N_1}{N} \ge M_1$ を満たす最小の N_1 に対し 2^{N_1} 組となる。

＜線形化攻撃＞　攻撃方程式(3.7)は、連立高次代数方程式であるが、それを K に関し、ブール多項式展開し、K の各ビットの積である高次項も一つの未知数と考えて線形化し、逆行列計算で、真の鍵 K を求める手法が効果的である[SMK97]。その時の独立な未知項の個数をＬとするならば、必要な N 階差分組数は、$M_2 = \left\lfloor L / |H| \right\rfloor$ であり、計算量は、逆行列計

[1] 偽鍵がふるい落とされるためには、生き残り偽鍵数の期待値（$2^{|K|}$-1）*$2^{-|H|M1}$ が十分小さい事が必要である。ここでは、その値が１未満となる組数 M_1 を採用した。

算の計算量[2]を無視すれば、

$$T_2 = 2^N M_2 L \qquad (3.9)$$

であり、必要な選択平文は最大$M_2 2^N$組、最小2^{N_2}組（ただし N_2は$\binom{N_2}{N} \geq M_2$を満たす最小値）となる。

＜線形化＋総当たり攻撃＞　一部の鍵を総当たりしながら、残りを線形化して解くことも可能であり、総当たり部分の鍵ビット数を$|K_3|$残り鍵部分に関し、ブール多項式展開したときの項数を L_3とする。$|K_3|$ビット仮定し、L_3個の未知項に対し、L_3+m本（$m \geqq 1$）の線形方程式を解けば、その方程式が不能か否かで仮定ビットの当否が判断できる。偽鍵に対し、線形方程式が不能にならない確率は$\left(2^{-L_3}\right)^m$と見積もる事ができ、$2^{|K_3|}2^{-L_3 m} << 1$なるL_3+m本の線形方程式を用意すれば偽鍵は、全て排除されるであろう。$m = \left\lfloor |K_3| \Big/ L_3 \right\rfloor$として、そのような線形方程式を用意するのに必要な、高階差分組数は$M_3 = \left\lfloor L_3 + m \Big/ |H| \right\rfloor$である。この時、計算量は

$$T_3 \leq 2^{N+|K_3|} \left\lfloor (L_3+1) \Big/ |H| \right\rfloor L_3 \qquad (3.10)$$

となる。ここで総当たり部分の鍵$|K_1|$ビットは、線形方程式が不能か否かで、ふるいにかけられる。そのため、高階差分組の及び計算量の見積もりにおいて、$L_3 \rightarrow L_3+1$と評価した。必要な選択平文は最大$M_3 2^N$組、最小2^{N_3}組（ただし N_3は$\binom{N_3}{N} \geq M_3$を満たす最小値）となる。

３．３　高階差分攻撃に係わる評価量

前節で述べたように、高階差分攻撃は、線形空間 $V^{(N)}$ や中間段の変数 Hを何らかの方法で求めることから始まる。最適な $V^{(N)}$を求めることは、例え 64 ビットブロック暗号であっても計算量的に不可能である。通常は、暗号系の構成部品に対し、ブール多項式次数や項数などの高階差分攻撃の立場の評価量を求め、それを基に暗号系の高階差分攻撃耐性を推定していく。

２節の評価(1)及び(2)では構成部品の次数及び項数を評価し、それをもとに、評価(3)で高階差分攻撃耐性を評価した。

部品の評価及びその過程で得られた特徴をもとに(3-1)では、適切な $V^{(N)}$を選び、代数次数の評価を行う。真の次数評価は、通常、計算量的に困難である為、多くの場合、形式的

---

[2] 逆行列計算の計算量は、$O(L^3)$である。L が大きい場合は無視できなくなる。この方法で、求めた計算量が鍵の総当たりに近い場合は、さらなる考察が必要である。

代数次数評価でそれを代用した。即ち、次数は積で上昇し、関係する変数ビット数を超えないとの条件で次数評価を行った。

評価(3-2)では、入力平文ビットから、8 ビット以下を変数として選ぶ高階差分の範囲で、計算機により最適な $V^{(N)}$の取り方を探索した。また、多くの暗号が 32 ビットを一つの小ブロックとして処理する構造を持つため、その小ブロック単位の 32 階及び 31 階差分に関し最適な $V^{(N)}$の取り方を計算機探索した。

評価(3-3)では、１対１写像性を持つ暗号の部分ブロックに着目し、１対１性が保証される段数を求め、SQUARE 型の高階差分攻撃耐性を評価した。

(3-6)では、(3-1)から(3-5)の結果をもとに、高階差分攻撃又は線形和攻撃耐性の評価を行った。平文ブロック長を$|P|$、秘密鍵のビット数を$|K|$として、解読に必要な選択平文組数が　$2^{|P|}$未満、かつ計算量が$2^{|K|}$回の段関数計算以下の場合、解読が可能と考えその段数を求めた。各暗号についてこれら評価量データは、付録 A－Ｉに示す。

４．　補間攻撃

補間攻撃[JK97]は、広い範囲の概念を含むが、その中で実際的なものは、１変数型補間攻撃であろう。そこでは、暗号系の部分関数をガロア体 $GF(q)$上の１変数多項式で表す。$GF(q)$の元 xから平文 Pへの写像 $p(x)$を適切に選び、中間段の変数 Hもガロア体 $GF(q)$の元と考える。平文 $p(x)$の暗号化過程を変数 Hまで考えると、xから Hへの写像は、ガロア体 $GF(q)$上の多項式関数

$$H = f_K(x) = \sum_{i=0}^{q-1} a(K)_i x^i \qquad (4.1)$$

と表すことができる。i次項係数$a(K)_i$は、秘密鍵Kの関数[3]であり、未知である。しかし、暗号系の解析により未知係数項数がN個と判っているならば、平文と Hの対 N 組に対し、Lagrange 補間により、その未知係数$a(K)_i$を推定できる。途中の段鍵を仮定し暗号文 C から逆算した値 Hの正当性（即ち、仮定した段鍵の真偽）は、N+1 組の(x,H)対で判断できる。従って、平文 $P=p(x)$および対応する暗号文 C が N+1 組与えられれば、段鍵が推定できる事になる。ガロア体 $GF(q)$の元の個数は q種類であり、N<q ならば、この攻撃に必要な平文・暗号文組が用意できる。

未知係数$a(K)_i$の間に、秘密鍵 K に依存しない線形従属性がある場合、推定すべき未知係数の個数は減りN’個となる。この N’個の未知係数を推定する攻撃法として、1 変数型補間攻撃を拡張したのが線形和攻撃である[A00]。この場合 N’+1 組の平文・暗号文組を使用する。Hを暗号文 C 側から、計算する関数を $G(C;K)$とし、ラグランジェ補間の計算量を無視するならば、解読計算量は

$$T_L = 2^{|H|}(N'+1) \qquad (4.2)$$

---

[3] 正確には、平文から Hまでの暗号化過程で影響を持つ段鍵 $K_j\{j=1,2,\ldots\}$の関数

回の G 関数計算量である。

最適な、ガロア体 $GF(q)$及び写像 $p(x)$を選び出すことは、計算量的に困難である。ここでは、平文 P を 8 ビット単位の小ブロック 8 個（64 ビット暗号）又は 16 個(128 ビット暗号)に区切り、その小ブロックをガロア体 GF(2^8)の多項式基底で表現された元と見なして、線形和攻撃耐性を文献[A00]の手法で調査した。結果を付録Ｊに示す。

５．　高階差分／補間攻撃耐性

５．１　64 ビットブロック暗号

CIPHERUNICORN-E、MISTY1、FEAL-NX、Hierocrypt-L1 の４暗号について調査し、結果は付録Ａ、Ｂ、Ｃ、Ｄ及びＪに示した。提案暗号に関し、高階差分／補間攻撃の立場で、問題のある暗号は、存在しない。各暗号に対し、高階差分／補間攻撃の立場で、必要平文組数が 2^{64} 未満、計算量が 2^{128} 未満で攻撃可能な最高段数及び仕様段数を表１に示す。攻撃可能段数は、実際に存在する高階差分特性に基ずく判断である。しかし、2^{64} 以上の計算量は、現在の計算機の能力からかけ離れたものであり、暗号の使用上問題が発生するものではない。

暗号名	攻撃可能段数	必要選択平文数	段関数計算量	仕様段数
CIPHERUNICORN-E	―	―	―	16
MISTY1(FL 無)	６段	2^{11}	2^{93}	―
MISTY1	5 段	2^{37}	2^{75}	8
FEAL-NX	9 段	2^{38}	2^{114}	32
Hierocrypt-L1	3.5 段（=7 層）	2^{37}	2^{117} *	6（=12 層）

*付録 D では 2^{137} の計算量であるが、部分総和法を使った場合、2^{117} と見積もれる。これは、文献[OSMMK]の結果を本報告書の計算量に換算したものである。

表１．　64 ビットブロック暗号の高階差分耐性

５．２　128 ビットブロック暗号

CIPHERUNICORN-A、Camellia、RC6、SC2000、MARS、Hierocrypt-3 の６暗号について調査し、結果は付録Ｅ、Ｆ、Ｇ、Ｈ、Ｉ、Ｄ及びＪに示した。提案暗号に関し、高階差分／補間攻撃の立場で問題のある暗号は、存在しない。256 ビット鍵を想定し、各暗号に対し、高階差分／補間攻撃の立場で、必要平文組数が 2^{64} 未満、計算量が 2^{256} 未満で攻撃可能な最高段数及び仕様段数を表２に示す。攻撃可能段数は、実際に存在する高階差分特性に基ずく判断である。しかし、2^{64} 以上の計算量は、現在の計算機の能力からかけ離れたものであり、暗号の使用上問題が発生するものではない。

暗号名	攻撃可能段数	必要選択平文数	段関数計算量	仕様段数
CIPHERUNICORN-A	―	―	―	16
Camellia(FL 無)	8 段	2^{14}	2^{214}	―
Camellia	6 段+FL	2^{51}	2^{255}	24
RC6	7 段	2^{9}	2^{226}	20
SC2000	8 段	2^{27}	2^{225}	22
MARS(core 部のみ)	8 段	2^{10}	2^{199}	16
Hierocrypt-3	3.5 段（=7 層）	2^{37}	2^{200} *	10（=20 層）

[L94] X.Lay,”Higher Order Derivatives and Differential Cryptanalysis,”Communications and Cryptography,pp.227-233,(1994)

[JK97] T.Jakobsen and L.R.Kunudsen,"The Interpolation Attack on Block Cipher.",FSE'97,LNCS 1267, pp.28-40,(1997)

[SMK97]T.Shimoyama, S.Moriai, T.Kaneko and S.Tsujii:"Improved Higher Order Differential Attack and Its Application to Nyberg-Knudsen's Designed Block Cipher",IEICE Trans.Vol.E82-A,No.9,pp.1971-1980,(1999)

[MSK98] S.Moriai, T.Shimoyama and T.Kaneko,”Higher Order Differential Attack of a CAST cipher,” FSE’98, LNCS 1372, pp.17-31 (1998)

[DKR97] J.Daemen, L.R.Knudsen and V.Rijmen, ”The block cipher Square”, FSE97, LNCS 1267, pp.149-165, (1997)

[A00] K.Aoki, "Practical Evaluation of Security against Generalized Interpolation Attack.", IEICE Trans.Vol. E83-A, No. 1, pp.33-38,(2000)

[OSMMK] 大熊健司、佐野文彦、村谷博文、本山雅彦、川村信一“ブロック暗号 Hierocrypt-3 および Hierocrypt-L1 の安全性について”,SCIS2001,11A-4,(2001)