2Z-7

ビット接続可能性を考慮したAESの差分攻撃耐性評価

遠藤拓也† 金子敏信†
東京理科大学大学院理工学研究科†

1 序論

AESはNISTにより米国標準暗号規格として制定された共通鍵暗号方式である。[1] 差分攻撃耐性評価として、truncate差分パス探索により最大差分特性確率の上界が2^{-330}(128bit鍵)、2^{-450}(192bit鍵)、2^{-480}(256bit鍵)と報告されている。本稿では、Sboxで接続可能な、差分パスのみを用いて実際の差分パスとして存在しうる差分パスを調査した。

2 差分攻撃

差分攻撃とは、差分伝搬を解析する事により高確率で伝搬するパスを求めて行う攻撃方法である。

2.1 差分確率

関数$f(x)$に於いて、入力差分Δxと出力差分Δyに対し、差分確率DP_fは次式で定義される。ここでnはxのビット長を示す。

$$DP_f(\Delta x,\Delta y)=\frac{\sharp\{x\in\{0,1\}^n|f(x)\oplus f(x\oplus\Delta x)=\Delta y\}}{2^n} \quad (1)$$

差分攻撃に対する関数$f(x)$の強度は、暗号化関数を構成する部品の差分確率の積により与えられる差分特性確率で評価を行い、それの最大値である最大差分特性確率DCP_{max}を強度指標とする。

2.2 truncate 差分解析

最大差分特性確率DCP_{max}の上界を簡易に求める手法がtruncate差分解析である。この手法は、複数bitの差分の有無を1bitで表す。差分有の場合activeと呼び、無の場合non-activeと呼ぶ。Sboxにおいて、Sboxの入力差分がactiveであれば、そのSboxをactive Sboxと呼ぶ。active Sbox数の合計をASと表し、その最小値をAS_{min}と表す。

3 AESの truncate 差分解析

従来結果であるDCP_{Tmax}は表1となる。[2]。これはactiveSboxに於いて、任意の非零入力差分が、任意の非零出力差分に確率2^{-6}でパス接続可能であると考えた評価であり、真の最大差分特性確率ではない。なお、4節の結果も合わせて載せておく。詳しい説明は4節で行う。

表1 段数とAS数及びDCP_{Tmax},4節の結果の関係

段数	AS 数	$DCP_{Tmax}[log_2]$	4節の結果 $[log_2]$
1	1	-6	-6
2	5	-30	-30
3	9	-54	-54
4	25	-150	-150
5	26	-156	-170
6	30	-180	-194
7	34	-204	-218
8	50	-300	-314
9	51	-306	-335
10	55	-330	-359
11	59	-354	-383
12	75	-450	-479
13	76	-456	-500
14	80	-480	-524

4 ビット接続可能性を考慮したAESの差分解析

ここでは、Sboxで接続可能な差分パスを用いて実際の差分パスとして存在しうる差分パスの解析方法を述べる。

4.1 Sboxの差分特性

Sboxの差分確率を調査すると、差分確率の最大値$DP_{max}=2^{-6}$のものと、次点の差分確率$DP_{sec}=2^{-7}$のみである。DP_{max}となる差分の組み合わせは255組存在する。これは、任意の非零入力差分に対し、一つの非零出力差分が確率2^{-6}でパス接続可能である事を意味している。また、DP_{sec}となる差分の組み合わせは32130組存在する。これは、任意の非零入力差分に対し、126個の非零出力差分が確率2^{-7}でパス接続可能である事を意味している。

4.2 最良 truncate パスの構造

3節で求めた最良パスはいずれも4ラウンド周期であり、繰り返し構造となっている。その為、1ラウンド目の非零入力差分と5ラウンド目の非零入力差分がビット単位で同一であれば、以降のラウンドに於いてビット単位の接続性を持つと言える。よって、4ラウンド間のビット単位での接続性を検証する。

図1は3節で導出した4ラウンドでの最良パスである。以下に4ラウンド最良パスの性質を記述する。

性質1 各段でのAS数増加量は$1\rightarrow4\rightarrow16\rightarrow4\rightarrow1$である。

性質2 最良パスは256通りあり、1ラウンド目に於いてAS数が1であれば、どのSboxをactiveにしても良い。

性質3 3ラウンド目の出力差分に制約があり、4ラウンド目のMixColumns一つに於いて、入力4バイトが非零差分である。他の12バイトは零差分になる。

性質4 4ラウンド目の出力は1バイトだけ非零差分であり、その非零差分はどの系列であっても良い。

始めにこの最良パスがSboxに於いて、差分確率2^{-6}でパ

Strength evaluation of AES by Differential Cryptanalysis with bit connectibility

† Takuya ENDO,Toshinobu KANEKO
† Department of Electrical Engineering,Faculty of Science and Technology,Tokyo University of Science

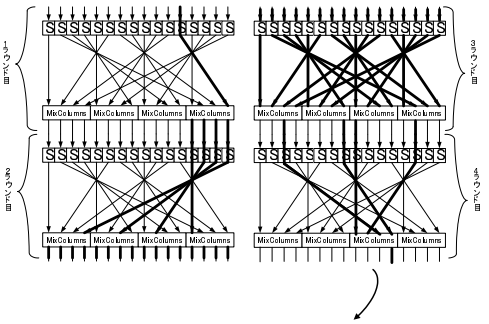

図1　4 ラウンド最良パス

ス接続可能かどうか検証する。MixColumns は MDS 行列である事から、任意の 1 バイト非零差分に対し、4 バイトの非零差分が出力される。よって 1 ラウンド目と 2 ラウンド目に於いて、図 1 のようなパスは存在する。3 ラウンド目に於いて、Sbox に入力される非零差分に対し最大差分確率でパス接続可能な出力差分を用いて、3 ラウンド目の出力 16 バイトの内 12 バイトが零差分になるかを計算機実験により調査した。結果、12 バイトが零差分になるパスは存在しなかった。

3 ラウンド目でパス接続しなかったので、3 ラウンド目の幾つかの Sbox に於いて、差分確率 2^{-7} で接続可能な非零差分を用い、対応する MixColumns の出力差分 3 バイトを零にする解析を行う。一つの MixColumns に対応する Sbox は 4 つあるので、それぞれ差分確率 2^{-6} と 2^{-7} で接続可能な非零差分を総当たりする事になるが、ここで効率的な解析方法を述べる。

4.3　効率的な解析手法

MixColumns の 1 ワード分に入力される差分を $X, (X = (\Delta x_0, \Delta x_1, \Delta x_2, \Delta x_3))$ とし、MixColumns によって出力される差分を $Y, (Y = (\Delta y_0, \Delta y_1, \Delta y_2, \Delta y_3))$ とする。但し、X, Y はそれぞれ $\mathrm{GF}(2^8)$ のベクトルで、$\Delta x_k, \Delta y_l,$ は $\mathrm{GF}(2^8)$ の元である。MixColumns 変換は行列を用いて式で表すと、

$$\begin{pmatrix} \Delta y_0 \\ \Delta y_1 \\ \Delta y_2 \\ \Delta y_3 \end{pmatrix} = \begin{pmatrix} 0\mathrm{x}02 & 0\mathrm{x}03 & 0\mathrm{x}01 & 0\mathrm{x}01 \\ 0\mathrm{x}01 & 0\mathrm{x}02 & 0\mathrm{x}03 & 0\mathrm{x}01 \\ 0\mathrm{x}01 & 0\mathrm{x}01 & 0\mathrm{x}02 & 0\mathrm{x}03 \\ 0\mathrm{x}03 & 0\mathrm{x}01 & 0\mathrm{x}01 & 0\mathrm{x}02 \end{pmatrix} \begin{pmatrix} \Delta x_0 \\ \Delta x_1 \\ \Delta x_2 \\ \Delta x_3 \end{pmatrix} \quad (2)$$

と書く事ができる。今回、3 ラウンド目の MixColumns を想定すると、バイト単位でのハミング重みはそれぞれ

$$Hw(X)=4, Hw(Y)=1 \quad (3)$$

である。(2) 式を初等代数計算で変形すると、

$$\begin{pmatrix} \Delta x_1 \\ \Delta x_2 \\ \Delta x_3 \end{pmatrix} = \Delta x_0 \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} \quad (4)$$

となる。c_0, c_1, c_2 は定数なので、右辺の Δx_0 を決めれば左辺のベクトルは一意に定まる。左辺のベクトルの値が実際に存在するかを判定すれば良い。定数 c_0, c_1, c_2 に於いて、Y の 4 バイトの内どの 1 バイトを非零差分にするかによって値は変化する。表 2 に定数の値をまとめておく。

表 2　定数 c_0, c_1, c_2 の値

	$\Delta y_0 \neq 0$	$\Delta y_1 \neq 0$	$\Delta y_2 \neq 0$	$\Delta y_3 \neq 0$
c_0	0x8c	0xec	0x71	0x26
c_1	0x35	0x9a	0x39	0x9f
c_2	0x5d	0xb7	0xa8	0xf7

4.4　解析結果

結果を表 1 に示す。また 5 ラウンドのパスの具体例を表 3 に示す。各ラウンドの AS 数は $1 \to 4 \to 16 \to 4$ となり、表 4 のような差分確率で繰り返しになる。5 ラウンド以上を途中で切る場合、この繰り返し構造のどの位置からでも構わない。また、平文側、暗号文側に隣接する 1 ラウンドは確率 2^{-6} に置き換える事ができ、それぞれに隣接する 3 ラウンドに対して、場合によって確率 2^{-6} に置き換える事が出来る。

表 3　5 ラウンドにおける本稿の結果を与える差分の一例

ラウンド数	ラウンド関数の入力差分	
1	$st_{1,0}$=(0x91,0,0,0)	$st_{1,1}$=(0,0,0,0)
	$st_{1,2}$=(0,0,0,0)	$st_{1,3}$=(0,0,0,0)
2	$st_{2,0}$=(0xdf,0xe2,0xe2,0x3d)	$st_{2,1}$=(0,0,0,0)
	$st_{2,2}$=(0,0,0,0)	$st_{2,3}$=(0,0,0,0)
3	$st_{3,0}$=(0xe1,0xfd,0xfd,0x1c)	$st_{3,1}$=(0x44,0x44,0xcc,0x88)
	$st_{3,2}$=(0xfb,0x16,0xed,0xfb)	$st_{3,3}$=(0x16,0xed,0xfb,0xfb)
4	$st_{4,0}$=(0,0x06,0,0)	$st_{4,1}$=(0,0,0xcd,0)
	$st_{4,2}$=(0,0,0,0x0c)	$st_{4,3}$=(0x06,0,0,0)
5	$st_{5,0}$=(0,0,0,0)	$st_{5,1}$=(0,0,0,0)
	$st_{5,2}$=(0,0,0,0)	$st_{5,3}$=(0,0,0,0x69)

表 4　AS の確率内訳

AS 数	確率の内訳
1	2^{-7}
4	$(2^{-6})^4$
16	$(2^{-6})^4(2^{-7})^{12}$
4	$(2^{-6})^2(2^{-7})^2$

5　結論

Sbox で接続可能な、差分確率 2^{-6} と 2^{-7} の差分パスを用いて実際の差分パスとして存在しうる差分パスを調査した。その結果、4 ラウンド繰り返しとなるパスが存在したので、全ラウンドにおいても接続性があると言える。

参考文献

[1] NIST,“FIPS197”,http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf(2001)

[2] CRYPTREC 技術報告書
“共通鍵ブロック暗号の線形攻撃耐性評価報告書”
http://www.cryptrec.go.jp/estimation/techrep_id2101_3.pdf