L-021

擬似乱数生成器 *Enocoro* の差分線形攻撃耐性評価

Security evaluation of *Enocoro* against Differential Linear Cryptanalysis

徳田康平 † 金子敏信 †
Kouhei Tokuda Toshinobu Kaneko

概 要

Enocoro は日立製作所によって 2007 年に ISEC で提案されたストリーム暗号向け擬似乱数生成器である。パラメータ指定アルゴリズムとして Enocoro-80/128v1.1/v2 が提案されている。本稿では、*Enocoro*-80/128v1.1 について差分線形攻撃耐性評価を行った。その際、最良差分線形パスを与える可能性が高い、バッファb_7 のみ、b_{17} のみ active としたパスをそれぞれ差分パスとして用いて、最良線形パス探索を行った。その結果、最小 active Sbox 数 (AS_{Dmin},AS_{Lmin}) はそれぞれ (1, 22)、(0, 37) と求まり、最大差分線形確率の上界 $ldcp_{max}$ は 2^{-178},2^{-296} となった。これは鍵長 $k$bit の場合の安全指標である 2^{-k} よりも小さいので *Enocoro*-80/-128v1.1 は差分線形攻撃に対して十分な耐性を持つと言える。

1. はじめに

Enocoro は日立製作所によって 2007 年に ISEC で提案されたストリーム暗号向け疑似乱数生成器である。パラメータを与えることで内部構造が決定する仕様となっており、パラメータ指定のアルゴリズムとして *Enocoro*-80/*Enocoro*-128v1.1/*Enocoro*-128v2 が提案されている。現在までに、差分攻撃 [3]、線形攻撃 [3]、高階差分攻撃 [4] については十分な耐性をもつという報告がされているが、差分線形攻撃耐性については未知であるので、本稿では *Enocoro*-80/128v1.1 について差分攻撃耐性評価を行った。

2.*Enocoro* の構造

Enocoro は、内部状態であるステートとバッファ、状態更新関数である ρ 関数と，λ 関数、出力関数から構成される。入力として、鍵長は 80bit 及び 128bit、初期ベクトル (IV) は 64bit を持ち、8bit を 1byte とした byte 単位で疑似乱数列を出力する。

2.1. 内部状態

ステート a は 2byte からなり、上位 byte から順に a_0, a_1 と表す。バッファb は $n_b$byte からなり、上位 byte から順に $b_0, b_1, \cdots, b_{n_b-1}$ と表す。また、時刻 t における状態を $a^{(t)}, b^{(t)}$ と表すことにする。

2.2. 状態更新関数

状態更新関数の概要は図 1 に従う。図の左側が λ 関数、右側が ρ 関数である。

[λ 関数]

λ 関数はステート a をパラメータとする線形変換である。バッファb を次式に従って更新する。

$$\begin{aligned} b_i^{(t+1)} &= b_{i-1}^{(t)} \quad (i \neq 0, q_1+1, q_2+1, q_3+1) \\ b_0^{(t+1)} &= b_{n_b-1}^{(t)} \oplus a_0^{(t)} \\ b_{q_j+1}^{(t+1)} &= b_{q_j}^{(t)} \oplus b_{p_j}^{(t)} \quad (j=1,2,3) \end{aligned} \tag{1}$$

[ρ 関数]

Enocoro の ρ 関数は、バッファb の特定バイトの値 $b_{k_1}, ..., b_{k_4}$ をパラメータとして用いる非線形関数である。Sbox s_8 と線形変換 L, 排他的論理和で構成される（s_8 と L は後述)。ステート a を次式に従って更新する。

$$\begin{aligned} u_0 &= a_0^{(t)} \oplus s_8[b_{k_1}^{(t)}] \\ u_1 &= a_1^{(t)} \oplus s_8[b_{k_2}^{(t)}] \\ (v_0, v_1) &= L(u_0, u_1) \\ a_0^{(t+1)} &= v_0 \oplus s_8[b_{k_3}^{(t)}] \\ a_1^{(t+1)} &= v_1 \oplus s_8[b_{k_4}^{(t)}] \end{aligned} \tag{2}$$

2.3. 部品

2.3.1. 線形変換 L

Enocoro-80/128v1.1 では線形変換 L として次式を用いる。

$$\begin{pmatrix} v_0 \\ v_1 \end{pmatrix} = L(u_0, u_1) = \begin{pmatrix} 1 & 1 \\ 1 & d \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} \quad d \in \mathrm{GF}(2^8) \tag{3}$$

有限体 GF(2^8) の定義多項式は次式を用いる。

$$\varphi_8(x) = x^8 + x^4 + x^3 + x + 1 = \texttt{0x11b} \tag{4}$$

2.3.2.Sbox s_8

Sbox s_8 は 8bit 入出力の Sbox である。実際には 4bitSbox を組み合わせて SPS 変換を構成し 8bit Sbox としている。なお、本稿では 4 つの Sbox を区別するために図 1 の Sbox を上から s_1、s_2、s_3、s_4 とする。

2.4.*Enocoro*-80/-128v1.1

Enocoro-80/-128v1.1 の内部構造はパラメータ $(n_b; k_1, k_2, k_3, k_4)$ を与えることで決定する。それ以外のパラメータ (q_j, p_j) は次式で定め、$i \neq j$ ならば $p_i - q_i \neq p_j - q_j$ とする。

$$\begin{cases} q_j &= k_j \\ p_j &= k_{j+1} - 1 \end{cases} \quad (j=1,2,3) \tag{5}$$

†東京理科大学理工学研究科電気工学専攻,Department of Electrical Engineering,Faculty of Science and Technology,Tokyo University of Science

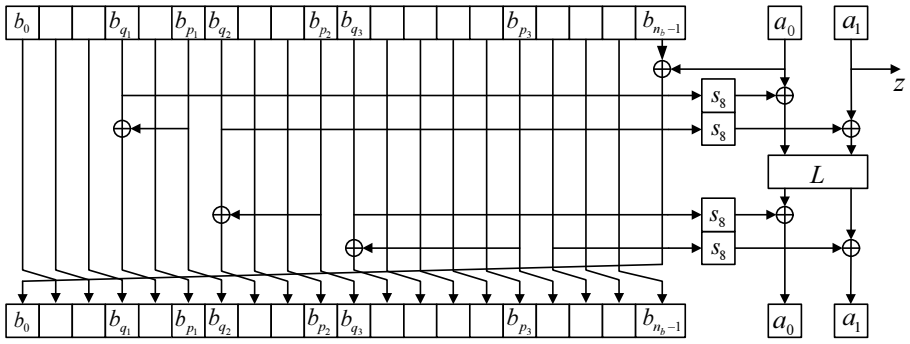

図 1: *Enocoro* の状態更新関数

内部構造を定めるパラメータは以下である。

- *Enocoro*-80 : $(20; 1, 4, 6, 16)$
- *Enocoro*-128 ver.1.1 : $(32; 2, 7, 16, 29)$

2.4.1. 初期化

Enocoro-80/-128/-128 ver.1.1 の初期状態 $(a^{(0)}, b^{(0)})$ は、秘密鍵 K_i, 初期ベクトル I_i を用いて次式のように定める。

[*Enocoro*-80] ($Next^{40}(S^{(0)})$ は状態更新関数 $Next$ を 40 回繰り返して適用することを意味)

$$\begin{aligned} b_i^{(0)} &= K_i \ \ (0 \le i < 10) \\ b_{i+10}^{(0)} &= I_i \ \ (0 \le i < 8) \\ b_{18}^{(0)} &= \texttt{0x66}, \ \ b_{19}^{(0)} = \texttt{0xe9}, \ \ a_0^{(0)} = \texttt{0x4b}, \ \ a_1^{(0)} = \texttt{0xd4} \\ S^{(40)} &= Next^{40}(S^{(0)}) \end{aligned} \tag{6}$$

[*Enocoro*-128 ver.1.1]

$$\begin{aligned} b_i^{(0)} &= K_i \ \ (0 \le i < 16) \\ b_{i+16}^{(0)} &= I_i \ \ (0 \le i < 8) \\ b_{24}^{(0)} &= \texttt{0x66}, \ \ b_{25}^{(0)} = \texttt{0xe9}, \ \ b_{26}^{(0)} = \texttt{0x4b}, \ \ b_{27}^{(0)} = \texttt{0xd4} \\ b_{28}^{(0)} &= \texttt{0xef}, \ \ b_{29}^{(0)} = \texttt{0x8a}, \ \ b_{30}^{(0)} = \texttt{0x2c}, \ \ b_{31}^{(0)} = \texttt{0x3b} \\ a_0^{(0)} &= \texttt{0x88}, \ \ a_1^{(0)} = \texttt{0x4c} \\ S^{(64)} &= Next^{64}(S^{(0)}) \end{aligned} \tag{7}$$

3. 差分線形攻撃

差分線形攻撃 [2] とは S.K. Langford 及び M. E. Hellman によって提案された主にブロック暗号に対して用いられる暗号解読法の一種であり、差分についての線形近似式の偏りを攻撃に利用する攻撃法である。ここでは、差分線形攻撃とその耐性を考える際に必要な事柄をまとめる。

3.1. 差分線形確率

平文を x, x^*、暗号文を y, y^* , 中間段変数を z, z^* としたとき差分線形確率は次式で定義される。

$$\left| \ 2 \underset{x,x^*}{Pr} \{\Gamma_y \bullet y \oplus \Gamma_y \bullet y^* = \Gamma_z \bullet \Delta z | x \oplus x^* = \Delta x\} - 1 \ \right|^2 = P \tag{8}$$

差分線形確率 P は攻撃者が非線形関数の入力差分を制御できる場合 (9) 式で評価される。

$$p_D = \left| \ 2^{\frac{\#\{x \in \{0,1\}^n | \Gamma_x \bullet \Delta_x = \Gamma_y \bullet \Delta_y\}}{2^n} - 1} \ \right|^2 \tag{9}$$

制御ができない場合 (10) 式で評価する。これは、線形確率の 2 乗に等しい。

$$p_L = \left| \ 2^{\frac{\#\{z \in \{0,1\}^n, z^* \in \{0,1\}^n | \Gamma_z \bullet \Delta_z = \Gamma_y \bullet \Delta_y\}}{2^{2n}} - 1} \ \right|^2 \tag{10}$$

3.2. 差分線形特性確率

暗号系全体に対して差分線形確率の最大値を求め安全性評価とする。通常は構成部品の差分線形確率を求めそれを線形パスに沿って接続し、構成部品の確率の積で差分線形確率の指標とする。これを差分線形特性確率と呼ぶ。(以下、LDCP とする）秘密鍵長 $k$bit の暗号系において最大差分線形特性確率が 2^{-k} より小さければ安全と判断される。

3.3.truncate 解析

truncate 解析とは、複数 bit をひとまとめにして差分・マスクの有無を 1bit で表現し、その 1bit の情報の伝播を解析するものである。このとき、ひとまとめにするビット幅が小さいほど詳細な評価となる。また、差分・マスクが非 0 である事を active と呼ぶ。

$$\begin{cases} \Gamma \neq 0 \rightarrow \Gamma = 1 \ \ (\text{acive}) \\ \Gamma = 0 \rightarrow \Gamma = 0 \ \ (\text{non-active}) \end{cases} \tag{11}$$

$$\begin{cases} \Delta \neq 0 \rightarrow \Delta = 1 \ \ (\text{acive}) \\ \Delta = 0 \rightarrow \Delta = 0 \ \ (\text{non-active}) \end{cases} \tag{12}$$

truncate 解析において差分の伝播条件は分岐においては図 2、排他的論理和においては図 3、マスクの伝播条件は分岐については図 4 排他的論理和においては図 5 のようになる。図中の太線は active 差分・マスクが伝播しているパスを示している。

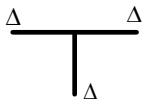

図 2: 分岐における差分の伝播

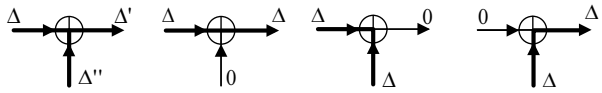

図 3: 排他的論理和における差分の伝播

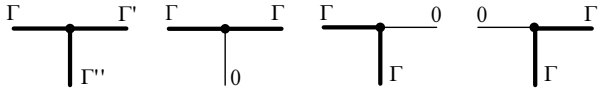

図 4: 分岐におけるマスクの伝播

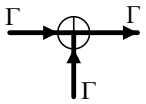

図 5: 排他的論理和におけるマスクの伝播

3.4.active Sbox

Sbox への入力差分、入力マスクが共に active の時その Sbox を active Sbox と呼ぶ。以降、ラウンド t の処理で生じる active Sbox の数を $as^{(t)}$ と書き、active Sbox 数の合計を AS(=$\Sigma as^{(t)}$) と表す。さらに AS のうち最小のものを AS_{min} と表す。

3.5. 最大差分線形特性確率の上界

最大差分線形特性確率の上界は truncation パス探索で評価でき、そのパスの上で active になっている Sbox の個数を用いて次式で評価できる。但し、Sbox の最大選択差分型差分線形確率を p_{Dmax}、Sbox の最大差分線形確率を p_{Lmax} それぞれを用いて評価する sbox の最小個数をそれぞれ AS_{Dmin}、AS_{Lmin} とする。

$$\begin{aligned} LDCP_{max} &\leq (p_{Dmax})^{AS_{Dmin}}(p_{Lmax})^{AS_{Lmin}} \\ &= ldcp_{max} \end{aligned}$$

4.*Enocoro* の解析

ここでは *Enocoro* の差分線形攻撃耐性を評価するために、最大差分線形確率の $LDCP_{\max}$ の上界 $ldcp_{max}$ を truncate 差分線形解析により導出するアルゴリズムを説明する。本評価では 8bit truncate を用いる。以降、1 時刻分の処理をラウンドと考え、時刻をラウンドと表記することにする。非線形関数は Sbox s_8 のみであることから、$ldcp_{max}$ を求めるためには、全てのパスに対する AS_{Dmin}, AS_{Lmin} を求めれば良い。

4.1. 探索するパス

線形パスを探索する際の評価関数としてのコストは選んだ差分パスに依存する。これより、$ldcp_{max}$ を求めるにはすべての差分パスに対して、最小のＡＳ数を与える線形パスの探索を行えば良い。しかしこれは、計算量的に困難であるので、本稿ではバッファ b_7 のみ (*Enocoro*-80)、バッファ b_{17} のみ (*Enocoro*-128v1.1)active としたときのパスを差分パス * として用いる。これはこの様にパスを選ぶことで、最も長いラウンドにわたって Sbox の入力差分を non-active に選ぶことができ、差分線形確率 p_L を用いて評価する AS 数を少なくすることができると考えられるからである。それはそれぞれ最初の 9 ラウンド、12 ラウンドとなる。また、この差分パスを用いたとき、制御できる Sbox は次の通りである。

Enocoro-80 ;10、19、28 ラウンドの s_4
Enocoro-128v1.1 ;13、25、37 ラウンドの s_4

差分線形解析では差分パスをこの様に選んだ時、AS_{Dmin}, AS_{Lmin} を与える線形パスを探索する。

4.2. 探索アルゴリズム

線形パス及び最大差分線形特性確率の上界を求める方法として、Viterbi アルゴリズムを用いる。以下に示すパラメータを状態と考え、トレリス線図で書き表し、Viterbi 探索を適用し、その中から最小の $AS^{(t)}$ を調べる。なお、8bit truncate による差分線形特性を考察するため、以下のパラメータはそれぞれ 1bit の値を持つ。

- $\Gamma_{a_0^{(t)}}, \Gamma_{a_1^{(t)}} \in \{0,1\}$
- $\Gamma_{a_0^{(t+1)}}, \Gamma_{a_1^{(t+1)}} \in \{0,1\}$
- $\Gamma_{b_0^{(t)}}, ..., \Gamma_{b_{n_b-1}^{(t)}} \in \{0,1\}$
- $\Gamma_{b_0^{(t+1)}}, ..., \Gamma_{b_{n_b-1}^{(t+1)}} \in \{0,1\}$

なお、 Γ は添え字の変数に対する線形マスクを表す。

4.3. 探索ラウンド

本稿の差分線形攻撃耐性評価では、Enocoro-80/-128v1.1 における初期化段 40 ラウンド、64 ラウンドについて評価を行う。

5.*Enocoro* の評価

5.1.Sbox s_8 の解析

Enocoro に使用される Sbox の最大選択差分型差分線形確率 $p_{D\max}$ を、式 (9), 最大差分線形確率 $p_{L\max}$ を式 (10) に基づき計算した結果 $p_{D\max} = 2^{-2}$,$p_{L\max} = 2^{-8}$ であった。$p_{D\max}$ を与える入出力マスク、入力差分値の一例を表 1 に,$p_{L\max}$ を与える入出力マスクを表 2 に示す。

表 1: $p_{D\max}$ を与える入出力マスク、入力差分の一例

Γx	0x02	0x22	0x2F	0x4E	0x6B	0x76
Γy	0xCC	0xCC	0xCC	0xCC	0xCC	0xCC
Δx	0xC0	0xC0	0xC0	0xC0	0xC0	0xC0

* この差分パスにおいては一度未知となった差分はその後既知にはならないとする

表 2: $p_{L\max}$ を与える入出力マスク

Γx	0x26	0x34	0x62	0x9A	0xB5	0xC1	0xF7
Γy	0x06	0x7f	0x60	0x46	0x9D	0x50	0xCD

5.2.truncate 差分線形解析

4.2 のアルゴリズムを用いて計算機での解析を行った結果、AS_{Dmin}、AS_{Lmin}、最大差分線形特性確率の上界 $ldcp_{max}$ は以下の表 3 の用になった。*Enocoro*-80 についてのラウンド数に対する AS 数とその時の $ldcp_{max}$ を表 4 にまとめる。また、その $ldcp_{max}$ を与える線形パスの一例を表 5 に示す。表 4 より 36 ラウンドで 2^{-80} を下回ることがわかる。これは、参考文献 [3] の差分攻撃の場合と比較すると、[3] においては 2^{-80} を下回るラウンドは 31 ラウンドであるので 5 ラウンド長い。表 3 を見ると、(AS_{Dmin},AS_{Lmin})=(1,22) (0,37) であり $ldcp_{max}$ は 2^{-184}、2^{-296} となった。これは安全指標 2^{-k} より小さいので *Enocoro*-80/-128v1.1 は差分線形攻撃に対して耐性を持つと言える。

表 3: truncate 差分線形解析の結果

	(AS_{Dmin},AS_{Lmin})	$ldcp_{max}$
Enocoro-80	(1 , 22)	2^{-178}
Enocoro-128	(0 , 37)	2^{-296}

表 4: truncate 差分線形解析の結果

ラウンド数	(AS_{Dmin},AS_{Lmin})	$ldcp_{max}$
1〜15	(0 , 0)	1
16〜27	(0 , 1)	2^{-8}
28	(1 , 3)	2^{-26}
29〜34	(1 , 6)	2^{-50}
35	(1 , 9)	2^{-74}
36,37	(1 , 12)	2^{-98}
38	(1 , 15)	2^{-122}
39	(1 , 19)	2^{-154}
40	(1 , 22)	2^{-178}

6. まとめ

Enocoro-80/-128v1.1 について差分線形攻撃耐性評価を行った。その結果、(AS_{Dmin},AS_{Lmin})=(1,22) (0,37) であったので最大差分線形特性確率の上界は 2^{-184}、2^{-296} であることが分かった。これは安全指標 2^{-k} より小さいので *Enocoro*-80/-128v1.1 は差分線形攻撃に対して耐性を持つと言える。

参考文献

[1] 渡辺大、金子敏信　”軽量な PANAMA 型疑似乱数生成器の構成に関する検討”, 信学技報,ISEC2007-78

[2] S.K. Langford and M. E. Hellman　”Differential Linear Cryptanalysis,” CRYOTO’94

[3] 岡本和人, 武藤健一郎, 金子敏信　”疑似乱数生成器 Enocoro-80 の差分／線形攻撃耐性評価（II）” 暗号と情報セキュリティシンポジウム, SCIS2009

[4] 春山知宏, 武藤健一郎, 金子敏信　”Enocoro-80/-128ver1.1 の高階差分特性”

資料・パス

表 5: $ldcp_{max}$ を与える線形パスの一例

t	線形マスク	t	線形マスク
0	0x000001	21	0x00ffd0
1	0x000002	22	0x00ffe0
2	0x000014	23	0x00ffc0
3	0x000068	24	0x01ff80
4	0x0100d0	25	0x03ff00
5	0x0301e0	26	0x07fe00
6	0x0703c0	27	0x0ffc00
7	0x0f0780	28	0x3cf895
8	0x3d0f95	29	0x18f1ff
9	0x1b1fff	30	0x00e3bf
10	0x073fef	31	0x01c73e
11	0x0f7fce	32	0x038e3c
12	0x3fff8d	33	0x071c38
13	0x3cffef	34	0x0e3870
14	0x3bffaf	35	0x3e7075
15	0x34ffaf	36	0x1ce03f
16	0x18ffee	37	0x09c06f
17	0x00ffdd	38	0x31805b
18	0x00fffa	39	0x310012
19	0x00fff4	40	0x200000
20	0x00ffe8		

線形パス:内部状態 a,b の truncate マスク値で表す。線形パス $= a_1||a_0||b_{19}||\cdots||b_1||b_0|$ の truncate マスクを表し、各 bit の 1,0 は active,non-active を意味する。