# ブロック暗号における鍵生成関数の丸め差分特性について

多賀 文吾 ∗†　　田中 秀磨 †　　金子 敏信 ‡

∗ 警察大学校 〒 183-8558 東京都府中市朝日町 3-12-1

† 独立行政法人情報通信研究機構 〒 184-8795 東京都小金井市貫井北町 4-2-1
b.taga@nict.go.jp , hidema@nict.go.jp

‡ 東京理科大学 〒 278-8510 千葉県野田市山崎 2641
kaneko@ee.noda.tus.ac.jp

**あらまし** 2013 年に予定されている電子政府推奨暗号リストの改訂において、関連鍵攻撃に対する安全性が評価項目の一つになっている。しかし、現行リストの策定においては関連鍵攻撃に対する安全性評価が行われていない。本稿では、現行リスト掲載の 128bit ブロック暗号について、関連鍵攻撃に対する安全性評価の考察を示す。関連鍵攻撃は未知の 2 つの秘密鍵の差分を攻撃者が操作できると仮定する攻撃であるから、攻撃の耐性は鍵生成関数の差分特性から見積もられると考えられる。評価は丸め差分特性で行い、active S-box 数が最小となる差分経路を Viterbi アルゴリズムで探索した。その結果、CIPHERUNICORN-A は十分な計算量的安全性を有すると見積もられた。

# On the Truncated Differential Property of Generation Function of Extended Key in Block Ciphers

Bungo Taga∗†　　Hidema Tanaka†　　Toshinobu Kaneko‡

∗ National Police Academy, 3-12-1 Asahi-cho, Fuchu, Tokyo, 183-8558, JAPAN

†National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi, Koganei, Tokyo, 184-8795, JAPAN
b.taga@nict.go.jp , hidema@nict.go.jp

‡Tokyo University of Science, 2641 Yamazaki, Noda, Chiba, 278-8510 JAPAN
kaneko@ee.noda.tus.ac.jp

**Abstract** We considered the evaluation of security against related-key attack for 128bit block ciphers in the e-Government Recommended Ciphers List of Japan. We consider that security against related-key attack is evaluated from the differential property of generation function of extended key because related-key attack allows that the attacker can control differential between two secret keys. We evaluated the security by searching for the truncated differential path which has the minimnum number of active S-boxes using Viterbi algorithm. As a result, we found that CIPHERUNICORN-A is computationally secure among 128bit block ciphers in the list.

# 1 はじめに

関連鍵攻撃 [1] は、2009 年、米国政府標準暗号である AES[2] に対して具体的な攻撃法が発表され、鍵長 192bit 及び 256bit の AES に対して、鍵の全数探索よりも有効な攻撃手法であることが示された [7][8][15]。また、2013 年に予定されている電子政府推奨暗号の改訂にあたって、関連鍵攻撃に対する安全性が評価項目の一つになっている [10]。しかし、現行の電子政府推奨暗号リスト（以下「現行リスト」）の策定当時、関連鍵攻撃に対する安全性は評価の対象とはなっていなかった。

本稿では、現行リストに掲載されている鍵長 128bit の以下の５つのブロック暗号について、関連鍵攻撃に対する安全性評価の考察を行う。

**(i)** AES[2]（米国政府標準暗号）

**(ii)** Camellia[3]（日本電信電話株式会社、三菱電機株式会社）

**(iii)** CIPHERUNICORN-A[4]（日本電気株式会社）

**(iv)** Hierocrypt-3[5]（株式会社東芝）

**(v)** SC2000[6]（富士通研究所）

関連鍵攻撃は未知の２つの秘密鍵の差分を攻撃者が操作できると仮定する攻撃である。ブロック暗号の暗号化においては、鍵生成関数を用いて秘密鍵から生成された拡大鍵を使用する。したがって、関連鍵攻撃に対する安全性は、攻撃者がどの程度の確率で拡大鍵の差分を制御できるかについて計算することにより、評価できると考えられる。

この確率は、鍵生成関数の差分特性確率で見積もることができる [11]。しかし、差分特性確率を求めることは計算量的に困難であるため、本稿では S-box の入出力についての差分の有無（active S-box）のみに着目した丸め差分特性について考えることとした [15][16]。評価の手順は以下の通りである。

**(i)** S-box の最大差分確率を計算し、鍵の全数探索の計算量を超えるのに必要な active S-box 数を求める。

**(ii)** Viterbi 探索により active S-box 数が最小となる経路と active S-box 数を計算する。

**(iii)** **(i)** と **(ii)** で求めた active S-box 数と比較する。

丸め差分は差分値そのものは無視して差分の有無のみに着目する方法であるので、攻撃者有利な評価である [12][13][14]。また、排他的論理和や定数加乗算などの鍵生成関数内部の関数においても、攻撃者に有利な差分伝播が確率 1 で生じるとして計算している。このため、計算結果から直ちに関連鍵攻撃が実行可能であるとは言えないが、関連鍵攻撃に対する安全性の概算的評価や他の暗号アルゴリズムとの相対的な評価を行うことは可能である。

本稿の構成は以下の通りである。第 2 節では、鍵生成関数に対する差分制御可能性の指標となる丸め差分特性と、active S-box 数が最小となる差分経路の探索アルゴリズムとして使用する Viterbi 探索 [17] について説明する。第 3 節は、経路探索の計算で使用する差分伝播のルールを具体例で示す。第 4 節では計算結果を、第 5 節では、この結果から考察される関連鍵攻撃に対する安全性について述べる。第 6 節でまとめと今後の課題について述べる。

# 2 丸め差分特性と Viterbi 探索

## 2.1 丸め差分特性

丸め差分は、複数 bit の差分の有無を 1bit で表現し、差分値そのものは無視する方法である。差分情報を扱わないことで精度が欠けるが、特性を算出する計算量は大きく減少する。このため、丸め差分特性確率は、差分特性確率を求めることが計算量的に困難である場合に用いられ、概算としての差分特性確率の評価を可能にする [11][12][13][14][15][16]。

本稿では、鍵生成関数で使用されている S-box の入出力差分の有無を 1bit に丸めた差分特性で評価する。具体的には、AES、Camellia、CIPHERUNICORN-A 及び Hierocrypt-3 は 8bit 入出力の S-box を使用しているため、8bit の差分の有無を 1bit で表し、SC2000 は 6bit

及び 5bit 入出力の S-box を使用しているため、6bit または 5bit の差分の有無を 1bit で表す丸め差分を考えることとした。安全性評価は、差分特性確率の最大値、すなわち、active S-box 数の最小値を探索することにより行う。

### 2.2 Viterbi 探索

Viterbi 探索は、ある条件の下で最適な経路を探索するアルゴリズムであり、誤り訂正検出符号の一種である畳込み符号の復号などに用いられる [17]。active S-box 数が最小になる鍵生成関数の差分経路の探索では、まず、各ラウンドでの差分値を状態と考えてトレリス線図を描く。次に、ある中間状態までの経路のうち active S-box 数が最小となる経路を生き残り経路として、小さいラウンドから順に探索していく。これにより、最終的に鍵生成関数の全ラウンドについて active S-box 数が最小となる経路を求めることができる。

今回の探索では、初期状態及び終状態について制限はなく、任意の値が可能であるとしている。

## 3 差分伝播のルール

本節では、排他的論理和及び定数加乗算等、鍵生成関数内部で使用されている関数により、差分がどのように伝播するかについて、CIPHERUNICORN-A を例に述べる [4]。

図 1 に、鍵長 128bit の CIPHERUNICORN-A の鍵生成関数の構造を示す。鍵生成関数は 156 ラウンドで構成されており、各ラウンド毎に MT 関数が左側 64bit に対して作用した後、32bit ずつ左巡回シフトが行われる。

MT 関数は図 2 に示すように $2^{32}$ を法とする定数 0x01010101 による乗算、$T_0$ 関数及び排他的論理和から構成されている。

図 3 に定数 0x01010101 による乗算及び $T_0$ 関数の構造を示す。定数 0x01010101 による乗算は、$2^{32}$ を法とする加算で表すことができる。また、$T_0$ 関数は 4 種類の 8bit 入出力 S-box から構成され、全体として 8bit 入力 32bit 出力関数

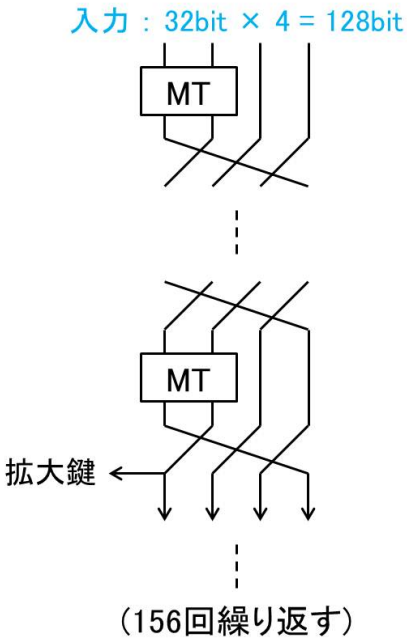


図 1: CIPHERUNICORN-A の鍵生成関数

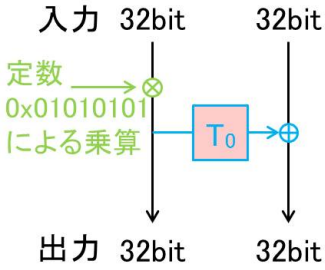


図 2: CIPHERUNICORN-A の MT 関数

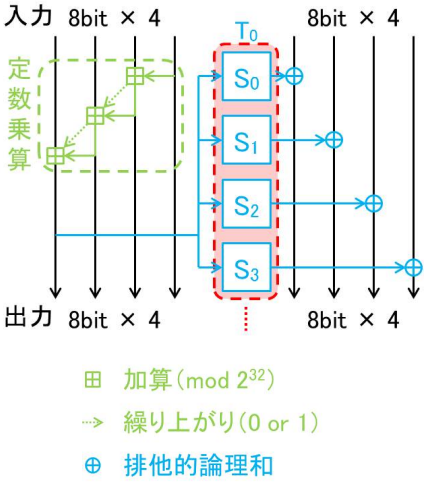


図 3: MT 関数（定数乗算と $T_0$ 関数）の構造

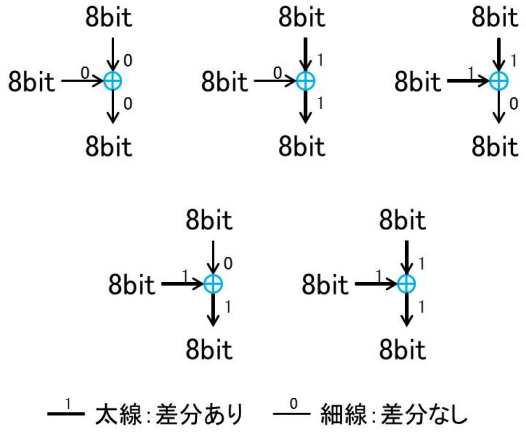


図 4: 排他的論理和の差分伝播

となっている。各 S-box が 8bit 入出力関数であるため、CIPHERUNICORN-A では、2.1 節で述べたように 8bit の差分の有無を 1bit で表す丸め差分について考えることとした。

### 3.1 $T_0$ 関数による差分伝播

$T_0$ 関数は、図 3 から、入力差分が 0 の場合は 4 つの S-box からの 8bit 出力差分はすべて 0、入力差分が非 0 の場合は 4 つの S-box からの 8bit 出力差分がすべて非 0 であることがわかる。また、$T_0$ 関数全体を一つの S-box と見なしたとき、入力値の差分が非 0 の場合の最大差分確率は $2^{-7}$ であることが数値計算により求められる。

### 3.2 排他的論理和による差分伝播

排他的論理和の差分伝播は、差分が非 0 の場合を 1、差分が 0 の場合を 0 で表したとき図 4 の 5 つの可能性が考えられる。本稿では、攻撃者にとって都合の良い、すなわち、active S-box 数が最小となるような差分伝播が確率 1 で生じるとした。したがって、実際には生じ得ない差分経路が選択される可能性があり、攻撃者有利な評価を行っている。

表 2: 計算結果

| アルゴリズム | a | b | c |
|---|---|---|---|
| AES | 4 | 22 | $2^{-6}$ |
| Camellia | 5 | 22 | $2^{-6}$ |
| CIPHERUNICORN-A | 37 | 19 | $2^{-7}$ |
| Hierocrypt-3 | 6 | 22 | $2^{-6}$ |
| SC2000 | 12 | 32 | $2^{-4}$ |

a：経路探索から導出された active S-box 数
b：全数探索の計算量を超えるのに必要な active S-box 数
c：S-box の最大差分確率

### 3.3 定数乗算による差分伝播

$2^{32}$ を法とする定数 0x01010101 の乗算を 32bit 入出力関数と考え、入出力 32bit を 4bit に丸めたときの差分伝播を表 1 に示した。表 1 で、縦は入力 32bit の丸め差分 (4bit)、横は出力 32bit の丸め差分 (4bit) を表す。排他的論理和の場合と同様に、active S-box 数が最小となるような差分伝播が確率 1 で生じるとした。

## 4 計算結果

鍵長 128bit の場合について、第 2 節及び第 3 節で述べた探索方法で最小となる active S-box 数を計算した結果を表 2 に示す。

この結果から、CIPHERUNICORN-A については、攻撃者は全数探索より少ない計算量で拡大鍵を操作することはできない。すなわち、関連鍵攻撃に対して十分な計算量的安全性を有していると言える。一方、他のアルゴリズムについては、b 欄の全数探索の計算量を超えるのに必要な active S-box 数が、a 欄の経路探索から導出された active S-box 数を大きく上回っている。これは、攻撃者が全数探索よりもかなり少ない計算量で拡大鍵を操作できる可能性があることを意味している。ただし、この評価はあくまでも差分特性確率の上界を示しているのであり、実際の経路の存在を保証するものではない。

表 1: $2^{32}$ を法とする定数 0x01010101 の乗算による差分伝播

| 入＼出 | 0x0 | 0x1 | 0x2 | 0x3 | 0x4 | 0x5 | 0x6 | 0x7 | 0x8 | 0x9 | 0xA | 0xB | 0xC | 0xD | 0xE | 0xF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0x0 | ○ | | | | | | | | | | | | | | | |
| 0x1 | | | | | | | | | | | | | | | | ○ |
| 0x2 | | | | | | | | | | | | | | | ○ | |
| 0x3 | | | | | | | | | | | | | | ○ | | ○ |
| 0x4 | | | | | | | | | | | | | ○ | | | |
| 0x5 | | | | | | | | | | | | ○ | | | | ○ |
| 0x6 | | | | | | | | | | | ○ | | | | ○ | |
| 0x7 | | | | | | | | | | ○ | | ○ | | ○ | | ○ |
| 0x8 | | | | | | | | | ○ | | | | | | | |
| 0x9 | | | | | | | | ○ | | | | | | | | ○ |
| 0xA | | | | | | | ○ | | | | | | | | ○ | |
| 0xB | | | | | | ○ | | ○ | | | | | | ○ | | ○ |
| 0xC | | | | | ○ | | | | | | | | ○ | | | |
| 0xD | | | | ○ | | | | ○ | | | | ○ | | | | ○ |
| 0xE | | | ○ | | | | ○ | | | | ○ | | | | ○ | |
| 0xF | | ○ | | ○ | | ○ | | ○ | | ○ | | ○ | | ○ | | ○ |

無印：確率 0　○：確率 $\neq 0$

## 5　関連鍵攻撃と本結果との関係

第 4 節の結果から、CIPHERUNICORN-A は、関連鍵攻撃に対して十分な計算量的安全性を有していることがわかった。一方、他のアルゴリズムについては、十分な安全性を有しているか、または関連鍵攻撃が可能であるかを明確に述べることはできない。しかし、現在最も解析が行われている暗号アルゴリズムの一つである AES との比較において、関連鍵攻撃に対する耐性を本計算結果から述べることは可能である [7][8][9][15]。

本稿では、表 2 の a 欄と b 欄の active S-box 数の比を比較することを考える。AES では a 欄の active S-box 数が 4、b 欄の active S-box 数が 22 であるのに対し、Camellia では a 欄の active S-box 数が 5、b 欄の active S-box 数が 22 である。このことから、Camellia は AES よりも、攻撃者が拡大鍵を操作できる度合いが小さく、関連鍵攻撃に対してより強い耐性を有すると推測できる。他のアルゴリズムについても、a 欄と b 欄の active S-box 数の比を比較することにより、AES よりも関連鍵攻撃に対してより強い耐性を有すると推測できる。

鍵長 192bit 及び 256bit の AES に対する関連鍵攻撃は、2009 年に示されたが、鍵長 128bit の AES に対して、全ラウンドを解読する関連鍵攻撃は示されていない。このことから、鍵長 128bit の場合、他の 4 つのアルゴリズムに対しても関連鍵攻撃は容易ではないと考えられる。

## 6　まとめ

本稿では、電子政府推奨暗号リストに掲載されている鍵長 128bit の 5 つのブロック暗号について、鍵生成関数の差分経路を探索することにより、関連鍵攻撃に対する安全性の概算評価を行った。その結果、計算量的安全性を有しているのは CIPHERUNICORN-A であることがわかった。また、米国標準暗号で、現在最も多く利用及び解析されている暗号アルゴリズムの一つである AES と比較した場合、他の 4 つのアルゴリズムは関連鍵攻撃に対してより強い耐性

を有すると評価できることがわかった。

本稿では鍵長 128bit の場合のみ評価を行ったが、今後は、鍵長 192bit 及び 256bit の場合の評価及び等価鍵の有無の検証が課題である。

## 参考文献


[1] E. Biham: New types of cryptanalytic attacks using related keys. J. Cryptology, 7(4): 229-246, 1994.

[2] National Institute of Standards and Technology: Advanced encryption standard (AES). FIPS 197, November 2001.

[3] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, Toshio Tokita: Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. Selected Areas in Cryptography 2000 LNCS 2012: 39-56

[4] Yukiyasu Tsunoo, Hiroyasu Kubo, Hiroshi Miyauchi, Katsuhiro Nakamura: 電子情報通信学会技術研究報告. ISEC 情報セキュリティ 100(76): 23-46, 2000-05-18

[5] Kenji Ohkuma, Hirofumi Muratani, Fumihiko Sano, Shin-ichi Kawamura: The Block Cipher Hierocrypt. Selected Areas in Cryptography 2000 LNCS 2001: 72-88

[6] Takeshi Shimoyama, Hitoshi Yanami, Kazuhiro Yokoyama, Masahiko Takenaka, Kouichi Itoh, Jun Yajima, Naoya Torii, Hidema Tanaka: The Block Cipher SC2000. FSE 2001 LNCS 2355: 312-327

[7] Alex Biryukov, Dmitry Khovratovich: Related-Key Cryptanalysis of the Full AES-192 and AES-256. ASIACRYPT 2009 LNCS 5912: 1-18

[8] Alex Biryukov, Dmitry Khovratovich, Ivica Nikolić: Distinguisher and Related-Key Attack on the Full AES-256. CRYPTO 2009 LNCS 5677: 231-249

[9] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, Adi Shamir: Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds. EUROCRYPT 2010 LNCS 6110: 299-319

[10] CRYPTREC ホームページ
`http://www.cryptrec.go.jp/`

[11] Eli Biham, Adi Shamir: Differential Cryptanalysis of DES-like Cryptosystems (Extended Abstract). CRYPTO 1990 LNCS 537: 2-21

[12] Lars R. Knudsen, Thomas A. Berson: Truncated Differentials of SAFER. FSE 1996 LNCS 1039: 15-26

[13] 関春樹、金子敏信, “差分解読法による GOST の解読実験”, 信学会技術研究報告, ISEC98-80, pp 61-66, 1999.

[14] Seonhee Lee, Seokhie Hong, Sangjin Lee, Jongin Lim, Seonhee Yoon: Truncated Differential Cryptanalysis of Camellia. ICISC 2001 LNCS 2288: 32-38

[15] Alex Biryukov, Ivica Nikolić: Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others. EUROCRYPT 2010 LNCS 6110: 322-344

[16] Mitsuru Matsui: On Correlation Between the Order of S-boxes and the Strength of DES. EUROCRYPT 1994 LNCS 950: 366-375

[17] Andrew J. Viterbi: Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. IEEE Transactions on Information Theory 13(2): 260-269, April 1967