コンピュータセキュリティ 10−13
(2000. 7. 25)

CAST-256の差分解読

関 春樹　金子 敏信†

通信・放送機構 横浜リサーチセンター
〒221-0031 横浜市神奈川区新浦島町1−1−32ニューステージ横浜

†東京理科大学 理工学部電気工学科
〒278-8510 千葉県野田市山崎2641

E-mail: hseki@yokohama.tao.go.jp, †kaneko@ee.noda.sut.ac.jp

あらまし ブロック暗号CAST-256はCAST-128を基本に設計され、AES Round 1の候補として提案された。本論文では、9 quad-roundのCAST-256に対する差分解読について報告する。ラウンド関数の1つは、高確率の非零差分 → 零差分特性を持つ。弱鍵の場合には、この特性が暗号全体の差分解読に適用できる。9 quad-roundのCAST-256のサブ鍵79ビットが、2^{123}個の選択平文と、約2^{100}の計算量で求められる。この時、弱鍵の存在する確率は2^{-35}である。

キーワード ブロック暗号，CAST-256，差分解読，AES

Differential Attack on CAST-256

Haruki SEKI　Toshinobu KANEKO†

Telecommunications Advancement Organization of Japan
1-1-32 Shin'urashima-cho, Kanagawa-ku, Yokohama 221-0031 Japan

†Department of Electrical Engineering, Science University of TOKYO
2641 Yamazaki Noda, Chiba, 278-8510 Japan

Abstract An block cipher CAST-256 based on CAST-128 was a candidate algorithm for the AES Round 1. In this paper we present a differential attack on CAST-256 reduced to 9 quad-rounds. One of the three round functions of CAST-256 has differential characteristics, which a non-zero inputxor result in a zero outputxor, with high probability. We also show that CAST-256 has weak keys with respect to differential attack. Thus CAST-256 reduced to 9 quad-rounds can be attacked using 2^{123} chosen plaintexts in the case of differentially weak keys. The time complexity is about 2^{100} encryptions.

key words Block cipher , CAST-256, differential attack, AES

1 はじめに

C.M.Adamsはブロック暗号 CAST-256[1]をAES Round 1の候補として提案した。この暗号は64bit入出力の CAST-128[2]を基本に設計されている。即ち、CAST-128と同じ4種の8 × 32 S-boxと、3種のラウンド関数を採用している。全体構造は、CAST-128がFeistel型に対して、CAST-256は入出力長を128bitに拡張するために Incomplete Feistel network 型としている[3]。Boomerang attackが、4 quad-roundのCAST-256の解読に適用されている[4]。本稿では9 quad-roundのCAST-256の差分攻撃について報告する。

差分攻撃はE.Biham等により提案され、多くの暗号に汎用的に適用出来る強力な攻撃法である[5]。攻撃の成否は高確率の差分特性が見つかるか否かによって決定される。特に、非零差分 → 零差分となる特性をラウンド関数が持つ場合は、Activeなラウンドを少なくし、暗号全体での差分特性確率が大きくなる事が期待できる。DESやLOKI97等の暗号の解読に効果を発揮している[5, 6]。

本稿では、最初にCAST-256のラウンド関数の差分特性について述べる。CAST-256のラウンド関数は、異なる演算系を組合わせて使用しており、差分攻撃、線形攻撃に対する強度や、CAST familyの一部に適用された高階差分攻撃[7]に対する強度がXORのみを演算とした場合に比べ向上していると考えられている。しかし、差分攻撃に関する限り、必ずしも強度が向上していないことを示す。即ち、高確率の非零差分 → 零差分特性が一部のラウンド関数で見つかった。これは、XORのみを用いた簡易型ラウンド関数では見つからなかったものである。ラウンド関数の持つこの様な差分特性の数が、randomに生成されたS-boxから構成されるラウンド関数において期待される数[8]に比べ多い事も示す。

次に、9 quad-round のCAST-256に差分攻撃を適用した。ラウンド関数の持つ前記の差分特性を利用すると、鍵依存ローテーションの一部を省いた9 quad-round のModified CAST-256の9 quad-round目の鍵の74ビットが、2^{123}の選択平文と、約2^{95}の計算量で求められる。また、オリジナルの CAST-256にもこの攻撃を拡張出来る。1~8 quad-round の一部のラウンド関数の鍵依存ローテーション値が等しくなる鍵を弱い鍵と定義する。この場合には9 quad-round のCAST-256のサブ鍵79ビットが、2^{123}個の選択平文と、約2^{100}の計算量で求められる。9 quad-round の CAST-256では2^{-35}という高い確率でこの弱い鍵がある。

本稿の構成は以下である。第2節では、暗号アルゴリズムの概要を述べる。第3節では、ラウンド関数の差分特性について述べる。第4節では、暗号全体の差分解読について述べる。最後に第5節でまとめる。

2 CAST-256のアルゴリズム

図 1に示すように全体は Incomplete Feistel network 構造[3]である。入出力ブロック長は128 bit、鍵長は128 ~ 256 bit、段数は12 quad-round(48 round)である。

S-box： CAST-256 は4種の8 × 32 S-box (S_1, S_2, S_3, S_4)を使っている。これらはCAST-128と同じものである。

ラウンド関数： CAST-128と同じ3種のラウンド関数f_1, f_2, f_3を使っている。その基本構造を図 2に示す。k_mは 32bitラウンド鍵、k_rは 5bitラウンド鍵である。

それぞれのラウンド関数は以下で定義される。ここで、$I = I_a \| I_b \| I_c \| I_d$($I_a, I_b, I_c, I_d$は 8bitデータ)。

$$
\begin{aligned}
f_1(D, k_r, k_m)&: I = (k_m + D)\lll k_r \\
&\quad O = \big((S_1[I_a] \oplus S_2[I_b]) - S_3[I_c]\big) + S_4[I_d] \\
f_2(D, k_r, k_m)&: I = (k_m \oplus D)\lll k_r \\
&\quad O = \big((S_1[I_a] - S_2[I_b]) + S_3[I_c]\big) \oplus S_4[I_d] \\
f_3(D, k_r, k_m)&: I = (k_m - D)\lll k_r \\
&\quad O = \big((S_1[I_a] + S_2[I_b]) \oplus S_3[I_c]\big) - S_4[I_d]
\end{aligned}
$$

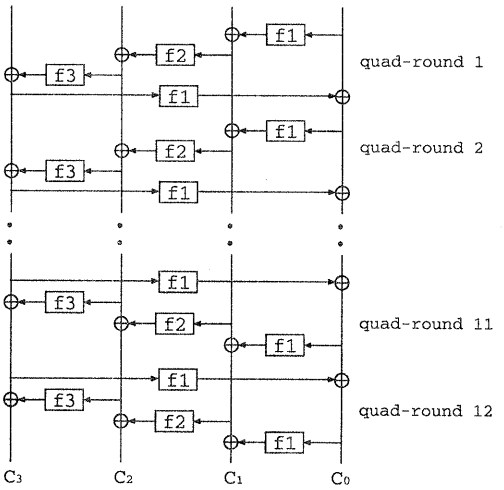

図 1: CAST-256のアルゴリズム

Quad-round 関数： 前半の第i forward quad-round $\beta \leftarrow Q_i(\beta)$ は以下で定義される。ここで、$\beta = A\|B\|C\|D$(A, B, C, Dは32bitデータ)。

- $C = C \oplus f_1(D, k_{r_0}^{(i)}, k_{m_0}^{(i)})$
- $B = B \oplus f_2(C, k_{r_1}^{(i)}, k_{m_1}^{(i)})$
- $A = A \oplus f_3(B, k_{r_2}^{(i)}, k_{m_2}^{(i)})$
- $D = D \oplus f_1(A, k_{r_3}^{(i)}, k_{m_3}^{(i)}) \qquad i = 1 \sim 6$

後半の第i reverse quad-round $\beta \leftarrow \overline{Q}_i(\beta)$ も同様に定義される。

全体の暗号化： $Enc = Q_1 \circ \cdots \circ Q_6 \circ \overline{Q}_7 \circ \cdots \circ \overline{Q}_{12}$

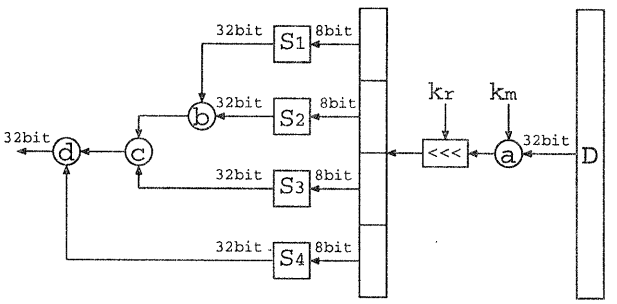

図 2: ラウンド関数

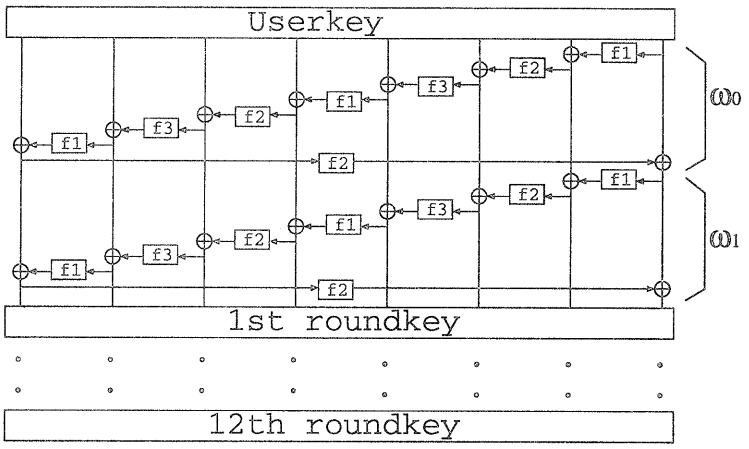

図 3: 鍵スケジュール

鍵スケジュール： 図 3に示す通りである。マスタ鍵Kを入力として暗号化と同じラウンド関数を使ってラウンド鍵が生成される。A, B, C, D, E, F, G, Hはそれぞれ32bitデータとし、$\kappa = A\|B\|C\|D\|E\|F\|G\|H$とする。この時、図中の一連の操作$\omega_{2i-1}(\kappa)(i = 1 \sim 12)$の出力から以下の様にラウンド鍵が生成される。ここで、$5LSB$は下位5bitをデータとする処理である。

$$k_{r_0}^{(i)} = 5LSB(A),\ k_{r_1}^{(i)} = 5LSB(C),\ k_{r_2}^{(i)} = 5LSB(E),\ k_{r_3}^{(i)} = 5LSB(G)$$
$$k_{m_0}^{(i)} = H,\ k_{m_1}^{(i)} = F,\ k_{m_2}^{(i)} = D,\ k_{m_3}^{(i)} = B$$

3 ラウンド関数の差分特性

本節では、ラウンド関数の差分特性について述べる。各ラウンド関数は異なる演算系を組合わせて使用しており、差分攻撃、線形攻撃に対する強度や、5段の簡易型CAST-128に適用された高階差分攻撃[7]に対する強度がXORのみを演算とした簡易型ラウンド関数に比べ向上していると考えられている。しかし、差分攻撃に関する限り、強度が必ずしも向上していないことを示す。

即ち、f_2ラウンド関数が2^{-15}という高確率の$\alpha \neq 0 \rightarrow 0$特性を持っている。これを3.1に示す。

更に、$\alpha \neq 0 \rightarrow 0$特性の数が、randomに生成したS-boxで構成されるラウンド関数において期待される数[8]に比べ、多い事も3.2で示す。

3.1 $\alpha \neq 0 \rightarrow 0$の確率

鍵依存ローテーションを省略したラウンド関数において、Active S-box 数が2の場合の$\alpha \neq 0 \rightarrow 0$特性を考える。

f_1, f_3関数では、演算aが$+, -$なので、高確率な特性を期待できないと思われる。そこでf_2関数について調べた。Active S-box 数が2となる組み合わせ6通りの内、以下の3通りの組み合わせを調べた[1]。

- f_2関数のS_1, S_2, S_3の何れか2個の組合わせ3通り

[1]残りの3通りの組み合わせについては計算量が大きい事から、今回は検討していない。今後の課題である。

以下に示す3つの$\alpha \neq 0 \rightarrow 0$特性が見つかった[2]。

$$f_2\text{関数}: Prob\{0000e0f7_x \rightarrow 00000000_x\} = 2^{-15}$$
$$Prob\{006a0069_x \rightarrow 00000000_x\} = 2^{-15}$$
$$Prob\{00e300f7_x \rightarrow 00000000_x\} = 2^{-15}$$

CAST design procedure [9]に基づく最も簡単な仕様であるXORのみを演算としたラウンド関数では、Active S-box 数が2の場合は$\alpha \neq 0 \rightarrow 0$特性が見つからなかった。異なる演算系をラウンド関数に採用したためにかえってこの差分が生じてしまったといえる。

3.2 ラウンド関数で生じる$\alpha \neq 0 \rightarrow 0$の数について

文献[8]ではxorテーブルの分布を、random に生成した S-box で構成される簡易型ラウンド関数(即ち、演算aと鍵依存ローテーションを省略し、残りの演算b, c, dが全てxor)について調べている。$\alpha \neq 0 \rightarrow 0$の数の期待値は、Active S-box 数が 2 となる 6 通りの全ての組合わせを考えた時 1.5 個と見積もっている。1 通り当たりでは0.25 個である。

一方、f_2関数では3通りのS-boxの組合わせで 3 個、即ち1 通り当たりでは1.0 個である。これは、文献[8]での期待値の約4倍と非常に多い出現率である[3]。表1に結果を纏める。

表 1: $\alpha \neq 0 \rightarrow 0$の出現数比較(Active S-box の組合わせ1 通り当たり)

	文献[8]の見積もり	CAST-256のf_2関数
出現個数	0.25	1.0

差分攻撃に有利な$\alpha \neq 0 \rightarrow 0$に関する限り、random に生成した S-box で構成されたラウンド関数に比べ改善されているとは言えない。

4 CAST-256の差分解読

本節では、9 quad-round のCAST-256の差分解読について述べる。4.1では、鍵依存ローテーションの一部を除いた9 quad-round のModified CAST-256で、2^{123}個の選択平文と、約2^{95}の計算量で最終 quad-round の鍵の一部74ビットを求められる事を示す。4.2では、4.1の差分攻撃が適用できるという意味で弱い鍵がある事を示す。これらの differentially weak key は2^{-35}の確率で存在し、この場合2^{123}個の平文と、2^{100}の計算量で最終 quad-round の鍵の一部74ビットとローテーション鍵5ビットが求められる事を示す。

4.1 Modified CAST-256の解読

最終 quad-round 以外の f_2関数のみから鍵依存ローテーション $(k_{r_1}^{(i)}, i = 1 \sim 8)$ を除いたModified CAST-256を考える。

特性：

3.1で求めたf_2ラウンド関数の$\alpha \neq 0 \rightarrow 0$特性の1つを用いると、次の 1 quad-round 繰り返し特性が実現出来る。

[2]入力値の組合わせは、S_1, S_2で$(23_x, ad_x)$と$(d4_x, 4d_x)$、S_1, S_3で$(e7_x, 26_x)$と$(8e_x, 4c_x)$及び$(4b_x, 3f_x)$と(bc_x, dc_x)。

[3]加算や減算の場合の差分確率は、XORの場合に対して$\frac{1}{2}$になる代わりに、生じる差分の数は2倍になる。それを加味しても出現率は大きくなっている。

$$Prob\{00000000000000000000e0f700000000_x \rightarrow 00000000000000000000e0f700000000_x\} = 2^{-15}$$

8 quad-round での差分特性確率は2^{-120}となり、9 quad-round のModified CAST-256に 1 quad-round attack が適用出来る。

S/N比：

次で定義されるS/N比を計算する [5]。

$$S/N = \frac{2^k \times p}{\alpha \times \beta}.$$

$k =$ 解読対象の鍵ビット数

$p =$ 差分特性確率

$\alpha =$ 1 ペアから推定される鍵数

$\beta = Wrong\ pair$の排除後に解析対象ペアが残る確率 (1)

各値は以下になる。ここでkは最終 quad-round のf_1, f_2関数のマスク鍵とローテーション鍵の合計である。

$$k = 74, \alpha = 2^{42}, \beta = 2^{-96}$$

これらを代入すると、$S/N = p \times 2^{128} = 2^8$ が得られる。S/Nが大きい事から、選択平文が約2^{123}(ペア数は2^{122})あれば最終 9 quad-round 目のf_1, f_2関数の鍵74bitを求める事が出来る。Wrong pair の排除後に$2^{123} \times 2^{-96} = 2^{27}$個の平文が残る。

鍵探索：

手順は以下である。

(1) f_1関数の鍵候補loop:
9 quad-round 目のf_1関数の鍵$k_{m_0}^{(9)}, k_{r_0}^{(9)}$を$0 \sim 2^{37} - 1$まで変化させ、以下の処理を繰り返す。

(2) 残った暗号文ペアloop：
排除後に残った2^{26}組の暗号文$CT = CT_3 \| CT_2 \| CT_1 \| CT_0$、$CT' = CT_3 \| CT_2' \| CT_1 \oplus 0000e0f7_x \| CT_0$の全てに対して、以下の処理を繰り返す。

(3) f_1関数出力候補計算：
出力候補Z_1を$f_1(CT_0, k_{r_0}^{(9)}, k_{m_0}^{(9)})$により計算する。

(4) f_2関数の入力候補計算：
入力候補ペアY_2, Y_2'を以下で計算する。

$$Y_2 = Z_1 \oplus CT_1, \qquad Y_2' = Z_1 \oplus CT_1 \oplus 0000e0f7_x$$

(5) f_2関数の鍵候補loop：
9 quad-round 目のf_2関数の鍵$k_{m_1}^{(9)}, k_{r_1}^{(9)}$を$0 \sim 2^{37} - 1$まで変化させ、以下の処理を繰り返す。

(6) f_2関数出力候補計算：
f_2関数の出力候補Z_2とZ_2'を$f_2(Y_2, k_{r_1}^{(9)}, k_{m_1}^{(9)})$と$f_2(Y_2', k_{r_1}^{(9)}, k_{m_1}^{(9)})$で計算する。

(7) 鍵カウント：
次式が成り立つ場合は、$k_{m_1}^{(9)}$と$k_{r_1}^{(9)}$の鍵値のカウンタを1増やす。

$$Z_2 \oplus CT_2 = Z_2' \oplus CT_2'.$$

カウント値が4であれば、この時の鍵を採用して処理を終了する。

メモリ量と計算量：

必要なメモリ量と計算量は次の様になる。

メモリ： 約2^{37}バイト。
フェーズ(7)で使う$k_{m_1}^{(9)}, k_{r_1}^{(9)}$の鍵カウンタテーブルのために$2^{37}$バイト。

計算量： 約2^{95}の暗号化処理。
フェーズ(6)の計算量が殆ど。平均で$2^{37} \times 2^{27} \times 2^{37}/2 = 2^{100}$の$f_2$の計算。9 quad-roundのCAST-256は$9 \times 4 = 36$回のラウンド関数計算と等価である。よって、この攻撃は平均で2^{95}の暗号化処理となる。

4.2 CAST-256の解読

Differentially weak keys：

8 quad-roundまでの8個のf_2関数の鍵ローテーション値$k_{r_1}^{(i)}(i = 1 \sim 8)$が全て等しく$k_{r_1}$であれば、次の1 quad-round繰り返し特性が実現出来る。

$$00000000_x \| 00000000_x \| 0000e0f7_x >\!>\!> k_{r_1} \| 00000000_x \rightarrow$$
$$00000000_x \| 00000000_x \| 0000e0f7_x >\!>\!> k_{r_1} \| 00000000_x$$

この様な条件が成り立つ鍵をDifferentially weak keysと定義する。Differentially weak keysが生じる確率は2^{-35}である[4]。

差分解読：

Differentially weak keysが成り立っているとする。攻撃は以下の手順で行われる。

(1) 平文の収集:
平文の第2ワードの32bitが相異なる値を持ち、他の3ワードの96bitが固定された2^{32}個の平文の集合を集める。これをstructureと呼ぶ事にする。2^{91}個のstructure(2^{123}個の平文)を集めて、以下の処理を行う。

(2) k_{r_1}の候補iのloop($i = 0 \sim 31$):
第2ワードの32bitの差分が$0000e0f7_x >\!>\!> i$となる平文ペアを集める。1つのstructureは2^{31}個のペアを、そして2^{91}個のstructureは2^{122}個のペアを生成出来る。

(3) 鍵探索:
4.1で示した攻撃を実行する。カウント値が4の鍵値があれば、それを採用し攻撃を終了する。

平均でk_{r_1}の候補iの16通りについて上記の処理を行えば、9 quad-round目のf_1とf_2の鍵74bitと5bitのk_{r_1}を求める事が出来る。以上から、$2^{-35} \times 2^{\text{鍵ビット数}}$の鍵空間については、$2^{123}$個の平文があれば、約$2^{100}$の計算量で攻撃が成功する。

[4]実験値はこれを裏付けた。

CAST-128との比較

上で述べてきた差分解読をCAST-128へ適用する。CAST-128は16段のFeistel構造である。各ラウンドはf_1, f_2, f_3ラウンド関数を順番に使用している。そのためf_2ラウンド関数の$\alpha \neq 0 \rightarrow 0$特性を用いた2 round繰り返し特性が繋がらず、5段程度の解読しか出来ない[5]。この事から、CAST-128の差分攻撃に対する強度が、CAST-256にうまく引き継げたと必ずしも言えない。

5 まとめ

本稿では9 quad-roundのCAST-256の差分攻撃について報告した。

まず、差分攻撃に対するラウンド関数の強度について述べた。3種のラウンド関数の内の1つf_2関数では、XORのみを演算として用いた簡易型ラウンド関数では見つからなかった非零差分 $\rightarrow$ 零差分が生じている。その差分確率は2^{-15}という高い値になっている。又、非零差分 $\rightarrow$ 零差分の出現する数が、randomに生成したS-boxで構成されたラウンド関数で期待される値[8]に比べ4倍程度大きくなっている。以上の点から、ラウンド関数に異なる演算系を使用した事が必ずしも差分攻撃に対する改善になっていないと言える。

次に、ラウンド関数の結果を用いて、9 quad-roundのCAST-256に差分攻撃を適用した。Differentially weak keysが8 quad-roundのCAST-256では、2^{-35}という高い確率で生じる。この様な鍵の場合、2^{123}の平文と、約2^{100}の計算量で9 quad-round目のサブ鍵の一部74bitと5bitローテーション鍵が求まる。

また、CAST-128の差分攻撃に対する強度が、CAST-256に必ずしも引き継げたと言えない事も示した。

参考文献

[1] C.M.Adams, *"http://www.nist.gov/aes,"*

[2] C.M.Adams, *"The CAST-128 Encryption Algorithm,"* RFC 2144, May 1997.

[3] B.Shneier, J.Kelsey, *"Unbalanced Feistel Networks and Block Cipher Design,"* Fast Software Encryption, Feb. 1996, LNCS 1039, Springer, pp.121-144.

[4] D.Wagner, *"The Boomerang Attack "*, Fast Software Encryption, March 1999, LNCS 1636, Springer, pp.156-170.

[5] E.Biham, A.Shamir, *"Differential Cryptanalysis of DES-like Cryptosystems "*, Journal of Cryptology, Vol.4, No.1, pp.3-72, 1991.

[6] V.Rijmen, L.R.Knudsen, http://www.adfa.oz.au/ lpb/research/loki97/

[7] S. Moriai, T. Shimoyama, T. Kaneko, *"Higher Order Differential Attack of a CAST Cipher,"* Fast Software Encryption, March 1998, LNCS 1372, Springer, pp.17-31.

[8] J. Lee, H. Heys, S. Tavares, *"Resistance of a CAST-like Encryption Algorithm to Linear and Differential Cryptanalysis,"* Designs, Codes and Cryptography, vol. 12, no. 3, 1997, pp.267-282.

[9] C.M.Adams, *"Constructing Symmetric Ciphers Using the CAST Design Procedure,"* in Selected Areas in Cryptography, E. Kranakis and P. Van Oorschot (ed.), Kluwer Academic Publishers, 1997, pp.71-104.

[5]但し、3 round繰り返し特性については調査していないので、存在するかもしれない