擬似乱数生成器 MUGI の安全性に関する
詳細調査報告書

2002 年 9 月 16 日

東京理科大学

金子 敏信

疑似乱数生成器 MUGI
の安全性に関する詳細調査報告書

平成 14 年 9 月 16 日

概 要

本報告書はストリーム暗号 MUGI に関し、安全性の側面から考察を加えたものである。自己評価書にある安全性評価は、概ね妥当なものであると考える。さらに D.Coppersmith らの Linear masking の手法を適用した。彼らの解析した SNOW には非線形部から線形部への帰還が無いが、MUGI にはそれが存在し、解析が複雑となる。ここでは、MUGI の線形部を線形動的システムとして捉え解析した。D.Coppersmith と同様に distiguisher として線形近似式を取り上げ、その最良線形確率を truncate linear 特性確率を計算機探索により評価した。非線形部から線形部への帰還入力が無いならば、線形動的システムの零入力応答で評価され、線形部の周期は 48 であり、D.Coppersmith の手法で、攻撃できる可能性が残るが、帰還信号まで考慮した場合は、truncate linear 特性確率評価では、活性 S-box 数の最小値は 23 であり、各 S-box の最大線形確率が 2^{-6} であることを顧慮すると、最大線形特性確率は 2^{-138} となり、この攻撃に対して安全であると言える。

1 はじめに

MUGI は 2001 年に株式会社日立製作所によって提案されたストリーム暗号向けの疑似乱数生成器 [1] である。提案者らは自己評価書 [2] において様々な観点から評価を行いその安全性を示している。提案者らの評価は概ね適切であると考える。一方で、D.Coppersmith らは"Cryptanalysis of stream ciphers with linear masking"[3] において SNOW に対して、linear masking を用いての真の乱数と出力乱数を区別する一手法を示し、その攻撃の MUGI への適用可能性を示唆している。

そこで我々は [3] の攻撃手法を MUGI へ適用することを試み、この攻撃に対する耐性評価を中心に検討を行った。

2 MUGI の構造[1]

MUGI は秘密鍵、初期ベクトル共に 128bit、出力ユニット長 n(自然数) を入力として持ち、n ユニットの乱数列を出力する。ここで言うユニットとは 64bit のデータブロックのことである。

2.1 内部状態

MUGI の内部状態はステート、バッファと呼ばれるの 2 つの部分で構成されている。時刻 t における各ユニットを以下のように表す。

- ステート a は 3 ユニットで構成され、上位からそれぞれ $a_0^{(t)}$,$a_1^{(t)}$,$a_2^{(t)}$ と表す。
- バッファb は 16 ユニットで構成され、上位からそれぞれ $b_0^{(t)}$,$\cdots$,$b_{15}^{(t)}$ と表す。

時刻 t から時刻 $(t+1)$ へのこれらの変数の処理をラウンドと呼ぶ。

2.2 全体構造

ρ 関数はステート a の状態遷移関数で、バッファb の出力である $b_4^{(t)}, b_{10}^{(t)}$ を鍵入力 $\boldsymbol{k^{(t)}}$ に持つ (図 1)。図中の $<<< m$ は m bit の左巡回シフト、C_1, C_2 は定数である。ρ 関数に含まれる F 関数を図 2 に示す。F 関数は AES で使用されている S-box と MDS 行列による行列変換 M、さらにバイト置換を内部構造として持つ非線形関数である。それは、バッファb をからの鍵入力 $\boldsymbol{k^{(t)}}$ を使ってステート a の更新を行う。

λ 関数はバッファb の状態遷移関数で、ステート a の一部である $a_0^{(t)}$ を入力に持つ線形関数である (図 3)。

MUGI の状態遷移関数 $Update$ は ρ 関数と λ 関数の組み合わせで記述される。

$$(a^{(t+1)}, b^{(t+1)}) = Update(a^{(t)}, b^{(t)}) = (\rho(a^{(t)}, b^{(t)}), \lambda(b^{(t)}, a^{(t)})) \tag{1}$$

MUGI は初期化の完了後、MUGI 全体の状態遷移を繰り返しながら、ラウンド t において $a_2^{(t)}$を乱数列 $Out[t]$ として出力する。

$$Out[t] = a_2^{(t)} \tag{2}$$

[1] 詳細は仕様書 [1] 参照

3 提案者らの評価 [2]

提案者らは自己評価書 [2] において様々な観点から評価を行い、その安全性を示している。その評価は §3.3.2 の線形解読法の適用、§3.4 の再同期攻撃を除き概ね妥当であると考える。§3.4 は初期化段階での評価が不十分であると考える。§3.4 に関しては提案者らが”鍵ストリーム生成器 MUGI の安全性評価 (1)”[4] において再評価を行い、再同期攻撃の適用は困難であることを示しており、その評価は妥当であると考える。一方、§3.3.2 は誤植及び複雑な安全性証明のため的確な理解が困難である。そこで、本報告書では D.Coppersmith らの”Cryptanalysis of stream ciphers with linear masking”の手法を適用し、安全性評価を行った。

4 Cryptanalysis of stream ciphers with linear masking[3]

D.Coppersmith らは [3] において、線形部と非線形部からなる疑似乱数生成器に対し出力乱数と真の乱数と区別する手法を示している。その手法は以下の手順に分かれている。

1. 非線形部に対しては真の乱数と区別できる $L(y(t), r(t))$ で線形性を持つものを探索する。ただし、$y(t)$ は線形部から非線形部への出力、$r(t)$ は乱数出力である。
2. $\sum C(t) \cdot y(t) = 0$ となる係数列 $C(t)$ を探索する。
3. $y(t)$ の項を消去した関数 $\sum C(t) \cdot L(y(t), r(t)) = M(r(t))$ を distingisher として使用し攻撃する。

ここで distingishier の有用性は $r(t)$ が真の乱数の時と、$r(t)$ が疑似乱数の時の $M(r(t))$ の出力の差の期待値 (これを統計距離と呼んでいる) で評価される。線形解読の場合、1 の step で線形近似式を採用するならば 3 の step で用いられる distingishier の有用性は線形特性確率となる。

彼らは SNOW に対し distingishier として線形近似式を採用し、出力乱数と真の乱数と区別している。

5 MUGI への適用

MUGI は、線形部である λ 関数と、非線形部である ρ 関数からなる構造を有している。線形部は時刻とともに、内部状態であるバッファ b が動的に変化しており、これらの値を直接観測することはできない。一方、非線形プロセスについては時刻 t において乱数出力である $Out[t]$ のみ直接観測が可能である。

D.Coppersmith らの解析した SNOW の場合、非線形部から線形部への帰還入力がないが、MUGI の場合それが存在し、解析が複雑となる。

我々は以下の手順に基づき、MUGI へ [3] の提案する攻撃手法の適用の可能性を考察する。

1. 非線形部である ρ 関数のみを取り出し、$L(k(t), Out(t))$ として線形近似式を採用する。ただし、$k(t)$ は線形部から非線形部への出力である。
2. 線形部である λ 関数のみを取り出し、線形動的システムと捉える。そこにおいては非線形部への鍵出力 $\boldsymbol{k^{(t)}}$ を出力変数、非線形部から供給される信号 $a_0^{(t)}$ を入力変数、バッファ b を状態変数とする。出力変数と入力変数からなる線形関係式として、係数列 $C(t)$ を導出する。

3. $k(t)$ の項を消去した関数 $\sum C(t) \cdot L(k(t), Out(t)) = M(out(t))$ を distingisher として使用し攻撃耐性の評価を行う。

本報告書では、1 の setp で $L(\cdot)$ として線形近似式を取り上げているので、攻撃耐性は線形特性確率で評価される。

6 非線形部 (ρ 関数) の解析

本章では F 関数の線形特性について考え、ρ 関数の線形特性を F 関数の組み合わせにより導出する。ここでは 64bit を一まとめとする truncate linear 解析で評価し、その線形確率は F 関数の active S-box 数で評価する。

6.1 F 関数の線形特性

F 関数の構造は図 2 である。行列 M の最小分岐数は 5 であり、S-box の最大線形確率は 2^{-6} である。自己評価書にもあるように、2 つの F 関数を近似する線形パス ($\Gamma_0 \xrightarrow{F} \Gamma_1 \xrightarrow{F} \Gamma_2$) を考えると、行列 M の最小分岐数が 5 であることから active S-box の最小個数は 5 個で最大線形特性確率は 2^{-30} となる。また、上記パスで $\Gamma_0 = \Gamma_2$ となる場合には、F 関数のバイト置換により、さらに active S-box 数が多くなる。この場合の active S-box の最小個数は 10 となり、最大線形特性確率は 2^{-60} となる。

6.2 ρ 関数の線形特性

6.2.1 ρ 関数の等価変形

評価を容易にするために ρ 関数の等価変形を行う (図 4)。図中では F 関数の一方を G と表記している。線形特性を考えているので定数 C_1, C_2 の排他的論理和は無視する。以降、等価変形した ρ 関数を単に ρ 関数と呼ぶこととする。また、時刻 t_n の F 関数と時刻 $(t_n + 1)$ の G 関数を一組として、ラウンド t_n と表すこととする。

6.2.2 ρ 関数の線形パス

以降、ラウンド t_n における active S-box 数の下限を $as^{(t_n)}$ と表す。ラウンド t を近似するすべての線形パスを図 5〜7 に示す。なお、図中の t はラウンド t を明示するものである。太線は active な線形パスを表す。また、A における点線は少なくともどちらか一方が active である線形パスを表す。Case 1〜Case 4 は A の線形パスに関わらず $as^{(t)}$ が一意に定まる。図中に $as^{(t)}$ を併せて示す。Case 5,Case 6 は A の線形パスとラウンド $(t-1)$ の線形パスにより $as^{(t)}$ が異なった値となる。ラウンド t において Case5 では Case7 となる線形パスを除き $as^{(t)} = 1$、Case6 では Case8 となる線形パスを除き $as^{(t)} = 1$ である。Case7、Case8 のみラウンド $(t-1)$ がラウンド t に影響を与え、$as^{(t)} = 4$ となる。

7　線形部 (λ 関数) の解析

ここでは、λ 関数を線形動的システムと捉えて解析を行う。状態変数、入力変数、出力変数をそれぞれ以下のように捉える。

- 状態変数 $\boldsymbol{b}^{(i)}$: i ラウンドのバッファの値

$$\boldsymbol{b}^{(i)} = \begin{pmatrix} b_0^{(i)} & b_1^{(i)} & b_2^{(i)} & \cdots & b_{15}^{(i)} \end{pmatrix} \tag{3}$$

$$b_j^{(i)} \in GF(2^{64}) \qquad (j = 0 \cdots 15)$$

- 入力変数 $a_0^{(i)}$: i ラウンドの ρ 関数からの入力

$$a_0^{(i)} \in GF(2^{64})$$

- 出力変数 $\boldsymbol{k}^{(i)}$: i ラウンドの ρ 関数への鍵出力

$$\boldsymbol{k}^{(i)} = \begin{pmatrix} k_0^{(i)} & k_1^{(i)} \end{pmatrix} \tag{4}$$

$$k_j^{(i)} \in GF(2^{64}) \qquad (j = 0, 1)$$

λ 関数において、$<<<$ 32 が用いられているが、これをオペレーター s で表す。すなわち変数 $x \in GF(2^{64})$ に対し、

$$s \cdot x = x <<< 32 \tag{5}$$

を表す。なお、s^2は $s \circ s$=1 の恒等変換である。

7.1　状態方程式

λ 関数は線形動的システムであり、次の状態方程式と出力方程式で表すことができる。

$$\boldsymbol{b}^{(i+1)} = \boldsymbol{A} \cdot \boldsymbol{b}^{(i)} + \boldsymbol{B} \cdot a_0^{(i)} \tag{6}$$

$$\boldsymbol{k}^{(i)} = \boldsymbol{C} \cdot \boldsymbol{b}^{(i)} \tag{7}$$

ここで、$\boldsymbol{A}$ は 16×16 のシステム行列であり、$\boldsymbol{B}$ は 16×1 の駆動行列であり、$\boldsymbol{C}$ は 2×16 の出力行列である。それらは $GF(2^{64})$ 上の行列であり、各要素は MUGI の定義より、以下のようになる。

$$
\boldsymbol{A} = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & s & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
$$

$$
\boldsymbol{B} = \begin{pmatrix}
1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0
\end{pmatrix}
$$

$$
\boldsymbol{C} = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
$$

7.1.1 零入力応答

線形動的システムである λ 関数において、入力変数 $a_0^{(i)} = 0 \quad (i = 0 \cdots)$ の時の状態変数 $\boldsymbol{b}^{(n)}$ は初期状態 $\boldsymbol{b}^{(0)}$ を用いて、

$$
\boldsymbol{b}^{(n)} = \boldsymbol{A}^n \cdot \boldsymbol{b}^{(0)} \tag{8}
$$

と表される。

7.1.2 強制入力がある場合の応答

入力変数 $a_0^{(i)}$ が非零の場合のシステム出力は一般に以下の式で表される。

$$\boldsymbol{k}^{(n)} = \boldsymbol{C} \cdot \left(\boldsymbol{A}^n \cdot \boldsymbol{b}^{(0)} + \sum_{j=0}^{n-1} \boldsymbol{A}^{n-j-1} \cdot \boldsymbol{B} \cdot a_0^{(j)} \right) \tag{9}$$

7.2 λ 関数の周期

$\boldsymbol{A}$ は $GF(2^{64})$ の行列であることと、式 (5) に注意し、$\boldsymbol{A}^n$ を順次計算するならば、n=48 で初めて、単位行列となる。したがって、零入力時の λ 関数の周期は 48 である。

7.3 λ 関数の線形特性

ここでは、入出力変数の線形和が 0 となる関係式を導出し、以降これを消去関係式と呼ぶ。システム出力の一般解は式 (9) で与えられ、これを時刻 0 から t まで連立し、状態変数 $b^{(j)}$ を消去する。特定時刻で $k_0^{(0)}$,$k_1^{(0)}$, を含む最短のものを導出すると、以下の 2 つの式となる [2]。

$$k_0^{(0)} + s \cdot k_1^{(1)} + k_1^{(5)} = 0 \tag{10}$$

$$k_1^{(0)} + k_1^{(7)} + k_0^{(11)} + a_0^{(5)} = 0 \tag{11}$$

すべての消去関係式は式 (10),(11) を時刻ごとにずらした関係式の線形結合で表現される。これらの線形結合の係数を式 (10) については $(C_{k_0}^{(0)}, C_{k_0}^{(1)}, \cdots, C_{k_0}^{(t)})$、式 (11) については $(C_{k_1}^{(0)}, C_{k_1}^{(1)}, \cdots, C_{k_1}^{(t)})$ と表す。ここで、t は時刻を表し、$t = 0, 1, 2 \cdots$ である。

8 MUGI に対する線形解読の適用

MUGI はブロック暗号とは異なりラウンド数が固定されていないので、計算機を使って全ての線形パスを探索することは困難である。8.2 では動的計画法 (DP) を用いた場合、ある条件が満たされる有限ラウンドまでの探索で十分であることを示す。さらに計算量を減らすため、6,7 節の解析をもととして 8.1 に示すアルゴリズムを用いて active S-box の数の下限を与える線形パスを 64bit を一まとめとした truncate liner 解析により探索した。以降、全体の active S-box の数を AS と表記し、$AS = \sum as^{(t)}$ である。

8.1 探索アルゴリズム

以降、ラウンド t_n の F 関数,G 関数のアクティブ状態を $F^{(t_n)}$,$G^{(t_n)}$ と表す。ラウンド t_n の $as^{(t_n)}$ は以下のパラメータと図 5〜図 7 により一意に定まる。ここでは 64bit truncation を想定しているため以下のパラメータは 1bit の値を持つ。

[2] 式 (10),(11) の導出過程は付録に示す。

- $F^{(t_n)}, G^{(t_n)} \in \{0,1\}$
- $F^{(t_n-1)}$,$G^{(t_n-1)} \in \{0,1\}$
- $a_1^{(t_n)} \in \{0,1\}$
- $a_1^{(t_n+1)} \in \{0,1\}$
- $(C_{k_0}^{(t_n)}, C_{k_0}^{(t_n-1)}, \cdots, C_{k_0}^{(t_n-5)})$

$$C_{k_0}^{(t_n-i)} \in \{0,1\} \quad (i = 0 \cdots 5)$$

- $(C_{k_1}^{(t_n)}, C_{k_1}^{(t_n-1)}, \cdots, C_{k_1}^{(t_n-11)})$

$$C_{k_1}^{(t_n-i)} \in \{0,1\} \quad (i = 0 \cdots 11)$$

これらのパラメータを状態と考え、トレリス線図を書くことができる。

始点ラウンドが t_s であり、終点ラウンドが t_e である、閉じる truncate 線形パス考える。これは $(t_s - 1)$ における状態が 0 であり、なおかつ $(t_e + 1)$ における状態が 0 であることに相当する。前述の条件下で AS を最小とする非自明な truncate 線形パスを動的計画法によって探索する。具体的にはビタビ復号法 [6] の手順を応用した。

8.2 探索すべきラウンドの上限

ラウンド t_s で始まり、ラウンド $(t_s + M)$ 以内で閉じる truncate 線形パスの AS の下限を AS_{min} とする時、時刻 M の全ての状態において AS が AS_{min} 以上となるならば、以降のラウンドではどのような truncate 線形パスとなったとしても、AS は AS_{min} 以下とならない。すなわち、この時の AS_{min} が MUGI の active S-box 数の下限となる。さらに、前述の条件が成り立つラウンドが探索すべきラウンドの上限である。

8.3 探索結果

計算機で探索を行った結果、閉じる線形パスの AS の下限は 23 であり、110 ラウンドで全ての状態における AS の下限が 23 を超える。110 ラウンド以内の閉じる線形パスの AS の下限を表 1 に示す。閉じる線形パスの AS の下限が 23 となる最短のラウンド数は表 1 より 14 ラウンドであり、最長のラウンド数は 25 である。それぞれの一例を図 8,9 に示す。図中に各ラウンド数と () 内にそのラウンドにおいて増加する $as^{(t)}$ を併せて表示する。なお、図 9 については λ 関数の truncate 線形パスに関しては図を省略する。

8.4 MUGI の最大線形特性確率

以上の結果、本評価手法で示し得る AS の下限は 23 個であることから、S-box の最大線形確率が 2^{-6} であることを考慮すると、MUGI の最大線形特性確率の上界は $(2^{-6})^{23} = 2^{-138}$ となる。

9 結論

本稿では、D.Coppersmith らの提案する Linear masking の手法を MUGI に対し適用することを試みた。この際、非線形部である ρ 関数については D.Coppersmith と同様に distinguisher として線形近似式を取り上げ、線形部である λ 関数についてはこれを線形動的システムとして捉え解析した。その上で、64bit を一まとめとする truncate linear 解析により最大線形特性確率の上界を導出した。

結果、本評価手法で示し得る active S-box 数の下限は 23 個となる。S-box の最大線形確率が 2^{-6} であることを顧慮すると、示し得る最大線形特性確率の上界は 2^{-138} となり、2^{-128} を下回る。したがって、D.Coppersmith らの提案する攻撃 [3] に対して MUGI は十分な耐性を持つと結論付ける。

参考文献

[1] 株式会社 日立製作所「疑似乱数生成器 MUGI 仕様書 Ver. 1.3」(2002)

[2] 株式会社 日立製作所「疑似乱数生成器 MUGI 自己評価書」(2001)

[3] D.Coppersmith, S.Halevi, and C.Jutla, "Cryptanalysis of stream ciphers with linear masking", ePrint@IACR February 16,2002

[4] 渡辺　大, 古屋聡一, 吉田博隆, 宝木和夫「鍵ストリーム生成器 MUGI の安全性評価 (1)」SCIS2002

[5] 正田英介「制御工学」培風館 (1982)

[6] 江藤良純, 金子敏信「誤り訂正符号とその応用」オーム社 (1996)

ラウンド	AS の下限	ラウンド	AS の下限	ラウンド	AS の下限	ラウンド	AS の下限
1	-	31	25	61	29	91	33
2	-	32	26	62	29	92	34
3	-	33	25	63	30	93	33
4	-	34	26	64	30	94	33
5	-	35	26	65	30	95	34
6	-	36	25	66	29	96	34
7	-	37	26	67	30	97	34
8	-	38	26	68	30	98	33
9	-	39	26	69	30	99	34
10	-	40	26	70	30	100	35
11	-	41	26	71	31	101	34
12	29	42	27	72	31	102	34
13	26	43	27	73	31	103	35
14	23	44	26	74	30	104	35
15	24	45	27	75	31	105	35
16	24	46	27	76	31	106	34
17	23	47	28	77	31	107	35
18	24	48	27	78	31	108	36
19	25	49	27	79	32	109	35
20	23	50	27	80	32	110	35
21	23	51	28	81	32		
22	23	52	28	82	31		
23	25	53	28	83	32		
24	25	54	28	84	33		
25	23	55	29	85	32		
26	24	56	29	86	32		
27	25	57	29	87	33		
28	24	58	28	88	33		
29	24	59	29	89	33		
30	25	60	29	90	32		

表 1: 各ラウンドで閉じる線形パスの AS の下限

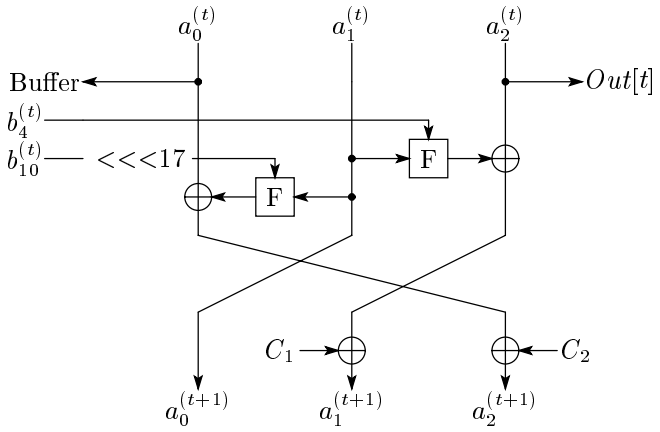


図 1: MUGI の ρ 関数

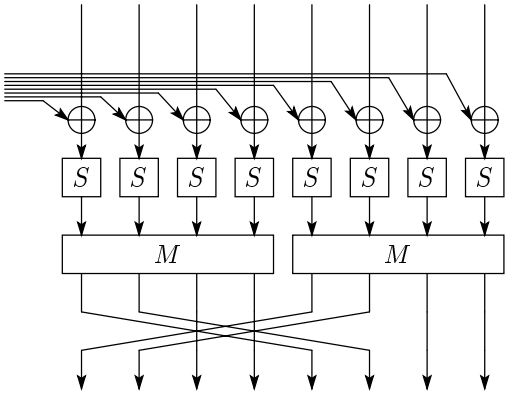


図 2: MUGI の F 関数

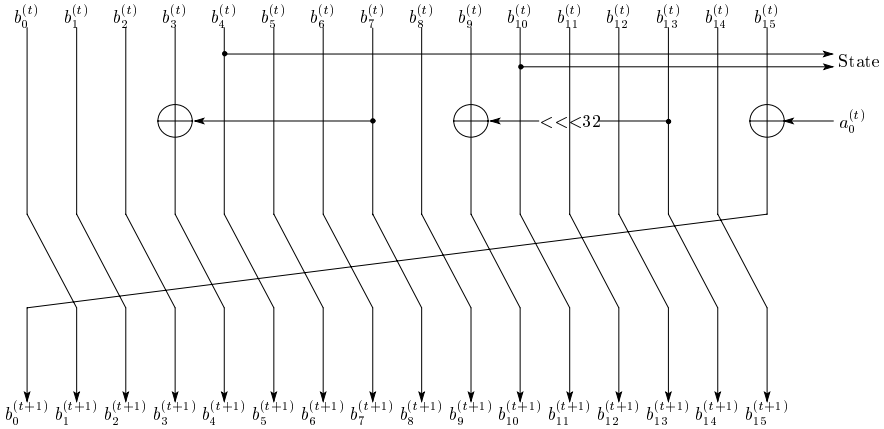


図 3: MUGI の λ 関数

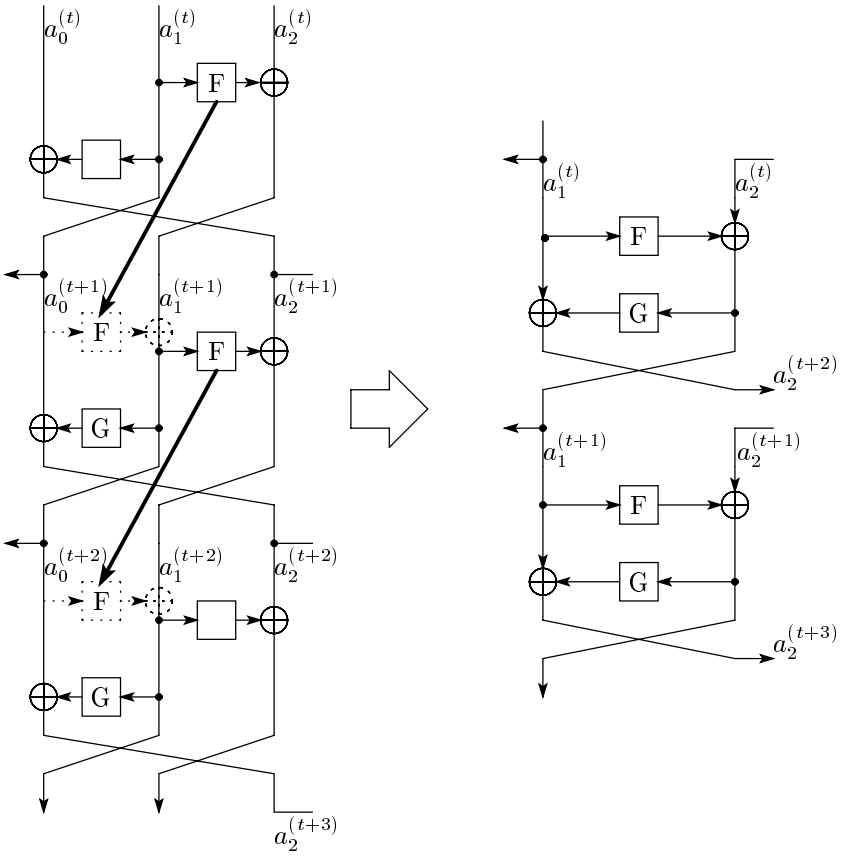
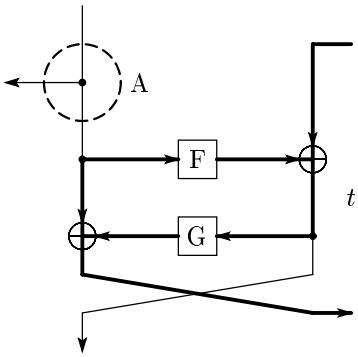
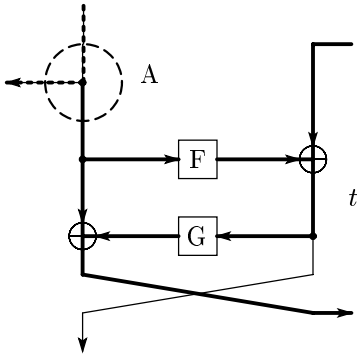


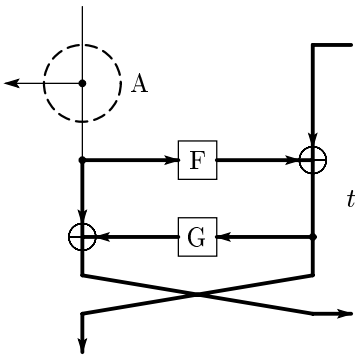
図 4: ρ 関数の等価変形



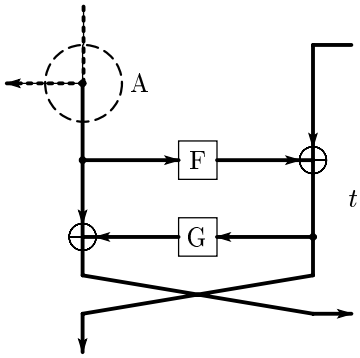
Case 1:
$as^{(t)} = 10$



Case 2:
$as^{(t)} = 5$

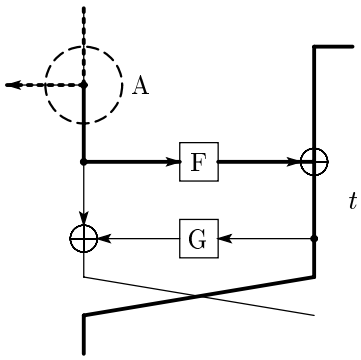


Case 3:
$as^{(t)} = 5$

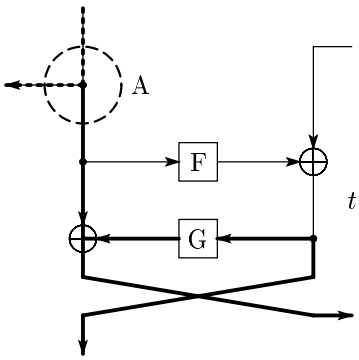


Case 4:
$as^{(t)} = 2$

図 5: ρ 関数の線形パス (1)

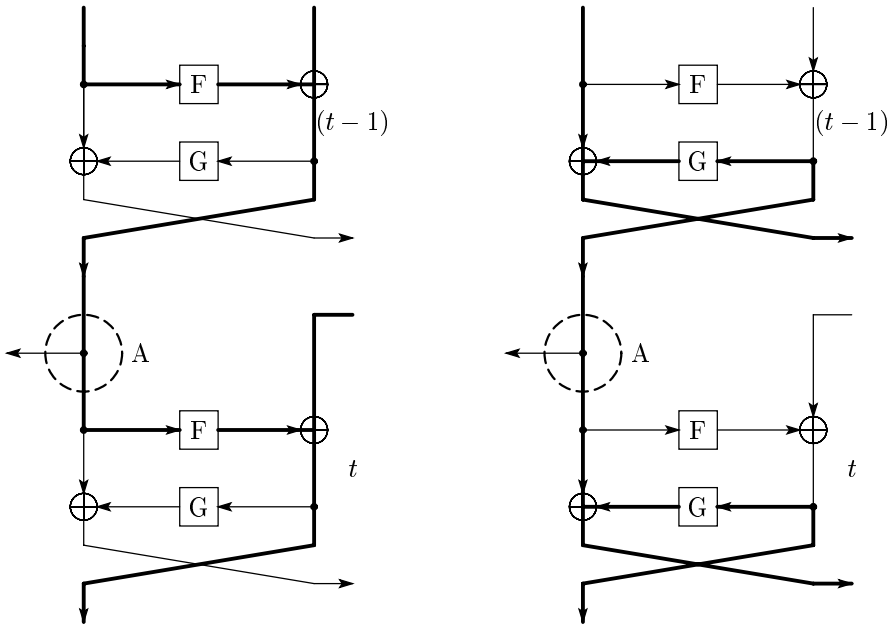


Case 5:
$as^{(t)} = 1$(Case 7 は除く)



Case 6:
$as^{(t)} = 1$(Case 8 は除く)

図 6: ρ 関数の線形パス (2)



Case 7:
$as^{(t)} = 4$

Case 8:
$as^{(t)} = 4$

図 7: ρ 関数の線形パス (3)

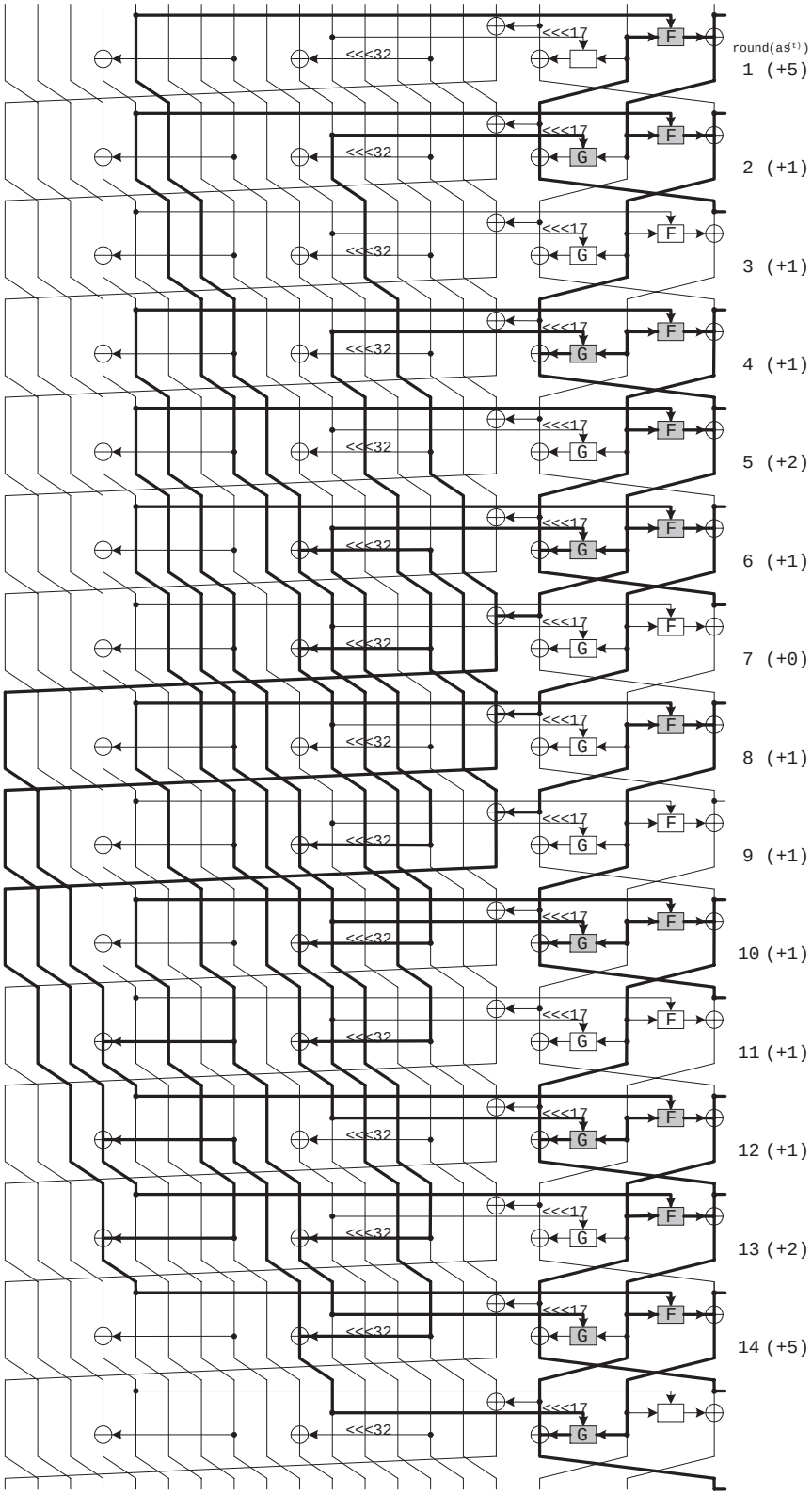


図 8: 全体の active S-box 数の下限が 23 となる truncate 線形パス (1)

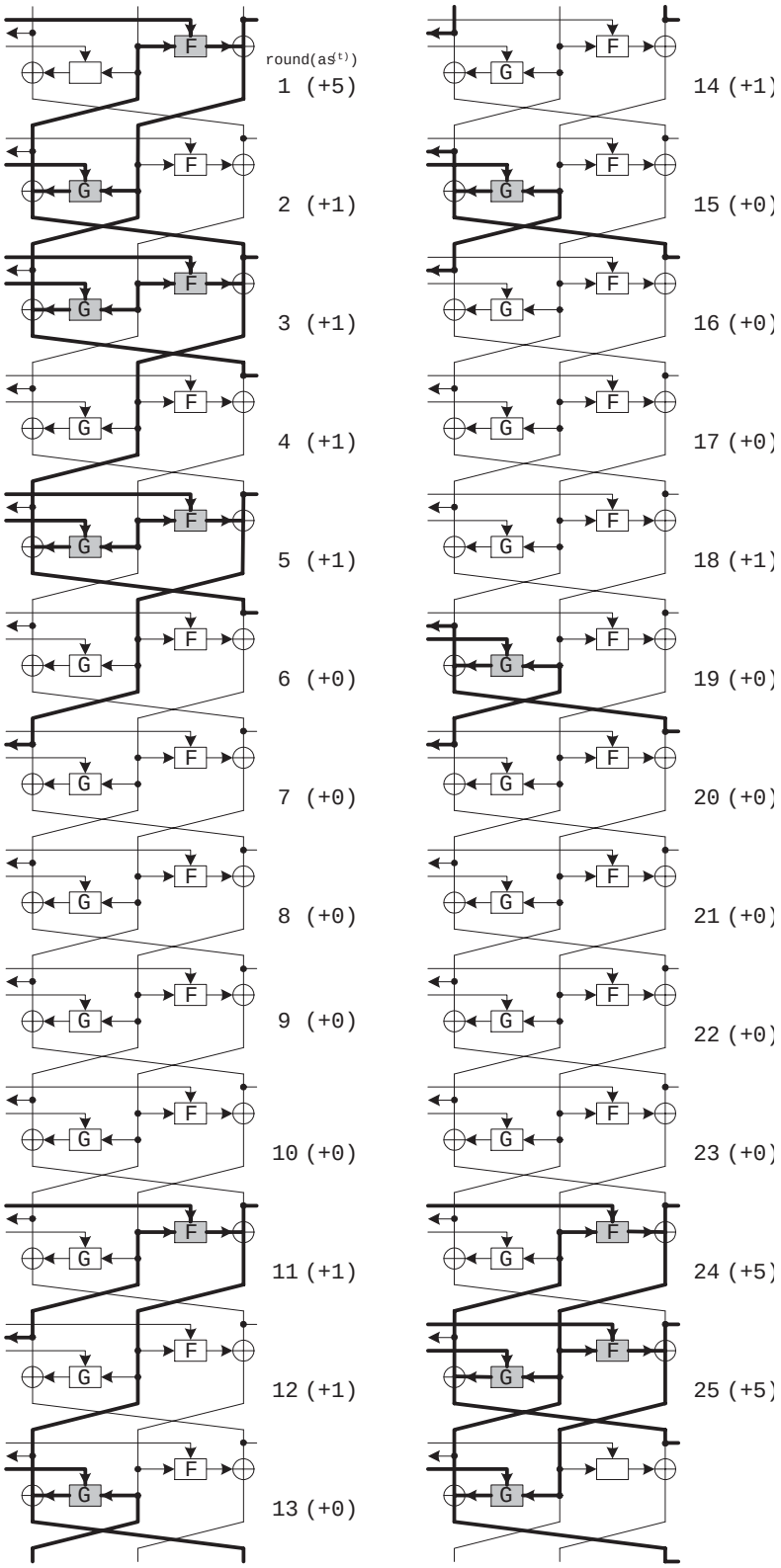


図 9: 全体の active S-box 数の下限が 23 となる truncate 線形パス (2)

付録

7.3 節で示す式 (8),(9) の導出過程を示す。ここでは、時刻 0 から 15 までのシステム出力の一般解である式 (7) を連立し、式 (8),(9) を導出する。

消去関係式の導出過程

(7) 式の左辺を右辺に移項すると、

$$\boldsymbol{C}\cdot\left(\boldsymbol{A}^{n}\cdot\boldsymbol{b}^{(0)}+\sum_{j=0}^{n-1}\boldsymbol{A}^{n-j-1}\cdot\boldsymbol{B}\cdot a_0^{(j)}\right)+\boldsymbol{k}^{(n)}=0 \tag{A}$$

となる。これを時刻 0 から 15 まで連立する。これを行列で表すと、以下のようになる。

$$\left(\begin{array}{c|c|c} & & \\ \boldsymbol{M_1} & \boldsymbol{M_2} & \boldsymbol{M_3} \\ & & \end{array}\right)\left(\begin{array}{c} b_0^{(0)} \\ b_1^{(0)} \\ \vdots \\ b_{15}^{(0)} \\ \hline a_0^{(0)} \\ a_0^{(1)} \\ \vdots \\ a_0^{(15)} \\ \hline k_0^{(0)} \\ k_1^{(0)} \\ k_0^{(1)} \\ k_1^{(1)} \\ \vdots \\ k_0^{(15)} \\ k_1^{(15)} \end{array}\right)=\boldsymbol{0} \tag{B}$$

各要素は式 (A) により以下のように定まる。

$$\boldsymbol{M_1}=\begin{pmatrix}\boldsymbol{C}\\ \boldsymbol{C}\cdot\boldsymbol{A}\\ \vdots\\ \boldsymbol{C}\cdot\boldsymbol{A^{15}}\end{pmatrix}$$

$$\boldsymbol{M_2}=\begin{pmatrix}\boldsymbol{C}\cdot\boldsymbol{H_0}\\ \boldsymbol{C}\cdot\boldsymbol{H_1}\\ \vdots\\ \boldsymbol{C}\cdot\boldsymbol{H_{15}}\end{pmatrix}$$

$$\boldsymbol{M_3}=\boldsymbol{I_{(32\times 32)}}$$

但し、$H=\sum_{j=0}^{n-1}\boldsymbol{A}^{n-j-1}\cdot\boldsymbol{B}$、$\boldsymbol{I_{(32\times32)}}$ は 32×32 の単位行列である。以降、$\boldsymbol{M}=\boldsymbol{M}_1|\boldsymbol{M}_2|\boldsymbol{M}_3$ とする。入出力変数の線形和が 0 となる関係を導出するため、行列 $\boldsymbol{M}$ に対し行の基本操作を行い式 (B) を、式 (C) ように変形する。

$$\left(\begin{array}{c|c} \boldsymbol{I}_{(16\times16)} & \boldsymbol{M''}_{(48\times16)} \\ \hline \boldsymbol{0}_{(16\times16)} & \boldsymbol{M'}_{(48\times16)} \end{array}\right)\left(\begin{array}{c} b_0^{(0)} \\ b_1^{(0)} \\ \vdots \\ b_{15}^{(0)} \\ \hline a_0^{(0)} \\ a_0^{(1)} \\ \vdots \\ a_0^{(15)} \\ \hline k_0^{(0)} \\ k_1^{(0)} \\ k_0^{(1)} \\ k_1^{(1)} \\ \vdots \\ k_0^{(15)} \\ k_1^{(15)} \end{array}\right)=\boldsymbol{0} \tag{C}$$

ただし、$\boldsymbol{I}$ は 16×16 の単位行列、$\boldsymbol{0}$ は 16×16 は 0 行列、$\boldsymbol{M''}$ は 48×16 の行列、$\boldsymbol{M'}$ は 48×16 の行列である。$\boldsymbol{M'}$ に着目し、式 (D) を導く。

$$\left(\begin{array}{c} \boldsymbol{M'}_{(48\times16)} \end{array}\right)\left(\begin{array}{c} a_0^{(0)} \\ a_0^{(1)} \\ \vdots \\ a_0^{(15)} \\ \hline k_0^{(0)} \\ k_1^{(0)} \\ k_0^{(1)} \\ k_1^{(1)} \\ \vdots \\ k_0^{(15)} \\ k_1^{(15)} \end{array}\right)=\boldsymbol{0} \tag{D}$$

式 (D) で与えられる線形式の線形結合はすべて消去関係式となる。このうち $k_0^{(0)}$,$k_1^{(0)}$ を含む, 最短のものは次の 2 式となる。

$$k_0^{(0)}+s\cdot k_1^{(1)}+k_1^{(5)}=0 \tag{E}$$

$$k_1^{(0)}+k_1^{(7)}+k_0^{(11)}+a_0^{(5)}=0 \tag{F}$$

式 (E),(F) は本文中の式 (8),(9) である。