コンピュータセキュリティ 10−15
(2000. 7. 25)

SPN 型ラウンド関数を利用した Feistel 暗号の最大差分／線形特性確率の上界値について

神田 雅透 *

*NTT 情報流通プラットフォーム研究所
〒 239-0847 神奈川県 横須賀市 光の丘 1−1
kanda@isl.ntt.co.jp

あらまし　差分攻撃や線形攻撃に対する耐性を評価する有用な評価尺度の一つに最大差分／線形特性確率の上界値を用いる方法がある。この評価尺度について、SPN 暗号では branch number を利用した differentially/linearly active s-boxes の最少個数によって最大差分／線形特性確率の上界値を評価する手法が知られているが、同様の手法によって Feistel 暗号を評価した場合の厳密な結果は知られていなかった。そこで、本稿では、SPN 型ラウンド関数を利用した Feistel 暗号の最大差分／線形特性確率の上界値について differential/linear branch number $\mathcal{B}_d$, $\mathcal{B}_l$ を利用した differentially/linearly active s-boxes の最少個数の観点から明らかにする。結果として、3、4、6、8、12 段の Feistel 暗号の differentially/linearly active s-boxes の最少個数は、それぞれ 2, $\mathcal{B}_d$ $(\mathcal{B}_l)$, $\mathcal{B}_d+2$ $(\mathcal{B}_l+2)$, $2\mathcal{B}_d+1$ $(2\mathcal{B}_l+1)$, $3\mathcal{B}_d+1$ $(3\mathcal{B}_l+1)$ となる。

和文キーワード　ブロック暗号、暗号設計、差分攻撃、線形攻撃、特性確率、安全性評価

A Study on the Upper Bounds of the Maximum Differential/Linear Characteristic Probabilities of Feistel ciphers with SPN round function

Masayuki KANDA *

*NTT Information Sharing Platform Laboratories
1−1 Hikarinooka, Yokosuka-shi, Kanagawa, 239-0847, Japan

Abstract　This paper studies the upper bounds of the maximum differential/linear characteristic probabilities of Feistel ciphers with SPN round function. In the same way as SPN ciphers, we consider the minimum number of differentially/linearly active s-boxes, which are proportion to the upper bounds of these probabilities, in order to evaluate the security against differential/linear attacks. The purpose of this work is to clarify the minimum numbers of active s-boxes in some consecutive rounds of Feistel ciphers, i.e., in three, four, six, eight, and twelve consecutive rounds, using differential/linear branch numbers $\mathcal{B}_d$, $\mathcal{B}_l$. As a result, we clarified that the minimum number of differentially (resp. linearly) active s-boxes are 2, $\mathcal{B}_d$ $(\mathcal{B}_l)$, $\mathcal{B}_d+2$ $(\mathcal{B}_l+2)$, $2\mathcal{B}_d+1$ $(2\mathcal{B}_l+1)$, and $3\mathcal{B}_d+1$ $(3\mathcal{B}_l+1)$, respectively.

英文 key words　Block cipher, Design strategy, Differential attack, Linear attack, Characteristic probability, Security measure

1 はじめに

差分攻撃 [3] や線形攻撃 [6] に対する耐性を評価するための評価尺度はいくつか知られているが、その中の一つに最大差分／線形特性確率の上界値を用いる方法がある。これは、攻撃者が利用するのに最も効果的な差分パスや線形近似を探索的に発見したと仮定して、それらの差分パスや線形近似が成立する確率 (最大差分／線形特性確率) に対する理論的な上界値を与えようとするものである。

Rijmen らは、SPN 暗号について最大差分／線形特性確率の上界値を示すために、Branch number $\mathcal{B}$ を定義した [8]。さらに、最大差分／線形特性確率が active s-box の個数に依存して変化することから、Branch number $\mathcal{B}$ を利用して全ての差分パスや線形近似における active s-box の最少個数を明らかにすることによって最大差分／線形特性確率の上界値を示す手法を述べている。

一方、Knudsen は、一般の Feistel 暗号について、最大差分／線形特性確率の上界値がブロック長の逆数で表される安全性閾値以下となることが示されるのであればいかなる差分パスや線形近似も攻撃には利用できないことを意味すると考えられるので、その暗号は安全 (practically secure) であるとみなすことが出来ると述べている [4]。しかし、文献 [4] では Feistel 暗号全てに共通して議論をしているため、最大差分／線形特性確率の上界値はラウンド関数での最大差分／線形確率と段数だけに依存した表現となっている。具体的には、ラウンド関数の最大差分／線形確率を p, q として、$2r$-round Feistel 暗号の最大差分／線形特性確率の上界値は p^r, q^r である。このため、ラウンド関数の最大差分／線形確率 p, q があまり小さくない値だが複数段での最大差分／線形確率が急速に小さくなるような暗号の場合、必ずしも Knudsen の評価が有用なわけではない。さらにいえば、ラウンド関数の構成によっては、Knudsen の評価よりもさらに厳密な評価が可能になることも考えられる。

そこで、本稿では、ラウンド関数の構成を SPN 型に限定することによって Feistel 暗号の最大差分／線形特性確率の上界値を示すことを目的とする。具体的には、SPN 暗号の場合と同様の議論、すなわち、Branch number $\mathcal{B}$ を利用して差分パスや線形近似における active s-box の最少個数を明らかにすることによって最大差分／線形特性確率の上界値を示す。

2 準備

2.1 表記

- $X = (x_1, \ldots, x_n)$, $x_i \in \mathrm{GF}(2^m)$, $(1 \leq i \leq n)$: vecter X over $\mathrm{GF}(2^m)^n$ and element x_i of X over $\mathrm{GF}(2^m)$.
- ΔX, ΓY : difference of X, mask value of Y.
- $X \cdot \Gamma X$: parity bitwise product X and ΓX.
- $X \oplus Y$: bitwise exclusive-OR (XOR).
- $X|Y$: concatenation between X and Y.
- $\{S\}$, $\#\{S\}$: elements in set S and a number of elements in set S.

2.2 考察モデル

本稿では mn-bit 長の SPN 型ラウンド関数を利用した Feistel 暗号を考える (図 1)。ただし、各段に利用される拡大鍵は独立かつ一様に生成されており、データとの排他的論理和に利用されると仮定する。さらに拡大鍵との排他的論理和を取られるデータも独立かつ一様なランダムビット列であると仮定する。これらの仮定により、本稿においては拡大鍵の影響は議論の対象外とする。

データの表記として、$X^{(i)}$ を第 i 段目でのラウンド関数への入力データ、$Y^{(i)}$ を第 i 段目のラウンド関数の出力データとする。これを用いると、r-round Feistel 暗号は以下のように記述できる。

$$X^{(i+1)} = X^{(i-1)} \oplus Y^{(i)}, \ (1 \leq i \leq r),$$

ここで、$(X^{(1)}|X^{(0)})$ が平文、$(X^{(r)}|X^{(r+1)})$ が暗号文を表す。

また、ラウンド関数を以下のように表記する。

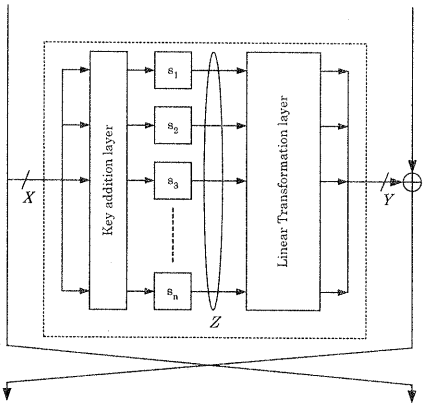

Figure 1: SPN 型ラウンド関数

$$
\begin{aligned}
S\text{ 関数}: \quad & \mathrm{GF}(2^m)^n && \longrightarrow && \mathrm{GF}(2^m)^n \\
& X=(x_1,\ldots,x_n) && \longmapsto && Z=S(X)=(s_1(x_1),\ldots,s_n(x_n))
\end{aligned}
$$

$$
\begin{aligned}
P\text{ 関数}: \quad & \mathrm{GF}(2^m)^n && \longrightarrow && \mathrm{GF}(2^m)^n \\
& Z=(z_1,\ldots,z_n) && \longmapsto && Y=P(Z)=(y_1,\ldots,y_n)
\end{aligned}
$$

$$
\begin{aligned}
F\text{ 関数}: \quad & \mathrm{GF}(2^m)^n && \longrightarrow && \mathrm{GF}(2^m)^n \\
& X=(x_1,\ldots,x_n) && \longmapsto && Y=F(X)=P(S(X))=(y_1,\ldots,y_n)
\end{aligned}
$$

2.3 定義

定義 1 任意の Δx, Δz, Γx, $\Gamma z \in \mathrm{GF}(2^m)$ について、*s-box* s_i の差分／線形確率は以下のように定義される：

$$DP^{s_i}(\Delta x \to \Delta z) = \frac{\#\{x \in \mathrm{GF}(2^m) | s_i(x) \oplus s_i(x \oplus \Delta x) = \Delta z\}}{2^m}$$

$$LP^{s_i}(\Gamma z \to \Gamma x) = \left(2 \times \frac{\#\{x \in \mathrm{GF}(2^m) | x \cdot \Gamma x = s_i(x) \cdot \Gamma z\}}{2^m} - 1\right)^2$$

定義 2 *s-box* の最大差分／線形確率は以下のように定義される：

$$p_s = \max_{\Delta x \neq 0, \Delta z, i} DP^{s_i}(\Delta x \to \Delta z), \qquad q_s = \max_{\Gamma x, \Gamma z \neq 0, i} LP^{s_i}(\Gamma z \to \Gamma x)$$

これは、p_s, q_s として全ての *s-box* を通じて最も大きな値の最大差分／線形確率を採用することを意味している。

定義 3 入力差分が非ゼロとなる *s-box* のことを *differentially active s-box*、出力マスク値が非ゼロとなる *s-box* を *linearly active s-box* という *[5]*。
注意：*s-box* が全単射であるとき、出力差分／入力マスク値が非ゼロとなる *s-box* もそれぞれ *active s-box* である。

定義 4 $X=(x_1,\ldots,x_n) \in \mathrm{GF}(2^m)^n$ とする。このとき、X のハミング重みは以下のように定義される：

$$H_w(X) = \#\{i | x_i \neq 0\}$$

これは、*m-bit* ごとの要素のうち非ゼロであるものの個数と X のハミング重みが等しいことを意味する。

定義 5 *SPN* 型構造において、*differential/linear branch number* $\mathcal{B}_d$, $\mathcal{B}_l$ は以下のように定義される：

$$\mathcal{B}_d = \min_{\Delta X \neq 0} (H_w(\Delta X) + H_w(\theta(\Delta X))), \qquad \mathcal{B}_l = \min_{\Gamma Y \neq 0} (H_w(\theta^*(\Gamma Y)) + H_w(\Gamma Y))$$

ここで、ΔX, $\theta(\Delta X)$ は拡散層（線形変換層）θ の入力差分／出力差分を表し、ΓY, $\theta^*(\Gamma Y)$ は拡散層（線形変換層）θ に対するマスク値拡散層 θ^* の出力マスク値／入力マスク値を表す。

3 Feistel暗号の差分特性確率の上界値

本章では、SPN型ラウンド関数を利用したFeistel暗号での差分特性確率の上界値を示す。まず、その準備として以下にいくつかの定義及び補題を与える。

補題 1 *Feistel*暗号において、以下の関係が成り立つ：

$$H_w(\Delta Y^{(i)}) = H_w(\Delta X^{(i-1)} \oplus \Delta X^{(i+1)}) \leq H_w(\Delta X^{(i-1)}) + H_w(\Delta X^{(i+1)})$$

(proof)

$$\begin{aligned} H_w(\Delta Y^{(i)}) &= H_w(\Delta X^{(i-1)} \oplus \Delta X^{(i+1)}) \\ &= \#\{s|\Delta x_s^{(i-1)} \neq 0 \text{ and } \Delta x_s^{(i+1)} = 0\} \\ &\quad +\#\{t|\Delta x_t^{(i-1)} = 0 \text{ and } \Delta x_t^{(i+1)} \neq 0\} \\ &\quad +\#\{u|\Delta x_u^{(i-1)} \neq 0 \text{ and } \Delta x_u^{(i+1)} \neq 0 \text{ and } x_u^{(i-1)} \neq x_u^{(i+1)}\} \\ &\leq H_w(\Delta X^{(i-1)}) + \#\{t|\Delta x_t^{(i-1)} = 0 \text{ and } \Delta x_t^{(i+1)} \neq 0\} \\ &\leq H_w(\Delta X^{(i-1)}) + H_w(\Delta X^{(i+1)}) \end{aligned}$$

Q.E.D.

補題 2 全ての *s-box* が全単射であるならば、線形変換層 P での *differential branch number* $\mathcal{B}_d$ は以下のように表すことができる：

$$\mathcal{B}_d = \min_{\Delta Z \neq 0}(H_w(\Delta Z) + H_w(\Delta Y)) = \min_{\Delta X \neq 0}(H_w(\Delta X) + H_w(\Delta Y))$$

ここで、ΔZ は線形変換層 P の入力差分を、ΔX, ΔY はラウンド関数の入力差分／出力差分をそれぞれ表す。

(proof)
s-box が全単射のとき、$s(x_i) \neq s(x_i')$, $x_i \neq x_i'$ より $\Delta z_i = s(x_i) \oplus s(x_i') \neq 0$ である。したがって、$\#\{\Delta x_i | x_i \neq 0\} = \#\{\Delta z_i | z_i \neq 0\}$ となるのは明らか。

Q.E.D.

定義 6 *SPN*型ラウンド関数を利用した *Feistel* 暗号について、r 段での差分特性確率は以下の関係式を満たす。

$$p_d^{(r)} \leq p_s^{\min_{(\Delta X^{(0)}, \Delta X^{(1)}, \ldots, \Delta X^{(r+1)}) \neq (0,0,\ldots)} \sum_{i=1}^{r} H_w(\Delta X^{(i)})}$$

ここで、$H_w(\Delta X^{(i)})$ は第 i 段目での *differentially active s-box* の個数を表す。

このように定義することにより、SPN 暗号の場合と同じように、差分特性確率の上限値を議論することとdifferentially active s-box の最少個数について議論をすることとが等価になる。そこで、これ以降の議論を簡単にするためにdifferentially active s-box の最少個数を以下のように表記することにする。また、$\mathcal{B}_d \geq 2$ と仮定する。

$$\mathcal{D}^{(r)} = \min_{(\Delta X^{(0)}, \Delta X^{(1)}, \ldots, \Delta X^{(r+1)}) \neq (0,0,\ldots)} \sum_{i=1}^{r} H_w(\Delta X^{(i)})$$

定理 1 任意の連続する *3* 段での *differentially active s-box* の最少個数は、$\mathcal{D}^{(3)} \geq 2$ を満たす。

(proof)

- $\Delta X^{(i)} = 0$ のとき、$\Delta Y^{(i)} = 0$ であるので、$\Delta X^{(i-1)} = \Delta X^{(i+1)}$ である。ゆえに、$\mathcal{D}_1^{(3)} = 2 \times H_w(\Delta X^{(i-1)}) \geq 2$ となる。
- If $\Delta X^{(i)} \neq 0$ のとき、補題 1より $\mathcal{D}_2^{(3)} \geq H_w(\Delta X^{(i)}) + H_w(\Delta Y^{(i)}) \geq \mathcal{B}_d$ となる。

Q.E.D.

定理 2 任意の連続する *4* 段での *differentially active s-box* の最少個数は、$\mathcal{D}^{(4)} \geq \mathcal{B}_d$ を満たす。

(proof)
連続する 2 段のラウンド関数への入力差分がゼロとなることはないので、以下の 8 通りの場合について検討すればよい。

(1) $\Delta X^{(1)} \neq 0, \Delta X^{(2)} \neq 0, \Delta X^{(3)} \neq 0, \Delta X^{(4)} \neq 0$

(2) $\Delta X^{(1)} = 0, \Delta X^{(2)} \neq 0, \Delta X^{(3)} \neq 0, \Delta X^{(4)} \neq 0$

(3) $\Delta X^{(1)} \neq 0, \Delta X^{(2)} = 0, \Delta X^{(3)} \neq 0, \Delta X^{(4)} \neq 0$

(4) $\Delta X^{(1)} \neq 0, \Delta X^{(2)} \neq 0, \Delta X^{(3)} = 0, \Delta X^{(4)} \neq 0$

(5) $\Delta X^{(1)} \neq 0, \Delta X^{(2)} \neq 0, \Delta X^{(3)} \neq 0, \Delta X^{(4)} = 0$

(6) $\Delta X^{(1)} = 0, \Delta X^{(2)} \neq 0, \Delta X^{(3)} = 0, \Delta X^{(4)} \neq 0$

(7) $\Delta X^{(1)} = 0, \Delta X^{(2)} \neq 0, \Delta X^{(3)} \neq 0, \Delta X^{(4)} = 0$

(8) $\Delta X^{(1)} \neq 0, \Delta X^{(2)} = 0, \Delta X^{(3)} \neq 0, \Delta X^{(4)} = 0$

(1) の場合、定理 1より $\mathcal{D}_1^{(4)} = \mathcal{D}_2^{(3)} + H_w(\Delta X^{(4)}) \geq \mathcal{B}_d + H_w(\Delta X^{(4)}) \geq \mathcal{B}_d + 1$ となる。

(2) の場合、$\Delta X^{(1)} = 0$ より $\Delta Y^{(2)} = \Delta X^{(3)}$ となる。よって、$\mathcal{D}_2^{(4)} = H_w(\Delta X^{(2)}) + H_w(\Delta Y^{(2)}) + H_w(\Delta X^{(4)}) \geq \mathcal{B}_d + H_w(\Delta X^{(4)}) \geq \mathcal{B}_d + 1$ となる。(3), (4), (5) の場合も同様。

(6) の場合、$\Delta X^{(1)} = \Delta X^{(3)} = 0$ より $\Delta Y^{(2)} = 0$ である。このことは、$\Delta X^{(2)} \geq \mathcal{B}_d$ であることを意味するから、$\mathcal{D}_6^{(4)} = H_w(\Delta X^{(2)}) + H_w(\Delta X^{(4)}) \geq \mathcal{B}_d + 1$ である。(8) の場合も同様。

(7) の場合、定理 1より $\mathcal{D}_7^{(4)} = \mathcal{D}_2^{(3)} \geq \mathcal{B}_d$ である。

Q.E.D.

さらに、上記の証明より以下の系が導かれる。

系 1 任意の連続する *4* 段での *differentially active s-box* の最少個数は、
(i) 1 段目と *4* 段目の入力差分がゼロのときに限り、$\mathcal{D}^{(4)} \geq \mathcal{B}_d$ を満たす。
(ii) それ以外の場合は、$\mathcal{D}^{(4)} \geq \mathcal{B}_d + 1$ を満たす。

定理 3 任意の連続する *6* 段での *differentially active s-box* の最少個数は、$\mathcal{D}^{(6)} \geq \mathcal{B}_d + 2$ を満たす。

(proof)

- $\Delta X^{(2)} \neq 0$、$\Delta X^{(5)} \neq 0$ のとき、定理 1より $\mathcal{D}_1^{(6)} = \mathcal{D}_2^{(3)} + \mathcal{D}_2^{(3)} \geq 2 \times \mathcal{B}_d$ となる。
- $\Delta X^{(2)} = \Delta X^{(5)} = 0$ のとき、$\Delta X^{(1)} = \Delta X^{(3)}$ かつ $\Delta Y^{(3)} = \Delta X^{(4)} = \Delta X^{(6)}$ となる。よって、$\mathcal{D}_2^{(6)} = 2 \times (H_w(\Delta X^{(3)}) + H_w(\Delta X^{(4)})) = 2 \times (H_w(\Delta X^{(3)}) + H_w(\Delta Y^{(3)})) \geq 2 \times \mathcal{B}_d$ となる。
- $\Delta X^{(2)} = 0$ かつ $\Delta X^{(5)} \neq 0$、もしくは $\Delta X^{(2)} \neq 0$ かつ $\Delta X^{(5)} = 0$ のとき、定理 1より $\mathcal{D}_3^{(6)} = \mathcal{D}_1^{(3)} + \mathcal{D}_2^{(3)} \geq \mathcal{B}_d + 2$ となる。

Q.E.D.

定理 4 任意の連続する *8* 段での *differentially active s-box* の最少個数は、$\mathcal{D}^{(8)} \geq 2 \times \mathcal{B}_d + 1$ を満たす。

(proof)

系 1より、任意の連続する 4 段での differentially active *s*-box の最少個数は、(i) 最初と最後の段の入力差分がゼロのときに限り $\mathcal{D}^{(4)} \geq \mathcal{B}_d$ であり、(ii) それ以外のときは $\mathcal{D}^{(4)} \geq \mathcal{B}_d + 1$ である。

一方、連続する 2 段の入力差分が同時にゼロになることはないので、(i)-(i) という連結が起こることはない。したがって、$\mathcal{D}^{(8)} \geq \mathcal{B}_d + (\mathcal{B}_d + 1) \geq 2 \times \mathcal{B}_d + 1$ である。

Q.E.D.

定理 5 任意の連続する *12* 段での *differentially active s-box* の最少個数は $\mathcal{D}^{(12)} \geq 3 \times \mathcal{P}_d + 1$ を満たす。

(proof)

$\mathcal{D}^{(12)}$ は $4 \times \mathcal{D}^{(3)}, 2 \times \mathcal{D}^{(6)}, \mathcal{D}^{(8)} + \mathcal{D}^{(4)}$ の 3 つの表現で表すことができる。しかし、これらは同じものを表現しているはずなので、$\mathcal{D}^{(12)} = \max\{4 \times \mathcal{D}^{(3)}, 2 \times \mathcal{D}^{(6)}, \mathcal{D}^{(8)} + \mathcal{D}^{(4)}\} \geq \mathcal{D}^{(8)} + \mathcal{D}^{(4)} \geq 3 \times \mathcal{B}_d + 1$ となる。

Q.E.D.

Knudsen は、最大差分特性確率の上界値が安全性閾値以下、すなわち 64-bit ブロック暗号なら 2^{-64}、128-bit ブロック暗号なら 2^{-128} 以下となるような Feistel 暗号を差分攻撃に対して安全 (practically secure) な暗号であると述べている。したがって、以下の系により、Camellia [1] は差分攻撃に対して practically secure な暗号であることが示される。

系 2 *s-box* の最大差分確率が $p_s = 2^{-6}$ で、*differential branch number* $\mathcal{B}_d = 5$ であるような *SPN* 型ラウンド関数を考える。このようなラウンド関数を利用した *128-bit Feistel* 暗号では少なくとも *16* 段で差分攻撃に有用な差分パスは存在しない。

(proof)
定義 6 と定理 4 より、$p_d^{(16)} \leq (2^{-6})^{2\times(2\times5+1)} = 2^{-132} < 2^{-128}$ となる。

Q.E.D.

4 Feistel 暗号の線形特性確率の上界値

本章では、前章と同じように線形特性確率の上界値を示す。ここでは、差分パスと線形近似との双対性 [2, 7] を利用し、線形特性確率の上界値を linearly active s-box の最少個数で評価することを考える。まず、そのための準備として以下の定理を導くことにする。

定理 6 *SPN* 型ラウンド関数を利用した *Feistel* 暗号において、線形変換層 P が全単射であるならば、ラウンド関数が *PSN* 型となる *Feistel* 暗号に等価変換可能である。

(proof)
線形変換層 P が全単射であることから、P による変換を $P(Z)$、逆変換を $P^{-1}(Z)$ と表す。
すでに述べているように、SPN 型ラウンド関数を利用したときの Feistel 暗号では、$X^{(i+1)} = X^{(i-1)} \oplus P(S(X^{(i)}))$ を満たしている。ここで、$V^{(i)} = P^{-1}(X^{(i)})$ とおくと、上式は、任意の (A, B, C) について $C = A \oplus P(B) \Leftrightarrow C = P(P^{-1}(A) \oplus B)$ となることから、以下のように変形できる。

$$\begin{aligned} X^{(i+1)} = X^{(i-1)} \oplus P(S(X^{(i)})) \quad &\Leftrightarrow \quad X^{(i+1)} = P(P^{-1}(X^{(i-1)}) \oplus S(X^{(i)})) \\ &\Leftrightarrow \quad P(V^{(i+1)}) = P(V^{(i-1)} \oplus S(P(V^{(i)}))) \\ &\Leftrightarrow \quad V^{(i+1)} = V^{(i-1)} \oplus S(P(V^{(i)})) \end{aligned}$$

最後の式 $V^{(i+1)} = V^{(i-1)} \oplus S(P(V^{(i)}))$ は明らかに PSN 型ラウンド関数を利用したときの Feistel 暗号での関係式を表している。したがって、平文 $(X^{(1)}, X^{(0)})$ を SPN 型ラウンド関数を利用した Feistel 暗号で暗号化した暗号文 $(X^{(r)}, X^{(r+1)})$ と、平文 $(X^{(1)}, X^{(0)})$ を P^{-1} で変換した $(V^{(1)}, V^{(0)})$ に対して PSN 型ラウンド関数を利用した Feistel 暗号で暗号化して $(V^{(r)}, V^{(r+1)})$ を得た後、P で再変換することによって得られる暗号文 $(X^{(r)}, X^{(r+1)})$ とが等しいこと示される。

Q.E.D.

ここで、差分パスと線形近似との双対性を利用して differential branch number $\mathcal{B}_d$ と同じように、linear branch number $\mathcal{B}_l$ を表す。なお、線形変換層 P に対するマスク値拡散層 P^* が存在する、すなわち $\Delta Y = P(\Delta Z)$, $\Gamma Z = P^*(\Gamma Y)$ を同時に満たす線形変換層 P であると仮定する。

補題 3 線形変換層 P での *linear branch number* $\mathcal{B}_l$ は仮定より以下のように表すことが出来る：

$$\mathcal{B}_l = \min_{\Gamma Y \neq 0} (H_w(P^*(\Gamma Y)) + H_w(\Gamma Y)) = \min_{\Gamma Y \neq 0} (H_w(\Gamma Z) + H_w(\Gamma Y))$$

ここで、ΓY, ΓZ は線形変換層 P の出力マスク値／入力マスク値をそれぞれ表す。

さらに、前章と同様に、最大線形確率の上界値を linearly active s-box の最少個数を用いて表すために、以下の関係式を定義する。

定義 7 *SPN* 型ラウンド関数を利用した *Feistel* 暗号において、r 段での線形特性確率は以下の関係式を満たす。

$$p_l^{(r)} \leq p_s^{\min_{(\Gamma Y^{(0)}, \ldots, \Gamma Y^{(r)}, \Gamma Y^{(r+1)}) \neq (\ldots, 0, 0)} \sum_{i=1}^{r} H_w(\Gamma Z^{(i)})}$$

ここで、$H_w(\Gamma Z^{(i)})$ は第 i 段目での *linearly active s-box* の個数を表す。

これ以降の議論を簡単にするために、linearly active s-box の最少個数を以下のように表記する。また、$\mathcal{B}_l \geq 2$ と仮定する。

$$\mathcal{L}^{(r)} = \min_{(\Gamma Y^{(0)}, \ldots, \Gamma Y^{(r)}, \Gamma Y^{(r+1)}) \neq (\ldots, 0, 0)} \sum_{i=1}^{r} H_w(\Gamma Z^{(i)})$$

定理 7 *SPN*型ラウンド関数を利用した*Feistel*暗号を考える。このとき、全ての*s-box*と線形変換層Pが全単射であるならば、$\mathcal{L}^{(r)}$および$\mathcal{B}_l$に関しても定理*1*から定理*5*が同様に成立する。

(proof)

線形変換層Pが全単射であるので、定理6によって、SPN型ラウンド関数を利用したFeistel暗号はPSN型ラウンド関数を利用したFeistel暗号に変形できる。このとき、変形した暗号は、以下のような関係式で記述できる。

$$V^{(i+1)} = V^{(i-1)} \oplus S(P(V^{(i)})) = V^{(i-1)} \oplus S(X^{(i)}) = V^{(i-1)} \oplus Z^{(i)}$$

ここで、$V^{(i)} = P^{-1}(X^{(i)})$, $Z^{(i)} = S(X^{(i)})$である。

また、差分パスと線形近似との双対性により、変形した暗号のラウンド関数の線形近似は、concatenation rules [2, 7] を使うことによって以下のように表現することが出来る。

$$\Gamma V^{(i)} = \Gamma Z^{(i-1)} \oplus \Gamma Z^{(i+1)} = P^*(\Gamma X^{(i)})$$

一方、全てのs-boxが全単射であることから、linearly active s-boxとなるs-boxの入力マスク値Γx_iと出力マスク値Γz_iは互いに非ゼロである。したがって、$H_w(\Gamma X) = H_w(\Gamma Z)$を満たす。ゆえに、変形した暗号のlinear branch number $\mathcal{B}_l$は以下のように再定義できる。

$$\mathcal{B}_l = \min_{\Gamma X \neq 0}(H_w(P^*(\Gamma X)) + H_w(\Gamma X)) = \min_{\Gamma Z \neq 0}(H_w(\Gamma V) + H_w(\Gamma Z))$$

以上より、$\Delta X^{(i)}$と$\Delta Y^{(i)}$をそれぞれ$\Gamma Z^{(i)}$と$\Gamma V^{(i)}$に置き換えることによって、定理1から定理5までの証明と同様の証明をつけることが出来る。

Q.E.D.

例えば、Camelliaにおける線形変換層Pおよびマスク値拡散層P^*は、以下のように表記できる。

$$P_{Camellia} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \quad P^*_{Camellia} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

したがって、$\mathcal{B}_d = \mathcal{B}_l = 5$であることがわかるので、以下の系が成立する。

系 3 少なくとも*16*段以上の*Camellia*について、線形攻撃に有用な線形近似は存在しない。

(proof)

*Camellia*でのs-boxの最大線形確率は$q_s = 2^{-6}$であり、かつ$\mathcal{B}_l = 5$である。よって、定理7より少なくとも16段以上のCamelliaでの最大線形特性確率の上界値は2^{-132}となる。

Q.E.D.

5 まとめ

本稿では、SPN型ラウンド関数を利用したFeistel暗号における最大差分／線形特性確率の上界値について考察した。ここで利用したテクニックは、SPN暗号でのbranch numberを利用したdifferentially/linearly active s-boxesの最少個数によって最大差分／線形特性確率の上界値を評価する手法と同様の考え方をFeistel暗号に適用したことである。これにより、SPN型ラウンド関数を利用したFeistel暗号においても、s-boxの最大差分／線形確率とdifferential/linear branch numberおよび段数を用いてKnudsenの結果よりも厳密な最大差分／線形特性確率の上界値が与えられた。

本稿の結果として、3、4、6、8、12段のFeistel暗号のdifferentially/linearly active s-boxesの最少個数は、それぞれ$2, \mathcal{B}_d\ (\mathcal{B}_l), \mathcal{B}_d + 2\ (\mathcal{B}_l + 2), 2\mathcal{B}_d + 1\ (2\mathcal{B}_l + 1), 3\mathcal{B}_d + 1\ (3\mathcal{B}_l + 1)$となる。このことは、4段ごとにほぼdifferentail/linear branch numberの個数分だけdifferentially/linearly active s-boxの個数が増加していくことを示している。すなわち、differentially/linearly active s-boxから算出する最大差分／線形特性確率の上界値を利用した差分攻撃／線形攻撃に対する安全性評価の観点からは、r段のSPN暗号と$2r$段のFeistel暗号がほぼ同等の評価になることが理論的に確認されたことになる。

References

[1] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "*Camellia* – A 128-bit Block Cipher," *IEICE Technical report*, ISEC2000-6, May, 2000.

[2] E. Biham, "On Matsui's Linear Cryptanalysis," *Advances in Cryptology — EUROCRYPT'94*, LNCS **950**, pp.341–355, Springer-Verlag, Berlin, 1995.

[3] E. Biham, and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, Vol.4, No.1, pp.3–72, 1991. (The extended abstract appeared at *CRYPTO'90*)

[4] L. R. Knudsen, "Practically Secure Feistel Ciphers," *Fast Software Encryption — Cambridge Security Workshop*, LNCS **809**, pp.211–221, Springer-Verlag, Berlin, 1994.

[5] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, and K. Ohta, "A strategy for constructing fast round functions with practical security against differential and linear cryptanalysis," *Selected Areas in Cryptography — 5th Annual International Workshop, SAC'98*, LNCS**1556**, pp.264–279, Springer-Verlag, Berlin, 1999.

[6] M. Matsui, "Linear cryptanalysis method for DES cipher," *Advances in Cryptology — EUROCRYPT'93*, LNCS**765**, pp.386–397, Springer-Verlag, Berlin, 1994.

[7] M. Matsui, "On Correlation Between the Order of S-boxes and the Strength of DES," *Advances in Cryptology — EUROCRYPT'94*, LNCS **950**, pp.366–375, Springer-Verlag, Berlin, 1995.

[8] V. Rijmen, J. Daemon, B. Preneel, A. Bosselaers, and E.D. Win, "The cipher SHARK," *Fast Software Encryption — Third International Workshop*, LNCS**1039**, pp.99–111, Springer-Verlag, Berlin, 1996.