詳細評価報告書
アバランシュ性検証評価

平成 13 年 1 月 10 日

1 概要

1.1 目的

本書は、電子政府における情報セキュリティ技術基盤技術として公募された共通鍵暗号アルゴリズムについて、アバランシュ性評価の実施結果を報告する。

アバランシュ性評価とは入力に特定の差分値を与えた場合の出力差分値について、出力ビット位置ごとに差分の出現頻度を調査する評価で、出力ビット位置ごとの詳細な挙動を知ることができる。本評価では暗号アルゴリズムをブラックボックス的に評価し、さらに数値化することで、構造の違いによらず統一的に比較できる。

1.2 対象

対象となる共通鍵暗号アルゴリズムを以下に示す。なお、評価プログラムの作成には応募資料に含まれるサンプルコードを使用した。

表 1.1 暗号アルゴリズム一覧

暗号名	ブロック長
CIPHERUNICORN-E	64 ビット
FEAL-NX	64 ビット
Hierocrypt-L1	64 ビット
MISTY1	64 ビット
Camellia	128 ビット
CIPHERUNICORN-A	128 ビット
Hierocrypt-3	128 ビット
MARS	128 ビット
RC6	128 ビット
SC2000	128 ビット

1.3 定義

本書で使用する用語を定義する。このほかの用語については各暗号の仕様に従うものとする。

∧	: 論理積
∨	: 論理和
⊕	: 排他的論理和
‖	: ビット列の連結
x<<y	: x を y ビット左論理シフト
X[i]	: X の第 i ビット
#{P}	: 条件 P が成立した回数
Hw(x)	: x のハミングウェイト
Pa(x)	: x のパリティ
$V^{(m)}$	: $a_0,a_1,...,a_{m-1}$ を GF(2^n)上で 1 次独立な m 個のベクトルとする。これらによって張られる、GF(2^m)上の部分空間

1.4 ビット／バイト／ワードの順序

本仕様書では、big endian 表記を用いる。

Q を 128 ビットデータ(quad word)、
D を 64 ビットデータ(double word)、
W を 32 ビットデータ(word)、
B を 8 ビットデータ(byte)、
E を 1 ビットデータ(bit)

とすると、

$$Q = D_0 \| D_1$$
$$= W_0 \| W_1 \| W_2 \| W_3$$
$$= B_0 \| B_1 \| B_2 \| \cdots\cdots \| B_{15}$$
$$= E_0 \| E_1 \| E_2 \| \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \| E_{127}$$

2 アバランシュ性評価

2.1 評価項目

入力データに差分を与えたときの出力データの差分値について評価値 AVA、平均拡散ビット数AVD、相関係数CC および有効鍵量 UKV を採取する。各値の詳細を以下に示す。

(1) AVA(Avalanche)

入力 X と鍵 K を入力とする評価対象関数 f(X, K)=Y において、ハミングウェイト m の入力差分値ΔX(ΔX ∈ $V^{(m)}$)を与えた場合の、
出力差分値ΔY = f(X, K) ⊕ f(X⊕ΔX, K)の第 j ビットの反転状態を
AVA[m, ΔX, j]とすると、

AVA[m, ΔX, j] = #{ΔY[j]=1} – #{ΔY[j]=0}

同様に、ハミングウェイト m の鍵差分値ΔK(ΔK ∈ $V^{(m)}$)を与えた場合の、出力差分値ΔY = f(X, K) ⊕ f(X, K⊕ΔK)の第 j ビットの反転状態を AVA[m, ΔK, j]とすると、

AVA[m, ΔK, j] = #{ΔY[j]=1} – #{ΔY[j]=0}

今回は、入力差分値ΔX、鍵差分値ΔK ともに m=1,2 について実施した。

(2) AVD(the average number of diffusion bits)

ハミングウェイト m の入力差分値(あるいは鍵差分値)を与えた場合の出力差分値ハミングウェイトの平均値

データ件数を N、t 件目の出力差分値を$\Delta Y_{(t)}$としたときの平均値を AVD[m]とすると、

$$AVD[m] = \left\{ \sum_{t=1}^{N} Hw(\Delta Y_{(t)}) \right\} / \quad N$$

(3) CC(Correlation Coefficient)

ハミングウェイト m の入力差分値ΔX を n 件与えた場合の出力差分値から選んだ任意の 2 ビット(A=ΔY[i], B=ΔY[j])の相関係数を CC[m, ΔX, i, j]とすると、

$$CC[m,\ \Delta X,\ i,\ j] = \frac{n \times \#\{A \wedge B=1\} - \#\{A=1\} \times \#\{B=1\}}{\sqrt{(n \times \#\{A^2=1\} - \#\{A=1\}^2) \times (n \times \#\{B^2=1\} - \#\{B=1\}^2)}}$$

同様に、ハミングウェイト m の鍵差分値ΔK を n 件与えた場合の出力差分値から選んだ任意の 2 ビット(A=ΔY[i], B=ΔY[j])の相関係数を CC[m, ΔK, i, j]とすると、

$$CC[m,\ \Delta K,\ i,\ j] = \frac{n \times \#\{A \wedge B=1\} - \#\{A=1\} \times \#\{B=1\}}{\sqrt{(n \times \#\{A^2=1\} - \#\{A=1\}^2) \times (n \times \#\{B^2=1\} - \#\{B=1\}^2)}}$$

今回は、入力差分値ΔX、鍵差分値ΔK ともに m=1 の場合のみ実施した。

(4) 有効鍵量 UKV(Useful Key Volume)

ハミングウェイト 1 の鍵差分値を与えた場合の評価から得られる AVA のうち相対基準値(2.5.1(2)節参照)を満たしている評価値の割合を求める。

鍵長 a ビット、出力データ b ビットとする。

step1)全てのΔK、j について AVA[1, ΔK, j]を求める。

step2)そのうち、相対基準値を満たしている要素数 D を求める。

step3)UKV = a × (D / (a × b))

2.2 擬似乱数生成法

32 ビットプロセッサでも乱数性を満たす手法(prng())を用いた乱数列生成関数 rand()を使用している。

(1) 乱数列生成関数 rand()

step1) seed = R1 = prng(seed)

step2) seed = R2 = prng(seed)

step3) R = R1 ⊕ (R2 << 2)

step4) return(R)

(2) 擬似乱数生成関数 prng(x)

prng(x) = ax mod m

$a = 7^5 = 16807$

$m = 2^{31} - 1 = 2147483647$

2.3 データの与え方

(1) 入力と出力の相関を調査する場合

最初に鍵乱数列シード $seed_K$、および入力乱数列シード $seed_D$ でそれぞれの乱数列を初期化する。

step1)鍵乱数 R_K を 1 つ生成する

step2)$seed_D$ で入力乱数列を初期化する

step3)入力乱数 R_D を 1 つ生成する

step4)評価対象関数 $f(R_D , R_K)$を計算し、評価値を採取する

step5)step3～step4 を必要な入力データ件数繰り返す

step6)step1～step5 を必要な鍵データ件数繰り返す

(2) 鍵と出力の相関を調査する場合

最初に鍵乱数列シード $seed_K$、および入力乱数列シード $seed_D$ でそれぞれの乱数列を初期化する。

step1)入力乱数 R_D を 1 つ生成する

step2)$seed_K$ で鍵乱数列を初期化する

step3)鍵乱数 R_K を 1 つ生成する

step4)評価対象関数 $f(R_D , R_K)$を計算し、評価値を採取する

step5)step3～step4 を必要な鍵データ件数繰り返す

step6)step1～step5 を必要な入力データ件数繰り返す

2.4 データ件数

本来、入力として与えるデータを総当りするのが理想であるが、入力のデータ幅によっては総当りが困難な場合がある。今回の評価では評価期間および計算機資源を考慮して可能な最大限のデータ件数に決定した。

2.5 期待値

2.5.1 AVA

(1) 最悪偏差率(WDR)

以下の式で得られる偏差率を最悪偏差率と呼ぶことにする。最悪偏差率が 1 に近づくほど相関関係が大きいことを表しており、なるべく小さな値であることが望ましい。

$ST_{max}[AVA]$: 評価値 AVA の絶対値のうち最大値

最悪偏差率 $WDR[AVA] = (ST_{max}[AVA] / (入力件数 \times 鍵件数))^2$

(2) 相対基準値(RSV)

統計的な偏りの有無を判断するための基準値を実験的に求めた。我々は、この値を相対基準値(RSV)と呼ぶことにし、評価対象関数における最悪偏差率が相対基準値より小さい場合には統計的な偏りが無いものとみなすことにした。

実際には、アルゴリズムが公開されている既存の共通鍵暗号を用いて初等統計データを採取し、その最悪偏差率を相対基準値とした。相対基準値にはデータ件数(入力件数×鍵件数)N と以下のような相関がある。

相対基準値 $RSV = 2^a / N$

なお、a の値は、データの総当りをしない場合、データ件数や乱数列のシードによってばらつきが若干あるが、おおよそ以下の値になる。

入力差分値(あるいは鍵差分値)のハミングウェイトが 1 のとき、

$a = 4 \pm 1$

入力差分値(あついは鍵差分値)のハミングウェイトが 2 のとき、

$a = 4.5 \pm 1$

となる。

2.5.2 AVD

評価対象関数の出力データ長を n とすると、おおよそ n/2 であることが望ましい。

2.5.3 CC

CC の範囲は-1≦CC≦1 であり、0 に近づくほど独立性が高い。

アルゴリズムが公開されている既存の共通鍵暗号を用いて CC を採取したところ、データ件数(入力件数×鍵件数)2^n と以下のような相関がある。

$2^{2.5} / 2^{0.5n}$

2.5.4 UKV

なるべくどの出力ビットにも全ての鍵ビットが影響することが望ましい。従って、UKV は鍵データ長に近いのが望ましい。

3 評価結果

3.1 評価結果概要

各暗号アルゴリズムの評価結果の概要を以下に示す。詳細な考察については4章に記載した。

3.1.1 64ビットブロック暗号

(1) CIPHERUNICORN-E

ラウンド関数では特徴は見られなかった。
データ攪拌部では 4 段以降の攪拌に特徴は見られなかった。
鍵スケジューラでは特徴は見られなかった。

(2) FEAL-NX

ラウンド関数では期待値から離れている部分があった。
データ攪拌部では 5 段以降の攪拌に特徴は見られなかった。
鍵スケジューラでは秘密鍵と拡大鍵間に大きな関係が存在した。

(3) Hierocrypt-L1

ラウンド関数では期待値から離れている部分があった。
データ攪拌部では 2 段以降の攪拌に特徴は見られなかった。
鍵スケジューラでは秘密鍵と拡大鍵間に大きな関係が存在した。

(4) MISTY1

ラウンド関数では期待値から離れている部分があった。
データ攪拌部では 4 段以降の攪拌に特徴は見られなかった。
鍵スケジューラでは秘密鍵と拡大鍵間に大きな関係が存在した。

3.1.2 128ビットブロック暗号

(1) Camellia

ラウンド関数では期待値から離れている部分があった。
データ攪拌部では 4 段以降の攪拌に特徴は見られなかった。
鍵スケジューラでは秘密鍵長によって異なる特徴が見られた。

(2) CIPHERUNICORN-A

ラウンド関数では特徴は見られなかった。
データ攪拌部では 3 段以降の攪拌に特徴は見られなかった。
鍵スケジューラでは特徴は見られなかった。

(3) Hierocrypt-3

ラウンド関数では期待値から離れている部分があった。
データ攪拌部では 2 段以降の攪拌に特徴は見られなかった。
鍵スケジューラでは秘密鍵と拡大鍵に大きな関係が存在した。

(4) MARS

ラウンド関数では期待値から離れている部分があった。

データ攪拌部では特徴は見られなかった。

鍵スケジューラでは乗算処理で使用する拡大鍵に特徴が見られた。

(5) RC6

ラウンド関数では期待値から離れている部分があった。

データ攪拌部では 6 段以降の攪拌に特徴は見られなかった。

鍵スケジューラでは特徴は見られなかった。

(6) SC2000

ラウンド関数では期待値から離れている部分があった。

データ攪拌部では 4 段以降の攪拌に特徴は見られなかった。

鍵スケジューラでは秘密鍵長が 192 ビットおよび 256 ビットのときに特徴が見られた。

3.2 評価結果詳細

次ページ以降に評価結果を示す。表中の略記は表 3.1を参照のこと。評価の対象となった入出力のパラメータを付録 C に記載した。

表 3.1 略記表現

暗号名	略記
CIPHERUNICORN-E	UNIE
FEAL-NX	FEAL
Hierocrypt-L1	HiL1
MISTY1	MIST
Camellia	Came
CIPHERUNICORN-A	UNIA
Hierocrypt-3	Hi3
MARS	MARS
RC6	RC6
SC2000	SC

3.3 AVA

表 3.2ラウンド関数

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)	相対 基準値	最悪偏差率									
				UNIE	FEAL	HiL1	MIST	Came	UNIA	Hi3	MARS	RC6	SC
入力と出力の相関	1	$2^{32}(2^{28}\times2^{4})$	$2^{-28.00}$	$2^{-28.51}$	$2^{0.00}$	$2^{-20.21(*2)}$	$2^{0.00}$	$2^{0.00}$	$2^{-28.34}$	$2^{-19.29(*2)}$	$2^{0.00}$	$2^{-0.19}$	$2^{0.00}$
	2	$2^{24}(2^{20}\times2^{4})$	$2^{-19.50}$	$2^{-19.87}$	$2^{0.00}$	$2^{-17.57(*2)}$	$2^{0.00}$	$2^{0.00}$	$2^{-19.64}$	$2^{-17.27(*2)}$	$2^{0.00}$	$2^{-0.28}$	$2^{0.00}$
拡大鍵と出力の相関	1	$2^{22}(2^{4}\times2^{18})$	$2^{-18.00}$	$2^{-18.47}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-18.23}$	$2^{0.00(*2)}$	$2^{0.00}$	$2^{0.00}$	—(*3)
	2	$2^{22}(2^{4}\times2^{18})$	$2^{-17.50}$	$2^{-17.57}$	$2^{0.00}$	$2^{0.00(*2)}$	$2^{0.00}$	$2^{0.00}$	$2^{-17.46}$	$2^{0.00(*2)}$	$2^{0.00}$	$2^{0.00}$	—(*3)
拡大鍵=0固定での入出力相関	1(*1)	$2^{32}(2^{32}\times2^{0})$	$2^{-28.00}$	$2^{-27.54}$	$2^{0.00}$	$2^{-17.87(*2)}$	$2^{0.00}$	$2^{0.00}$	$2^{-28.05}$	$2^{0.00(*2)}$	$2^{0.00}$	$2^{-0.19}$	—(*3)
	2	$2^{24}(2^{24}\times2^{0})$	$2^{-19.50}$	$2^{-20.14}$	$2^{0.00}$	$2^{-17.42(*2)}$	$2^{0.00}$	$2^{0.00}$	$2^{-19.45}$	$2^{-17.34(*2)}$	$2^{0.00}$	$2^{-0.28}$	—(*3)

(*1)UNIE, FEAL, MIST,MARS については入力データを総当たりした。その他については０からのシーケンシャルデータを与えた。

(*2) データ件数は他より 2 乗少ない。

(*3)鍵を含まないラウンド関数を対象としているため評価していない。

表 3.3データ攪拌部(秘密鍵長 128 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)	相対 基準値	最悪偏差率									
				UNIE	FEAL	HiL1	MIST	Came	UNIA	Hi3	MARS	RC6	SC
平文と暗号文の相関	1	$2^{20}(2^{16}\times 2^{4})$	$2^{-16.00}$	$2^{-15.99}$	$2^{-15.95}$	$2^{-16.23}$	$2^{-16.38}$	$2^{-15.73}$	$2^{-15.93}$	$2^{-16.05}$	$2^{-15.90}$	$2^{-15.87}$	$2^{-16.08}$
秘密鍵と暗号文の相関	1	$2^{20}(2^{4}\times 2^{16})$	$2^{-16.00}$	$2^{-16.11}$	$2^{-16.18}$	$2^{-16.15}$	$2^{-16.07}$	$2^{-15.58}$	$2^{-15.81}$	$2^{-15.68}$	$2^{-16.04}$	$2^{-15.58}$	$2^{-16.04}$
段数経過	1(*1)												
	R2	$2^{20}(2^{16}\times 2^{4})$	$2^{-16.00}$	$2^{-0.38}$	$2^{-0.26}$	$2^{-16.42}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-16.24}$	$2^{-15.71}$	$2^{0.00}$	$2^{-1.35}$
	R3			$2^{-2.37}$	$2^{-7.31}$	$2^{-16.02}$	$2^{-1.36}$	$2^{0.00}$	$2^{-16.18}$	$2^{-15.88}$	$2^{-15.92}$	$2^{0.00}$	$2^{-5.70}$
	R4			$2^{-16.40}$	$2^{-15.71}$	$2^{-16.54}$	$2^{-16.32}$	$2^{-16.10}$	$2^{-16.19}$	$2^{-16.05}$	$2^{-15.92}$	$2^{-2.26}$	$2^{-15.93}$
	R5			$2^{-16.10}$	$2^{-16.46}$	$2^{-16.01}$	$2^{-16.55}$	$2^{-16.00}$	$2^{-16.24}$	$2^{-16.07}$	$2^{-16.17}$	$2^{-12.54}$	$2^{-15.93}$
	R6			—	—	—	—	—	—	—	—	$2^{-15.62}$	—
	R7			—	—	—	—	—	—	—	—	$2^{-16.08}$	—

(*1)Rx は、平文とラウンド数 x の出力に関しての調査結果を表す。なお、R5 まではすべての暗号について実施し、R5 でも期待値から離れている暗号については期待値に近づくまで追加評価を実施した。

表 3.4データ攪拌部(秘密鍵長 192 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)	相対 基準値	最悪偏差率					
				Came	UNIA	Hi3	MARS	RC6	SC
平文と暗号文の相関	1	$2^{20}(2^{16}\times 2^{4})$	$2^{-16.00}$	$2^{-15.97}$	$2^{-15.81}$	$2^{-15.80}$	$2^{-16.14}$	$2^{-16.03}$	$2^{-15.81}$
秘密鍵と暗号文の相関	1	$2^{20}(2^{4}\times 2^{16})$	$2^{-16.00}$	$2^{-15.72}$	$2^{-15.57}$	$2^{-15.80}$	$2^{-16.15}$	$2^{-16.11}$	$2^{-15.91}$
段数経過	1(*1)								
	R2	$2^{20}(2^{16}\times 2^{4})$	$2^{-16.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.78}$	$2^{-16.20}$	$2^{0.00}$	$2^{-1.35}$
	R3			$2^{0.00}$	$2^{-15.70}$	$2^{-16.02}$	$2^{-16.25}$	$2^{0.00}$	$2^{-5.70}$
	R4			$2^{-15.57}$	$2^{-15.81}$	$2^{-15.71}$	$2^{-16.02}$	$2^{-2.27}$	$2^{-15.86}$
	R5			$2^{-15.87}$	$2^{-16.02}$	$2^{-15.82}$	$2^{-15.85}$	$2^{-12.72}$	$2^{-15.74}$
	R6			—	—	—	—	$2^{-15.96}$	—
	R7			—	—	—	—	$2^{-16.29}$	—

(*1)Rx は、平文とラウンド数 x の出力に関しての調査結果を表す。なお、R5 まではすべての暗号について実施し、R5 でも期待値から離れている暗号については期待値に近づくまで追加評価を実施した。

表 3.5データ攪拌部(秘密鍵長 256 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)	相対 基準値	最悪偏差率					
				Came	UNIA	Hi3	MARS	RC6	SC
平文と暗号文の相関	1	$2^{20}(2^{16}\times 2^{4})$	$2^{-16.00}$	$2^{-16.05}$	$2^{-16.09}$	$2^{-16.18}$	$2^{-16.04}$	$2^{-16.06}$	$2^{-16.02}$
秘密鍵と暗号文の相関	1	$2^{20}(2^{4}\times 2^{16})$	$2^{-16.00}$	$2^{-15.65}$	$2^{-15.69}$	$2^{-15.60}$	$2^{-15.82}$	$2^{-15.77}$	$2^{-15.67}$
段数経過	1(*1)								
	R2	$2^{20}(2^{16}\times 2^{4})$	$2^{-16.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.61}$	$2^{-16.01}$	$2^{0.00}$	$2^{-1.35}$
	R3			$2^{0.00}$	$2^{-15.72}$	$2^{-15.89}$	$2^{-15.81}$	$2^{0.00}$	$2^{-5.74}$
	R4			$2^{-15.63}$	$2^{-15.77}$	$2^{-15.65}$	$2^{-16.19}$	$2^{-2.26}$	$2^{-15.58}$
	R5			$2^{-15.91}$	$2^{-15.82}$	$2^{-15.91}$	$2^{-16.19}$	$2^{-12.70}$	$2^{-16.07}$
	R6			—	—	—	—	$2^{-16.13}$	—
	R7			—	—	—	—	$2^{-16.00}$	—

(*1)Rx は、平文とラウンド数 x の出力に関しての調査結果を表す。なお、R5 まではすべての暗号について実施し、R5 でも期待値から離れている暗号については期待値に近づくまで追加評価を実施した。

表 3.6鍵スケジューラ(秘密鍵長 128 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)	相対 基準値	最悪偏差率									
				UNIE	FEAL	HiL1	MIST	Came	UNIA	Hi3	MARS	RC6	SC
秘密鍵と拡大鍵の相関	1	2^{20}	$2^{-16.00}$	$2^{-15.36}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.40}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.44}$	$2^{-15.30}$
	2(*1)												
	W0	2^{20}	$2^{-15.50}$	$2^{-15.25}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.34}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.60}$	$2^{-15.25}$
	W1			$2^{-15.17}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.27}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.56}$	$2^{-15.23}$
	W2			$2^{-15.16}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.41}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.10}$	$2^{-15.61}$
	W3			$2^{-15.47}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.57}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.38}$	$2^{-15.04}$

(*1)Wx は、秘密鍵 Word#x の 32 ビット内でハミングウェイト 2 の差分値を与えた評価結果を表す。

表 3.7鍵スケジューラ(秘密鍵長 192 ビット)

大分類	Hw	ﾃﾞｰﾀ件数	相対基準値	最悪偏差率					
				Came	UNIA	Hi3	MARS	RC6	SC
秘密鍵と拡大鍵の相関	1	2^{20}	$2^{-16.00}$	$2^{0.00}$	$2^{-15.20}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.17}$	$2^{-15.30}$
	2(*1)								
	W0	2^{20}	$2^{-15.50}$	$2^{0.00}$	$2^{-15.40}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.43}$	$2^{-15.40}$
	W1			$2^{0.00}$	$2^{-15.29}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.37}$	$2^{-15.23}$
	W2			$2^{0.00}$	$2^{-15.44}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.54}$	$2^{-15.52}$
	W3			$2^{0.00}$	$2^{-15.43}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.49}$	$2^{-15.48}$
	W4			$2^{0.00}$	$2^{-15.43}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.43}$	$2^{-15.36}$
	W5			$2^{0.00}$	$2^{-15.46}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.61}$	$2^{-15.26}$

(*1)Wx は、秘密鍵 Word#x の 32 ビット内でハミングウェイト 2 の差分値を与えた評価結果を表す。

表 3.8鍵スケジューラ(秘密鍵長 256 ビット)

大分類	Hw	ﾃﾞｰﾀ件数	相対基準値	最悪偏差率					
				Came	UNIA	Hi3	MARS	RC6	SC
秘密鍵と拡大鍵の相関	1	2^{20}	$2^{-16.00}$	$2^{0.00}$	$2^{-15.48}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.65}$	$2^{-15.38}$
	2(*1)								
	W0	2^{20}	$2^{-15.50}$	$2^{0.00}$	$2^{-15.52}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.46}$	$2^{-15.23}$
	W1			$2^{0.00}$	$2^{-15.03}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.01}$	$2^{-15.56}$
	W2			$2^{0.00}$	$2^{-15.19}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.46}$	$2^{-15.52}$
	W3			$2^{0.00}$	$2^{-15.50}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.51}$	$2^{-15.48}$
	W4			$2^{0.00}$	$2^{-15.35}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.44}$	$2^{-15.36}$
	W5			$2^{0.00}$	$2^{-14.74}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.45}$	$2^{-15.26}$
	W6			$2^{0.00}$	$2^{-15.12}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.49}$	$2^{-15.44}$
	W7			$2^{0.00}$	$2^{-15.54}$	$2^{0.00}$	$2^{0.00}$	$2^{-15.38}$	$2^{-15.25}$

(*1)Wx は、秘密鍵 Word#x の 32 ビット内でハミングウェイト 2 の差分値を与えた評価結果を表す。

3.4 AVD

表 3.9ラウンド関数

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)		AVD									
				UNIE	FEAL	HiL1	MIST	Came	UNIA	Hi3	MARS	RC6	SC
			期待値	16.00	16.00	32.00	16.00	32.00	32.00	64.00	48.00	32.00	32.00
入力と出力の相関	1	$2^{32}(2^{28}\times 2^{4})$	測定値	16.00	9.90	32.00(*2)	16.14	21.92	32.00	64.00(*2)	38.87	25.06	24.71
	2	$2^{24}(2^{20}\times 2^{4})$		16.00	13.16	32.00(*2)	15.99	28.83	32.00	64.00(*2)	42.93	29.63	28.33
拡大鍵と出力の相関	1	$2^{22}(2^{4}\times 2^{18})$	測定値	16.00	9.41	27.28	9.24	21.92	32.00	54.06(*2)	19.98	1.94	—(*3)
	2	$2^{22}(2^{4}\times 2^{18})$		16.00	13.14	31.24(*2)	12.80	28.83	32.00	62.39(*2)	30.38	3.80	—(*3)
拡大鍵=0固定での入出力相関	1(*1)	$2^{32}(2^{32}\times 2^{0})$	測定値	16.00	9.90	32.00(*2)	16.13	21.92	32.00	63.72(*2)	12.48	24.42	—(*3)
	2	$2^{24}(2^{24}\times 2^{0})$		16.00	13.16	32.00(*2)	15.99	28.83	32.00	64.00(*2)	20.35	29.32	—(*3)

(*1)UNIE, FEAL, MIST, MARS については入力データを総当たりした。その他については0からのシーケンシャルデータを与えた。
(*2)データ件数は他より 2 乗少ない。
(*3)鍵を含まないラウンド関数を対象としているため評価していない。

表 3.10 データ攪拌部(秘密鍵長 128 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)		AVD									
				UNIE	FEAL	HiL1	MIST	Came	UNIA	Hi3	MARS	RC6	SC
			期待値	32.00	32.00	32.00	32.00	64.00	64.00	64.00	64.00	64.00	64.00
平文と暗号文の相関	1	$2^{20}(2^{16}\times 2^{4})$	測定値	32.00	32.00	32.00	32.00	64.00	64.00	64.00	64.00	64.00	64.00
秘密鍵と暗号文の相関	1	$2^{20}(2^{4}\times 2^{16})$	測定値	32.00	32.00	32.00	32.00	64.00	64.00	64.00	64.00	64.00	64.00
段数経過	1(*1)	$2^{20}(2^{16}\times 2^{4})$	測定値										
	R2			26.21	31.77	32.00	24.66	38.43	49.18	64.00	64.00	14.37	55.99
	R3			30.47	31.99	32.00	32.03	58.96	64.00	64.00	64.00	41.77	62.98
	R4			32.00	32.00	32.00	32.00	64.00	64.00	64.00	64.00	60.29	64.00
	R5			32.00	32.00	32.00	32.00	64.00	64.00	64.00	64.00	63.92	64.00
	R6			—	—	—	—	—	—	—	—	64.00	—

(*1)Rx は、平文とラウンド数 x の出力に関しての調査結果を表す。なお、R5 まではすべての暗号について実施し、R5 でも期待値から離れている暗号については期待値に近づくまで追加評価を実施した。

表 3.11データ攪拌部(秘密鍵長 192 ビット)

大分類	Hw	データ件数 (データ×鍵)		AVD					
				Came	UNIA	Hi3	MARS	RC6	SC
			期待値	64.00	64.00	64.00	64.00	64.00	64.00
平文と暗号文の相関	1	$2^{20}(2^{16}\times 2^{4})$	測定値	64.00	64.00	64.0	64.00	64.00	64.00
秘密鍵と暗号文の相関	1	$2^{20}(2^{4}\times 2^{16})$	測定値	64.00	64.00	64.00	64.00	64.00	64.00
段数経過	1 (*1)	$2^{20}(2^{16}\times 2^{4})$	測定値						
	R2			38.42	49.19	64.00	64.00	14.40	55.99
	R3			58.96	64.00	64.00	64.00	41.78	62.98
	R4			64.00	64.00	64.00	64.00	60.28	64.00
	R5			64.00	64.00	64.00	64.00	63.92	64.00
	R6			―	―	―	―	64.00	―

(*1)Rx は、平文とラウンド数 x の出力に関しての調査結果を表す。なお、R5 まではすべての暗号について実施し、R5 でも期待値から離れている暗号については期待値に近づくまで追加評価を実施した。

表 3.12 データ攪拌部(秘密鍵長 256 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)		AVD					
				Came	UNIA	Hi3	MARS	RC6	SC
			期待値	64.00	64.00	64.00	64.00	64.00	64.00
平文と暗号文の相関	1	$2^{20}(2^{16}\times 2^{4})$	測定値	64.00	64.00	64.00	64.00	64.00	64.00
秘密鍵と暗号文の相関	1	$2^{20}(2^{4}\times 2^{16})$	測定値	64.00	64.00	64.00	64.00	64.00	64.00
段数経過	1 (*1)	$2^{20}(2^{16}\times 2^{4})$	測定値						
	R2			38.43	49.19	64.00	64.00	14.38	55.99
	R3			58.96	64.00	64.00	64.00	41.79	62.98
	R4			64.00	64.00	64.00	64.00	60.28	64.00
	R5			64.00	64.00	64.00	64.00	63.92	64.00
	R6			―	―	―	―	64.00	―

(*1)Rx は、平文とラウンド数 x の出力に関しての調査結果を表す。なお、R5 まではすべての暗号について実施し、R5 でも期待値から離れている暗号については期待値に近づくまで追加評価を実施した。

表 3.13 鍵スケジューラ(秘密鍵長 128 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)		AVD									
				UNIE	FEAL	HiL1	MIST	Came	UNIA	Hi3	MARS	RC6	SC
			期待値	1312.00	320.00	448.00	128.00	64.00	1152.00	896.00	640.00	704.00	896.00
秘密鍵と拡大鍵の相関	1	2^{20}	測定値	1312.00	303.86	412.04	12.92	65.00	1152.00	653.13	624.00	704.00	896.00
	2(*1)	2^{20}											
	W0			1312.00	316.35	405.84	18.72	66.00	1152.00	881.05	624.00	704.00	896.00
	W1			1312.00	307.72	443.29	18.72	66.00	1152.00	889.37	624.00	704.00	896.00
	W2			1312.00	302.94	447.00	18.72	66.00	1152.00	658.95	624.00	704.00	896.00
	W3			1312.00	301.44	408.02	18.72	66.00	1152.00	669.25	624.00	704.00	896.00

(*1)Wx は、秘密鍵 Word#x の 32 ビット内でハミングウェイト 2 の差分値を与えた評価結果を表す。

表 3.14 鍵スケジューラ(秘密鍵長 192 ビット)

大分類	Hw	ﾃﾞｰﾀ件数		AVD					
				Came	UNIA	Hi3	MARS	RC6	SC
			期待値	128.00	1152.00	1024.00	640.00	704.00	1024.00
秘密鍵と拡大鍵の相関	1	2^{20}	測定値	129.33	1152.00	612.93	624.00	704.00	1024.00
	2(*1)	2^{20}							
	W0			130.00	1152.00	605.27	624.00	704.00	1024.00
	W1			130.00	1152.00	645.43	624.00	704.00	1024.00
	W2			130.00	1152.00	724.09	624.00	704.00	1024.00
	W3			130.00	1152.00	738.93	624.00	704.00	1024.00
	W4			132.00	1152.00	970.20	624.00	704.00	1024.00
	W5			132.00	1152.00	989.12	624.00	704.00	1024.00

(*1)Wx は、秘密鍵 Word#x の 32 ビット内でハミングウェイト 2 の差分値を与えた評価結果を表す。

表 3.15 鍵スケジューラ(秘密鍵長 256 ビット)

大分類	Hw	ﾃﾞｰﾀ件数		AVD					
				Came	UNIA	Hi3	MARS	RC6	SC
			期待値	128.00	1152.00	1152.00	640.00	704.00	1024.00
秘密鍵と拡	1	2^{20}	測定値	129.00	1152.00	794.60	624.00	704.00	1024.00
大鍵の相関	2(*1)	2^{20}							
	W0			130.00	1152.00	769.36	624.00	704.00	1024.00
	W1			130.00	1152.00	798.76	624.00	704.00	1024.00
	W2			130.00	1152.00	853.32	624.00	704.00	1024.00
	W3			130.00	1152.00	863.35	624.00	704.00	1024.00
	W4			130.00	1152.00	1135.48	624.00	704.00	1024.00
	W5			130.00	1152.00	1147.16	624.00	704.00	1024.00
	W6			130.00	1152.00	1010.21	624.00	704.00	1024.00
	W7			130.00	1152.00	1072.22	624.00	704.00	1024.00

(*1)Wx は、秘密鍵 Word#x の 32 ビット内でハミングウェイト 2 の差分値を与えた評価結果を表す。

3.5 CC

表 3.16 ラウンド関数

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)	期待値	CC									
				UNIE	FEAL	HiL1	MIST	Came	UNIA	Hi3(*2)	MARS	RC6	SC
入力と出力の相関	1	$2^{24}(2^{20}\times 2^{4})$	$2^{-9.5}$	$2^{-9.95}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-9.74}$	$2^{0.00}$	$2^{0.00}$	$2^{-0.94}$	$2^{0.00}$
拡大鍵=0 固定での入出力相関	1(*1)	$2^{24}(2^{24}\times 2^{0})$	$2^{-9.5}$	$2^{-9.96}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-9.85}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	—(*3)

(*1)UNIE, FEAL, MIST, MARS については入力データを総当たりした。

(*2)Hi3 のデータ件数は他より 2 乗少ない。

(*3)鍵を含まないラウンド関数を対象としているため評価していない。

表 3.17 データ攪拌部(秘密鍵長 128 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)	期待値	CC									
				UNIE	FEAL	HiL1	MIST	Came	UNIA	Hi3	MARS	RC6	SC
平文と暗号文の相関	1	$2^{20}(2^{16}\times 2^{4})$	$2^{-7.5}$	$2^{-7.92}$	$2^{-7.64}$	$2^{-7.76}$	$2^{-7.67}$	$2^{-7.74}$	$2^{-7.46}$	$2^{-7.57}$	$2^{-7.54}$	$2^{-7.70}$	$2^{-7.72}$
秘密鍵と暗号文の相関	1	$2^{20}(2^{4}\times 2^{16})$	$2^{-7.5}$	$2^{-7.72}$	$2^{-7.93}$	$2^{-7.84}$	$2^{-7.88}$	$2^{-7.75}$	$2^{-7.67}$	$2^{-7.78}$	$2^{-7.71}$	$2^{-7.54}$	$2^{-7.64}$
段数経過	1(*1)	$2^{20}(2^{16}\times 2^{4})$	$2^{-7.5}$										
	R2			$2^{-1.08}$	$2^{0.00}$	$2^{-7.86}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-7.57}$	$2^{-7.68}$	$2^{0.00}$	$2^{0.00}$
	R3			$2^{-2.18}$	$2^{-0.13}$	$2^{-7.71}$	$2^{0.65}$	$2^{0.00}$	$2^{-7.64}$	$2^{-7.58}$	$2^{-7.67}$	$2^{0.00}$	$2^{-2.68}$
	R4			$2^{-7.81}$	$2^{-3.66}$	$2^{-7.95}$	$2^{-7.79}$	$2^{-5.81}$	$2^{-7.72}$	$2^{-7.75}$	$2^{-7.66}$	$2^{-1.72}$	$2^{-7.69}$
	R5			$2^{-7.77}$	$2^{-7.85}$	$2^{-7.86}$	$2^{-7.80}$	$2^{-7.66}$	$2^{-7.68}$	$2^{-7.68}$	$2^{-7.77}$	$2^{-6.35}$	$2^{-7.77}$
	R6			—	—	—	—	—	—	—	—	$2^{-7.65}$	—

(*1)Rx は、平文とラウンド数 x の出力に関しての調査結果を表す。なお、R5 まではすべての暗号について実施し、R5 でも期待値から離れている暗号については期待値に近づくまで追加評価を実施した。

表 3.18データ攪拌部(秘密鍵長 192 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)	期待値	CC					
				Came	UNIA	Hi3	MARS	RC6	SC
平文と暗号文の相関	1	$2^{20}(2^{16}\times 2^{4})$	$2^{-7.5}$	$2^{-7.73}$	$2^{-7.70}$	$2^{-7.72}$	$2^{-7.73}$	$2^{-7.66}$	$2^{-7.74}$
秘密鍵と暗号文の相関	1	$2^{20}(2^{4}\times 2^{16})$	$2^{-7.5}$	$2^{-7.74}$	$2^{-7.66}$	$2^{-7.60}$	$2^{-7.60}$	$2^{-7.73}$	$2^{-7.61}$
段数経過	1	$2^{20}(2^{16}\times 2^{4})$	$2^{-7.5}$						
	R2			$2^{0.00}$	$2^{0.00}$	$2^{-7.65}$	$2^{-7.77}$	$2^{0.00}$	$2^{0.00}$
	R3			$2^{0.00}$	$2^{-7.63}$	$2^{-7.72}$	$2^{-7.60}$	$2^{0.00}$	$2^{-2.69}$
	R4			$2^{-5.85}$	$2^{-7.63}$	$2^{-7.75}$	$2^{-7.68}$	$2^{-1.71}$	$2^{-7.71}$
	R5			$2^{-7.69}$	$2^{-7.77}$	$2^{-7.49}$	$2^{-7.81}$	$2^{-6.35}$	$2^{-7.75}$
	R6			—	—	—	—	$2^{-7.79}$	—

(*1)Rx は、平文とラウンド数 x の出力に関しての調査結果を表す。なお、R5 まではすべての暗号について実施し、R5 でも期待値から離れている暗号については期待値に近づくまで追加評価を実施した。

表 3.19 データ攪拌部(秘密鍵長 256 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)	期待値	CC					
				Came	UNIA	Hi3	MARS	RC6	SC
平文と暗号文の相関	1	$2^{20}(2^{16}\times 2^{4})$	$2^{-7.5}$	$2^{-7.68}$	$2^{-7.70}$	$2^{-7.55}$	$2^{-7.67}$	$2^{-7.70}$	$2^{-7.72}$
秘密鍵と暗号文の相関	1	$2^{20}(2^{4}\times 2^{16})$	$2^{-7.5}$	$2^{-7.60}$	$2^{-7.50}$	$2^{-7.66}$	$2^{-7.75}$	$2^{-7.68}$	$2^{-7.57}$
段数経過	1	$2^{20}(2^{16}\times 2^{4})$	$2^{-7.5}$						
	R2			$2^{0.00}$	$2^{0.00}$	$2^{-7.77}$	$2^{-7.67}$	$2^{0.00}$	$2^{0.00}$
	R3			$2^{0.00}$	$2^{-7.66}$	$2^{-7.69}$	$2^{-7.66}$	$2^{0.00}$	$2^{-2.69}$
	R4			$2^{-5.75}$	$2^{-7.56}$	$2^{-7.71}$	$2^{-7.76}$	$2^{-1.70}$	$2^{-7.67}$
	R5			$2^{-7.66}$	$2^{-7.67}$	$2^{-7.69}$	$2^{-7.67}$	$2^{-6.34}$	$2^{-7.55}$
	R6			—	—	—	—	$2^{-7.68}$	—

(*1)Rx は、平文とラウンド数 x の出力に関しての調査結果を表す。なお、R5 まではすべての暗号について実施し、R5 でも期待値から離れている暗号については期待値に近づくまで追加評価を実施した。

表 3.20 鍵スケジューラ(秘密鍵長 128 ビット)

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)	期待値	CC									
				UNIE	FEAL	HiL1	MIST	Came	UNIA	Hi3	MARS	RC6	SC
秘密鍵と拡大鍵の相関	1	2^{20}	$2^{-7.5}$	$2^{-7.72}$	$2^{0.00}$	$2^{0.00}$	$2^{0.00}$	$2^{-7.86}$	$2^{-7.73}$	$2^{0.00}$	$2^{0.00}$	$2^{-7.81}$	$2^{-7.66}$

表 3.21 鍵スケジューラ(秘密鍵長 192 ビット)

大分類	Hw	ﾃﾞｰﾀ件数	期待値	CC					
				Came	UNIA	Hi3	MARS	RC6	SC
秘密鍵と拡大鍵の相関	1	2^{20}	$2^{-7.5}$	$2^{-7.80}$	$2^{-7.69}$	$2^{0.00}$	$2^{0.00}$	$2^{-7.61}$	$2^{0.00}$

表 3.22 鍵スケジューラ(秘密鍵長 256 ビット)

大分類	Hw	ﾃﾞｰﾀ件数	期待値	CC					
				Came	UNIA	Hi3	MARS	RC6	SC
秘密鍵と拡大鍵の相関	1	2^{20}	$2^{-7.5}$	$2^{-7.59}$	$2^{-7.75}$	$2^{0.00}$	$2^{0.00}$	$2^{-7.75}$	$2^{0.00}$

3.6 UKV

表 3.23 ラウンド関数

大分類	Hw	ﾃﾞｰﾀ件数 (ﾃﾞｰﾀ×鍵)		UKV									
				UNIE	FEAL	HiL1	MIST	Came	UNIA	Hi3	MARS	RC6	SC
拡大鍵と出力の相関	1	$2^{22}(2^4\times2^{18})$	期待値	128.00	16.00	128.00	112.00	64.00	128.00	256.00	64.00	64.00	—(*1)
			測定値	128.00	1.88	68.19	51.22	53.83	128.00	136.24	9.07	0.03	—(*1)

(*1)鍵を含まないラウンド関数を対象としているため評価していない。

4 考察

4.1 CIPHERUNICORN-E

結果グラフは付録 B.1 を参照のこと。

4.1.1 ラウンド関数

(1) AVA(表 3.2)

いずれの項目においても最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。

(2) AVD(表 3.9)

いずれの項目においても期待値に近い。グラフに特徴は見られない。

(3) CC(表 3.16)

いずれの項目においても期待値に近い。

(4) UKV(表 3.23)

期待値に近い。

4.1.2 データ攪拌部

(1) AVA(表 3.3)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。「段数経過(Hw=1)」では R2 および R3 のときに最悪偏差率が相対基準値より大きいが、R4 以降では相対基準値より小さい。

(2) AVD(表 3.10)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。グラフに特徴は見られない。「段数経過(Hw=1)」では R2 および R3 のときに期待値から遠いが、R4 以降では期待値に近い。

(3) CC(表 3.17)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2 および R3 のときに期待値から遠いが、R4 以降では期待値に近い。

4.1.3 鍵スケジューラ

(1) AVA(表 3.6)

いずれの項目においても最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。

(2) AVD(表 3.13)

いずれの項目においても期待値に近い。グラフに特徴は見られない。

(3) CC(表 3.20)

いずれの項目においても期待値に近い。

4.2 FEAL-NX

結果グラフは付録 B.2 を参照のこと。

4.2.1 ラウンド関数

(1) AVA(表 3.2)

いずれの項目においても最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.9)

「入力と出力の相関(Hw=1)」、「拡大鍵と出力の相関(Hw=1)」、「拡大鍵＝0固定での入出力相関(Hw=1)」では期待値より 6 ビット程度少ない。また、「入力と出力の相関(Hw=2)」、「拡大鍵と出力の相関(Hw=2)」、「拡大鍵＝0固定での入出力相関(Hw=2)」でも期待値より 3 ビット程度少ない。

(3) CC(表 3.16)

いずれの項目においても CC=1 となる部分がある。たとえば、入力ビット#0 を反転させたときに出力ビット#23 と#29 の反転状態に関係が見られる。

(4) UKV(表 3.23)

期待値から遠い。

4.2.2 データ攪拌部

(1) AVA(表 3.3)

「平文と暗号文の相関(Hw=1)」および「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。「段数経過(Hw=1)」では R2 および R3 のときに最悪偏差率が相対基準値より大きいが、R4 以降では相対基準値より小さい。

(2) AVD(表 3.10)

いずれの項目においても期待値に近い。

(3) CC(表 3.17)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3、R4 のときに期待値から遠い。R5 では期待値に近い。

4.2.3 鍵スケジューラ

(1) AVA(表 3.6)

いずれの項目においても最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.13)

「秘密鍵と拡大鍵の相関(Hw=1)」では期待値より 16 ビット程度少ない。「秘密鍵と拡大鍵の相関(Hw=2)」では期待値より 4〜19 ビット程度少なく、反転させるワードによってそのビット数は異なる。

(3) CC(表 3.20)

CC=1 となる部分がある。たとえば、秘密鍵ビット#0 を反転させたときに拡大鍵 K_1 の#7 と#13 の反転状態に関係が見られる。

4.3 Hierocrypt-L1

結果グラフは付録 B.3 を参照のこと。

4.3.1 ラウンド関数

(1) AVA(表 3.2)

「入力と出力の相関(Hw=2)」、「拡大鍵=0 固定での入出力相関(Hw=2)」においては最悪偏差率が相対基準値より小さい。その他の項目においては最悪偏差率が相対基準値より大きい。とくに「拡大鍵と出力の相関(Hw=1,2)」では最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.9)

「拡大鍵と出力の相関(Hw=1)」では期待値より 5 ビット程度少ない。その他の項目においては期待値に近い。

(3) CC(表 3.16)

いずれの項目においても期待値から遠い。

(4) UKV(表 3.23)

期待値から遠い。

4.3.2 データ攪拌部

(1) AVA(表 3.3)

いずれの項目においても最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。

(2) AVD(表 3.10)

いずれの項目においても期待値に近い。グラフに特徴は見られない。

(3) CC(表 3.17)

いずれの項目においても期待値に近い。

4.3.3 鍵スケジューラ

(1) AVA(表 3.6)

いずれの項目においても最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.13)

「秘密鍵と拡大鍵の相関(Hw=1)」では期待値より 36 ビット程度少ない。「秘密鍵と拡大鍵の相関(Hw=2)」では期待値より 1〜42 ビット程度少なく、反転させるワードによってそのビット数は異なる。

(3) CC(表 3.20)

CC=1 となる部分がある。

4.4 MISTY1

結果グラフは付録 B.4 を参照のこと。

4.4.1 ラウンド関数

(1) AVA(表 3.2)

いずれの項目においても最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.9)

「入力と出力の相関(Hw=1,2)」、「拡大鍵＝０固定での入出力相関(Hw=1,2)」では期待値に近い。「拡大鍵と出力の相関(Hw=1,2)」では期待値より 3〜7 ビット程度少ない。グラフに特徴が見られる。

(3) CC(表 3.16)

いずれの項目においても CC=1 となる部分がある。たとえば、入力ビット#12 を反転したときの出力ビット#0 と#9 の反転状態に関係が見られる。

(4) UKV(表 3.23)

期待値から遠い。

4.4.2 データ攪拌部

(1) AVA(表 3.3)

「平文と暗号文の相関(Hw=1)」および「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。「段数経過(Hw=1)」では R2 および R3 のときに最悪偏差率が相対基準値より大きいが、R4 以降では相対基準値より小さい。

(2) AVD(表 3.10)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」では期待値に近い。「段数経過(Hw=1)」では R2 のときに期待値より 7 ビット程度少ない。

(3) CC(表 3.17)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに期待値から遠い。R4 以降では期待値に近い。

4.4.3 鍵スケジューラ

(1) AVA(表 3.6)

いずれの項目においても最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.13)

いずれの項目も期待値より小さい。

(3) CC(表 3.20)

CC=1 となる部分がある。たとえば、秘密鍵 K_1 の#12 を反転させたときの拡大鍵 K'_1 の#2 と#17 の反転状態に関係が見られる。

4.5 Camellia

結果グラフは付録 B.5 を参照のこと。

4.5.1 ラウンド関数

(1) AVA(表 3.2)

いずれの項目においても最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.9)

「入力と出力の相関(Hw=1)」、「拡大鍵と出力の相関(Hw=1)」および「拡大鍵＝0固定での入出力相関(Hw=1)」では期待値より 10 ビット程度小さい。また、「入力と出力の相関(Hw=2)」、「拡大鍵と出力の相関(Hw=2)」および「拡大鍵＝0固定での入出力相関(Hw=2)」では期待値より 3 ビット程度小さい。グラフに特徴が見られる。

(3) CC(表 3.16)

いずれの項目においても CC=1 となる部分がある。たとえば、入力ビット#0 を反転させたときの出力ビット#0 と#8 の反転状態に関係がある。

(4) UKV(表 3.23)

期待値から遠い。

4.5.2 データ攪拌部(128bit)

(1) AVA(表 3.3)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1)」では R2、R3 のときに最悪偏差率が 1 となる部分があるが、R4 以降では相対基準値より小さい。

(2) AVD(表 3.10)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに期待値より小さいが、R4 以降は期待値に近い。

(3) CC(表 3.17)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに CC=1 となる部分がある。R4 のときは期待値から遠いが、R5 以降は期待値に近い。

4.5.3 データ攪拌部(192bit)

(1) AVA(表 3.4)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1)」においては R2、R3 では最悪偏差率が 1 となる部分がある。R4 以降は相対基準値より小さい。

(2) AVD(表 3.11)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに期待値より小さく、R4 以降は期待値に近い。

(3) CC(表 3.18)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに CC=1 となる部分がある。R4 のときは期待値から遠いが、R5 以降は期待値に近い。

4.5.4 データ攪拌部(256bit)

(1) AVA(表 3.5)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1)」においては R2、R3 では最悪偏差率が 1 となる部分がある。R4 以降は相対基準値より小さい。

(2) AVD(表 3.12)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに期待値より小さく、R4 以降は期待値に近い。

(3) CC(表 3.19)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに CC=1 となる部分がある。R4 のときは期待値から遠いが、R5 以降は期待値に近い。

4.5.5 鍵スケジューラ(128bit)

(1) AVA(表 3.6)

いずれの項目でも最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.13)

「秘密鍵と拡大鍵の相関(Hw=1)」では期待値より 1 ビット程度大きい。「秘密鍵と拡大鍵の相関(Hw=2)」では期待値より 2 ビット程度大きい。

(3) CC(表 3.20)

期待値に近い。

4.5.6 鍵スケジューラ(192bit)

(1) AVA(表 3.7)

いずれの項目でも最悪偏差率が 1 となる部分がある。

(2) AVD(表 3.14)

「秘密鍵と拡大鍵の相関(Hw=1)」では期待値より 1 ビット程度大きい。「秘密鍵と拡大鍵の相関(Hw=2)」では W0、W1、W2 および W3 のときに期待値より 2 ビット程度大きい。W4、W5 のときは期待値より 4 ビット程度大きい。

(3) CC(表 3.21)

期待値に近い。

4.5.7 鍵スケジューラ(256bit)

(1) AVA(表 3.8)

いずれの項目でも最悪偏差率が 1 となる部分がある。

(2) AVD(表 3.15)

「秘密鍵と拡大鍵の相関(Hw=1)」では期待値より 1 ビット程度大きい。「秘密鍵と拡大鍵の相関(Hw=2)」では期待値より 2 ビット程度大きい。

(3) CC(表 3.22)

期待値に近い。

4.6 CIPHERUNICORN-A

結果グラフは付録 B.6 を参照のこと。

4.6.1 ラウンド関数

(1) AVA(表 3.2)

いずれの項目においても最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。

(2) AVD(表 3.9)

いずれの項目においても期待値に近い。グラフに特徴は見られない。

(3) CC(表 3.16)

いずれの項目においても期待値に近い。

(4) UKV(表 3.23)

期待値に近い。

4.6.2 データ攪拌部(128bit)

(1) AVA(表 3.3)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。「段数経過(Hw=1) 」では R2 のときに最悪偏差率が相対基準値より大きいが、R3 以降では相対基準値より小さい。

(2) AVD(表 3.10)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)においては期待値に近い。「段数経過」では R2 のときに期待値より小さいが、R3 以降では期待値に近い。

(3) CC(表 3.17)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2 のときに期待値から遠いが、R3 以降では期待値に近い。

4.6.3 データ攪拌部(192bit)

(1) AVA(表 3.4)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1) 」では R2 のときに最悪偏差率が相対基準値より大きいが、R3 以降では相対基準値より小さい。

(2) AVD(表 3.11)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)においては期待値に近い。「段数経過」では R2 のときに期待値より小さいが、R3 以降では期待値に近い。

(3) CC(表 3.18)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2 のときに期待値から遠いが、R3 以降では期待値に近い。

4.6.4 データ攪拌部(256bit)

(1) AVA(表 3.5)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1) 」では R2 のときに最悪偏差率が相対基準値より大きいが、R3 以降では相対基準値より小さい。

(2) AVD(表 3.12)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過」では R2 のときに期待値より小さいが、R3 以降では期待値に近い。

(3) CC(表 3.19)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2 のときに期待値から遠いが、R3 以降では期待値に近い。

4.6.5 鍵スケジューラ(128bit)

(1) AVA(表 3.6)

いずれの項目においても最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。

(2) AVD(表 3.13)

いずれの項目においても期待値に近い。グラフに特徴は見られない。

(3) CC(表 3.20)

期待値に近い。

4.6.6 鍵スケジューラ(192bit)

(1) AVA(表 3.6)

いずれの項目においても最悪偏差率が相対基準値より小さい。

(2) AVD(表 3.14)

いずれの項目においても期待値に近い。

(3) CC(表 3.21)

期待値に近い。

4.6.7 鍵スケジューラ(256bit)

(1) AVA(表 3.8)

いずれの項目においても最悪偏差率が相対基準値より小さい。

(2) AVD(表 3.15)

いずれの項目においても期待値に近い。

(3) CC(表 3.22)

期待値に近い。

4.7 Hierocrypt-3

結果グラフは付録 B.7 を参照のこと。

4.7.1 ラウンド関数

(1) AVA(表 3.2)

「入力と出力の相関(Hw=2)」,「拡大鍵=0 固定での入出力相関(Hw=2)」においては最悪偏差率が相対基準値より小さい。その他の項目においては最悪偏差率が相対基準値より大きい。とくに「拡大鍵と出力の相関(Hw=1,2)」,「拡大鍵=0 固定での入出力相関(Hw=1)」においては最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.9)

「入力と出力の相関(Hw=1,2)」、「拡大鍵=0 固定での入出力相関(Hw=1,2)」においては期待値に近い。「拡大鍵と出力の相関(Hw=1)」では期待値より 10 ビット程度小さい。「拡大鍵と出力の相関(Hw=2)」では期待値より 2 ビット程度小さい。グラフに特徴が見られる。

(3) CC(表 3.16)

いずれの項目も CC=1 となる部分がある。

(4) UKV(表 3.23)

期待値から遠い。

4.7.2 データ攪拌部(128bit)

(1) AVA(表 3.3)

いずれの項目においても最悪偏差率が相対基準値より小さい。グラフに特徴が見られない。

(2) AVD(表 3.10)

いずれの項目においても期待値に近い。グラフに特徴が見られない。

(3) CC(表 3.17)

いずれの項目においても期待値に近い。

4.7.3 データ攪拌部(192bit)

(1) AVA(表 3.4)

いずれの項目においても最悪偏差率が相対基準値より小さい。

(2) AVD(表 3.11)

いずれの項目においても期待値に近い。

(3) CC(表 3.18)

いずれの項目においても期待値に近い。

4.7.4 データ攪拌部(256bit)

(1) AVA(表 3.5)

いずれの項目においても最悪偏差率が相対基準値より小さい。

(2) AVD(表 3.12)

いずれの項目においても期待値に近い。

(3) CC(表 3.19)

いずれの項目においても期待値に近い。

4.7.5 鍵スケジューラ(128bit)

(1) AVA(表 3.6)

いずれの項目においても最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.13)

いずれの項目においても期待値から離れている。「秘密鍵と拡大鍵の相関(Hw=1)」では期待値より 115 ビット程度小さい。「秘密鍵と拡大鍵の相関(Hw=2)」ではワードによって期待値より大きい場合と小さい場合がある。

(3) CC(表 3.20)

CC=1 となる部分がある。

4.7.6 鍵スケジューラ(192bit)

(1) AVA(表 3.7)

いずれの項目においても最悪偏差率が 1 となる部分がある。

(2) AVD(表 3.14)

いずれの項目においても期待値から離れている。「秘密鍵と拡大鍵の相関(Hw=1)」では期待値より 283 ビット程度小さい。「秘密鍵と拡大鍵の相関(Hw=2)」ではワードによって期待値より大きい場合と小さい場合がある。

(3) CC(表 3.21)

CC=1 となる部分がある。

4.7.7 鍵スケジューラ(256bit)

(1) AVA(表 3.8)

いずれの項目においても最悪偏差率が 1 となる部分がある。

(2) AVD(表 3.15)

いずれの項目においても期待値から離れている。「秘密鍵と拡大鍵の相関(Hw=1)」では期待値より 229 ビット程度小さい。「秘密鍵と拡大鍵の相関(Hw=2)」ではワードによって期待値より大きい場合と小さい場合がある。

(3) CC(表 3.22)

CC=1 となる部分がある。

4.8 MARS

結果グラフは付録 B.8 を参照のこと。

4.8.1 ラウンド関数

(1) AVA(表 3.2)

いずれの項目においても最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.9)

いずれの項目も期待値より小さい。グラフに特徴が見られる。「入力と出力の相関」と「拡大鍵＝０固定での入出力相関」のときでは結果が異なる。

(3) CC(表 3.16)

いずれの項目においても期待値から遠い。

(4) UKV(表 3.23)

期待値より小さい。

4.8.2 データ攪拌部(128bit)

(1) AVA(表 3.3)

いずれの項目においても最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。

(2) AVD(表 3.10)

いずれの項目においても期待値に近い。グラフに特徴は見られない。

(3) CC(表 3.17)

いずれの項目においても期待値に近い。

4.8.3 データ攪拌部(192bit)

(1) AVA(表 3.4)

いずれの項目においても最悪偏差率が相対基準値より小さい。

(2) AVD(表 3.11)

いずれの項目においても期待値に近い。

(3) CC(表 3.18)

いずれの項目においても期待値に近い。

4.8.4 データ攪拌部(256bit)

(1) AVA(表 3.5)

いずれの項目においても最悪偏差率が相対基準値より小さい。

(2) AVD(表 3.12)

いずれの項目においても期待値に近い。

(3) CC(表 3.19)

いずれの項目においても期待値に近い。

4.8.5 鍵スケジューラ(128bit)

(1) AVA(表 3.6)

いずれの項目においても最悪偏差率が 1 となる部分がある。

(2) AVD(表 3.13)

いずれの項目においても期待値より 16 ビット程度少ない。

(3) CC(表 3.20)

期待値から遠い。

4.8.6 鍵スケジューラ(192bit)

(1) AVA(表 3.7)

いずれの項目においても最悪偏差率が 1 となる部分がある。

(2) AVD(表 3.14)

いずれの項目においても期待値より 16 ビット程度少ない。

(3) CC(表 3.21)

期待値から遠い。

4.8.7 鍵スケジューラ(256bit)

(1) AVA(表 3.8)

いずれの項目においても最悪偏差率が 1 となる部分がある。

(2) AVD(表 3.15)

いずれの項目においても期待値より 16 ビット程度少ない。

(3) CC(表 3.22)

期待値から遠い。

4.9 RC6

結果グラフは付録 B.9 を参照のこと。

4.9.1 ラウンド関数

(1) AVA(表 3.2)

いずれの項目においても最悪偏差率が相対基準値より大きい。とくに「拡大鍵と出力の相関(Hw=1,2)」では最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.9)

いずれの項目においても期待値から遠い。グラフに特徴が見られる。

(3) CC(表 3.16)

「入力と出力の相関(Hw=1)」においては期待値から遠い。「拡大鍵＝０固定での入出力相関(Hw=1)」においては CC=1 となる部分がある。

(4) UKV(表 3.23)

期待値から遠い。

4.9.2 データ攪拌部（128bit）

(1) AVA(表 3.3)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1)」では R2、R3、R4、R5 のときに最悪偏差率が相対基準値より大きく、R6 で相対基準値より小さくなる。グラフに特徴が見られる。

(2) AVD(表 3.10)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3、R4 のときに期待値より小さく、R5 以降は期待値に近い。グラフに特徴が見られる。

(3) CC(表 3.17)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3、R4、R5 のときに期待値から遠く、R6 以降は期待値に近い。

4.9.3 データ攪拌部（192bit）

(1) AVA(表 3.4)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1)」では R2、R3、R4、R5 のときに最悪偏差率が相対基準値より大きく、R6 で相対基準値より小さくなる。

(2) AVD(表 3.11)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3、R4 のときに期待値より小さく、R5 以降は期待値に近い。

(3) CC(表 3.18)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3、R4、R5 のときに期待値から遠く、R6 以降は期待値に近い。

4.9.4 データ攪拌部（256bit）

(1) AVA(表 3.5)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1)」では R2、R3、R4、R5 のときに最悪偏差率が相対基準値より大きく、R6 で相対基準値より小さくなる。

(2) AVD(表 3.12)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3、R4 のときに期待値より小さく、R5 以降は期待値に近い。

(3) CC(表 3.19)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3、R4、R5 のときに期待値から遠く、R6 以降は期待値に近い。

4.9.5 鍵スケジューラ（128bit）

(1) AVA(表 3.6)

いずれの項目においても最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。

(2) AVD(表 3.13)

いずれの項目においても期待値に近い。グラフに特徴は見られない。

(3) CC(表 3.20)

期待値に近い。

4.9.6 鍵スケジューラ（192bit）

(1) AVA(表 3.7)

いずれの項目においても最悪偏差率が相対基準値より小さい。

(2) AVD(表 3.14)

いずれの項目においても期待値に近い。

(3) CC(表 3.21)

期待値に近い。

4.9.7 鍵スケジューラ（256bit）

(1) AVA(表 3.8)

いずれの項目においても最悪偏差率が相対基準値より小さい。

(2) AVD(表 3.15)

いずれの項目においても期待値に近い。

(3) CC(表 3.22)

期待値に近い。

4.10 SC2000

結果グラフは付録 B.10 を参照のこと。

4.10.1 ラウンド関数

(1) AVA(表 3.2)

いずれの項目においても最悪偏差率が 1 となる部分がある。グラフに特徴が見られる。

(2) AVD(表 3.9)

「入力と出力の相関(Hw=1)」では期待値より 7 ビット程度少ない。「入力と出力相関(Hw=2)」では期待値より 4 ビット程度少ない。グラフに特徴が見られる。

(3) CC(表 3.16)

CC=1 となる部分がある。たとえば、入力ビット#0 を反転させたときの出力ビット#1 と#33 の反転状態に関係がある。

(4) UKV

対象となるラウンド関数では拡大鍵を使用しないため、計測しなかった。

4.10.2 データ攪拌部(128bit)

(1) AVA(表 3.3)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1)」では R2、R3 のときに最悪偏差率が相対基準値より大きいが、R4 以降では相対基準値より小さい。

(2) AVD(表 3.10)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに期待値より小さいが、R4 以降では期待値に近い。

(3) CC(表 3.17)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに期待値から遠いが、R4 以降では期待値に近い。

4.10.3 データ攪拌部(192bit)

(1) AVA(表 3.4)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1)」では R2、R3 のときに最悪偏差率が相対基準値より大きいが、R4 以降では相対基準値より小さい。

(2) AVD(表 3.11)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに期待値より小さいが、R4 以降では期待値に近い。

(3) CC(表 3.18)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに期待値から遠いが、R4 以降では期待値に近い。

4.10.4 データ攪拌部(256bit)

(1) AVA(表 3.5)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては最悪偏差率が相対基準値より小さい。「段数経過(Hw=1)」では R2、R3 のときに最悪偏差率が相対基準値より大きいが、R4 以降では相対基準値より小さい。

(2) AVD(表 3.12)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに期待値より小さいが、R4 以降では期待値に近い。

(3) CC(表 3.19)

「平文と暗号文の相関(Hw=1)」、「秘密鍵と暗号文の相関(Hw=1)」においては期待値に近い。「段数経過(Hw=1)」では R2、R3 のときに期待値から遠いが、R4 以降では期待値に近い。

4.10.5 鍵スケジューラ(128bit)

(1) AVA(表 3.6)

いずれの項目においても最悪偏差率が相対基準値より小さい。グラフに特徴は見られない。

(2) AVD(表 3.13)

いずれの項目においても期待値に近い。グラフに特徴は見られない。

(3) CC(表 3.20)

期待値に近い。

4.10.6 鍵スケジューラ(192bit)

(1) AVA(表 3.7)

いずれの項目においても最悪偏差率が相対基準値より小さい。

(2) AVD(表 3.14)

いずれの項目においても期待値に近い。

(3) CC(表 3.21)

CC=1 となる部分がある。たとえば、秘密鍵ビット#128 を反転させたときの拡大鍵 ek[1]#30 と ek[3]#31 の反転状態に関係がある。

4.10.7 鍵スケジューラ(256bit)

(1) AVA(表 3.8)

いずれの項目においても最悪偏差率が相対基準値より小さい。

(2) AVD(表 3.15)

いずれの項目においても期待値に近い。

(3) CC(表 3.22)

CC=1 となる部分がある。たとえば、秘密鍵ビット#0 を反転させたときの拡大鍵 ek[1]#31 と ek[3]#30 の反転状態に関係がある。

A 参考文献

[UNIE] 暗号技術仕様書 CIPHERUNICORN-E, 電子政府応募資料.

[FEAL] FEAL-NX 仕様書, 電子政府応募資料.

[HIL1] 暗号技術仕様書:Hierocrypt-L1, 電子政府応募資料.

[MIST] 暗号技術仕様書 MISTY1, 電子政府応募資料.

[CAME] 128 ビットブロック暗号 Camellia アルゴリズム仕様書, 電子政府応募資料.

[UNIA] 暗号技術仕様書 CIPHERUNICORN-A, 電子政府応募資料.

[HI3] 暗号技術仕様書:Hierocrypt-3, 電子政府応募資料.

[MARS] MARS(AES 候補の暗号) 共通鍵暗号方式 技術仕様書, 電子政府応募資料.

[RC6] RC6 ブロック暗号, 電子政府応募資料.

[SC] 共通鍵ブロック暗号 SC2000 暗号技術仕様書, 電子政府応募資料.

[WT85] A. F. Webster and S.E. Tavares, “On the Design of S-boxes,” CRYPTO’85, pp.523-534, Springer-Verlag, 1985.

[F88] R. Forre, “The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition,” CRYPTO’88, LNCS403, pp.450-468, Springer-Verlag, 1990.

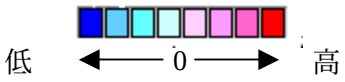
[KS97] K. Kurosawa and T. Satoh, “Design of SAC/PC(l) of Order k Boolean Functions and Three Other Cryptographic Criteria,” EUROCRYPT’97, LNCS1233, pp.434-449, Springer-Verlag, 1997.

[TOM00] Y. Tsunoo, R. Ohta, H. Miyauchi and K. Nakamura, “A Cipher Strength Evaluation System using PC’s Power,” SCIS2000-A53, The 2000 Symposium on Cryptography and Information Security, The Institute of Electronics, Information and Communication Engineers, 2000.

B 結果グラフ

グラフの書式は以下とする。

(1) カラー



(2) 座標

(A) AVA グラフ

Att.bit：反転させた入力(あるいは鍵)ビット番号

Rel.bit：出力ビット番号

(B) AVD グラフ

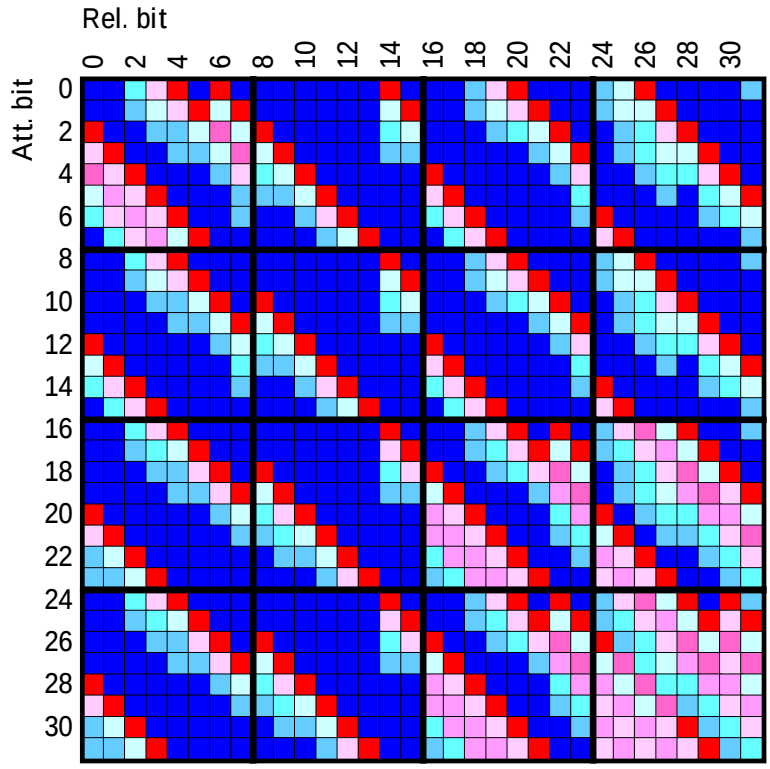
Att.bit：反転させた入力(あるいは鍵)ビット番号

Rel.bit：反転した出力ビット数

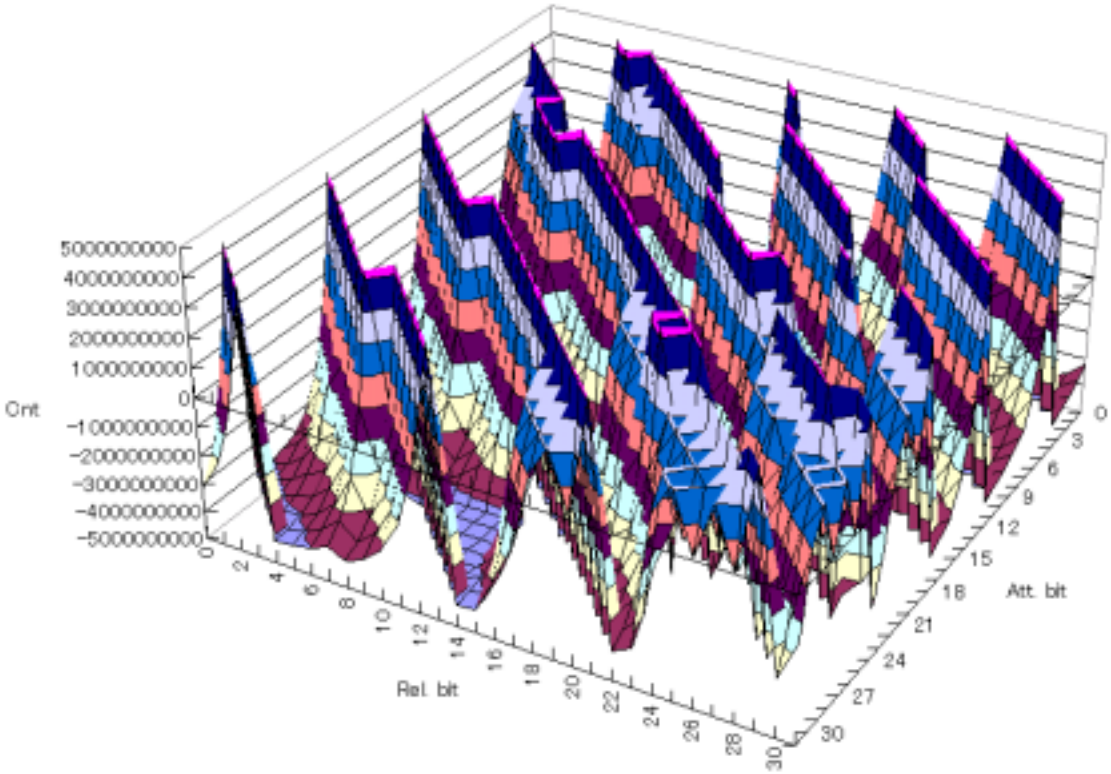
(3) 高低差のスケール

同一の評価項目であれは同一のスケールで表現しているのでグラフの高低をそのまま比較することができる。

(4) 例



例 1.グラフ A(２次元)



例 2.グラフ A(3 次元)

B 結果グラフ

B.1 CIPHERUNICORN-E

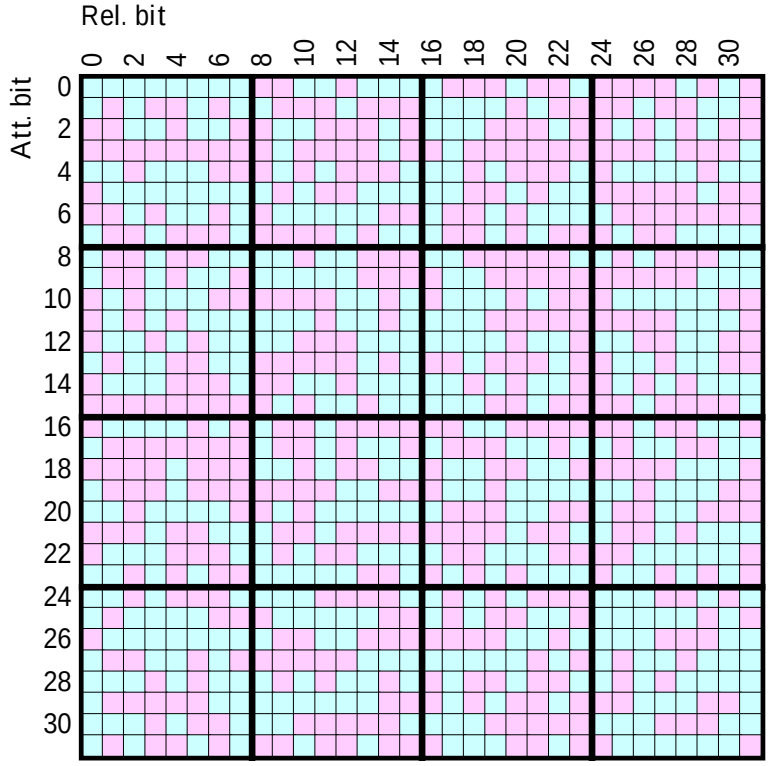


図 B.1.1 UNIE ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVA

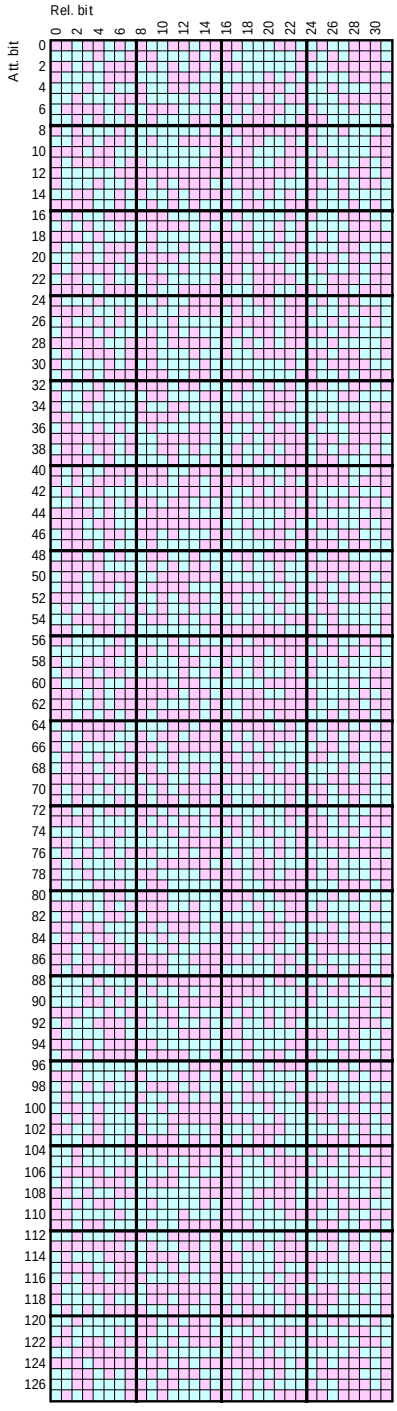


図 B.1.2 UNIE ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVA

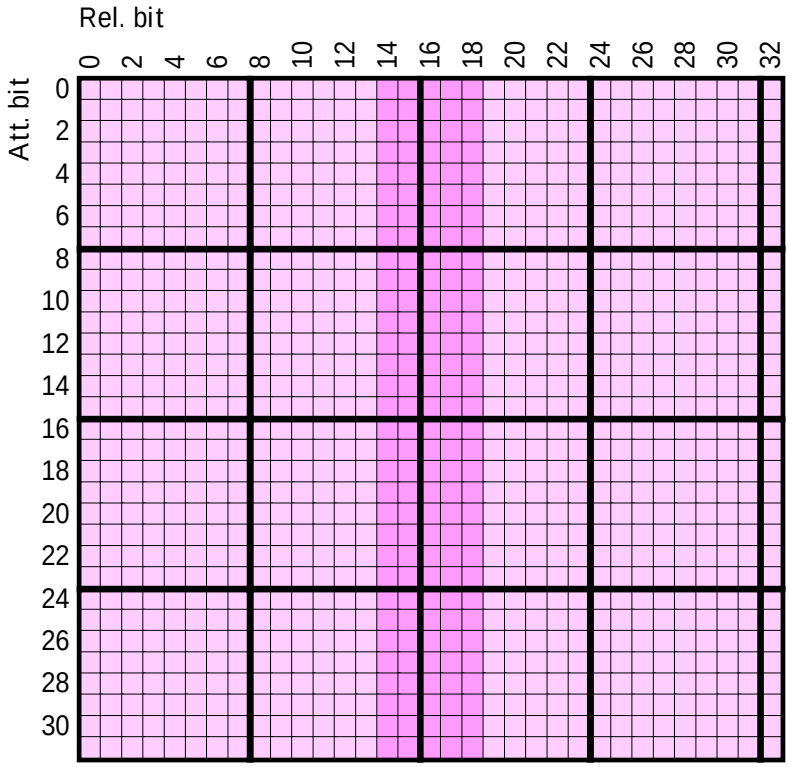


図 B.1.3 UNIE ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVD

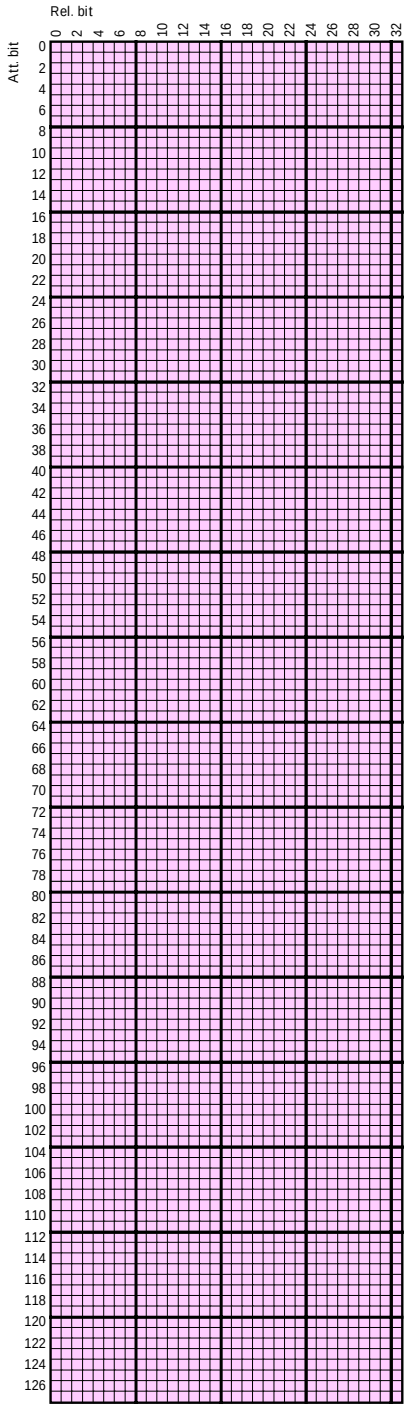


図 B.1.4 UNIE ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVD

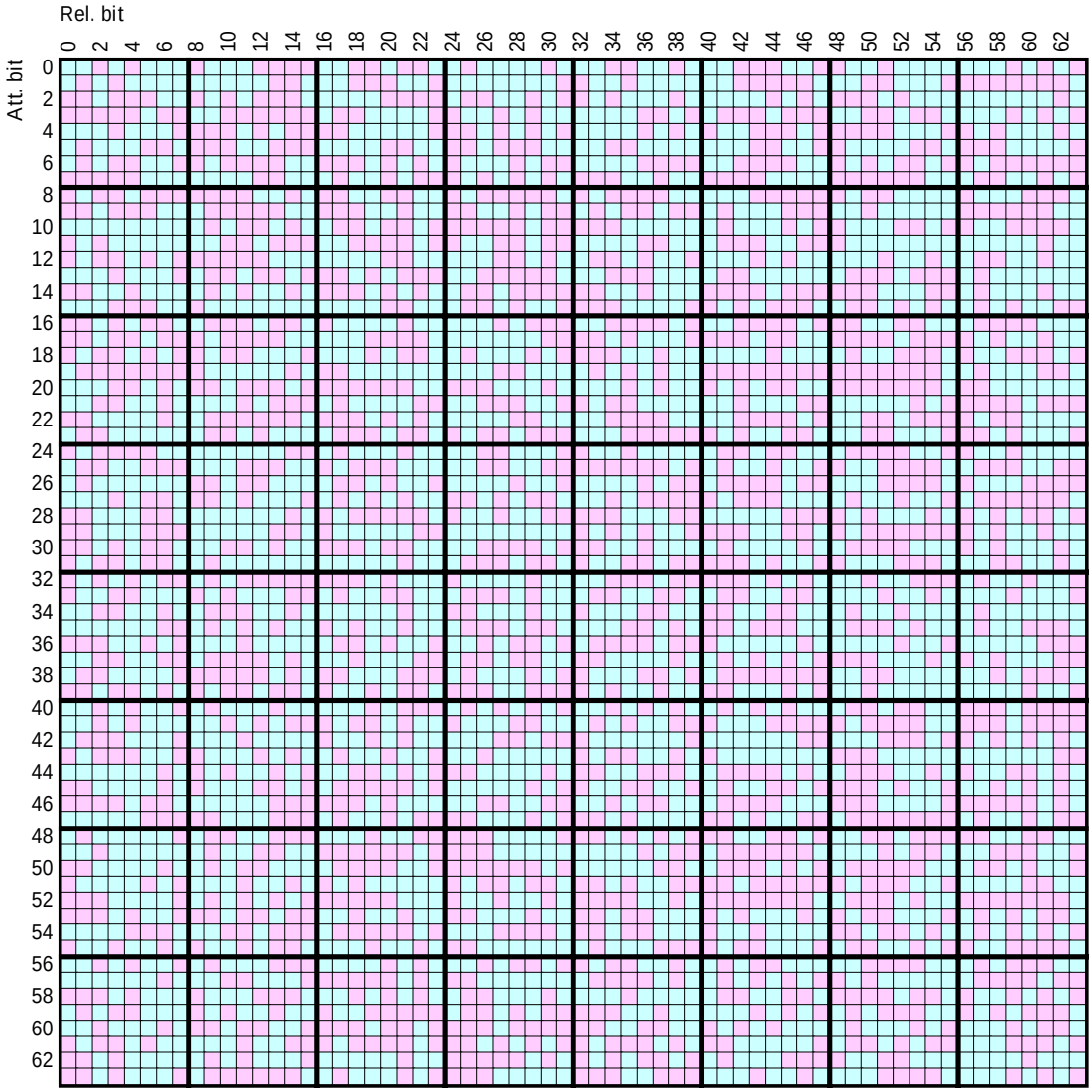


図 B.1.5 UNIE ﾃﾞｰﾀ攪拌部 段数経過(Hw=1) R4 AVA

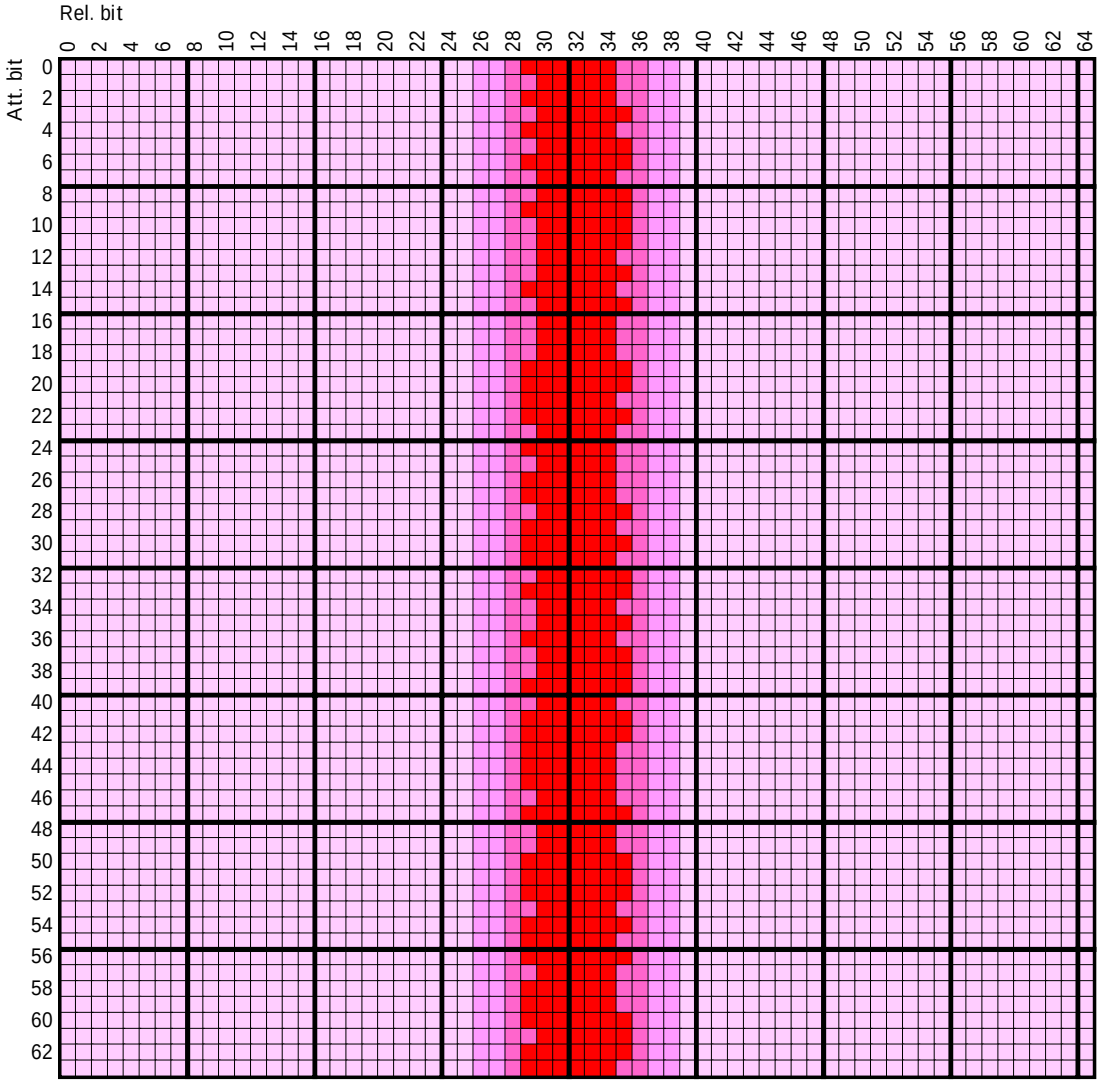


図 B.1.6 UNIE ﾃﾞｰﾀ攪拌部 段数経過(Hw=1) R4 AVD

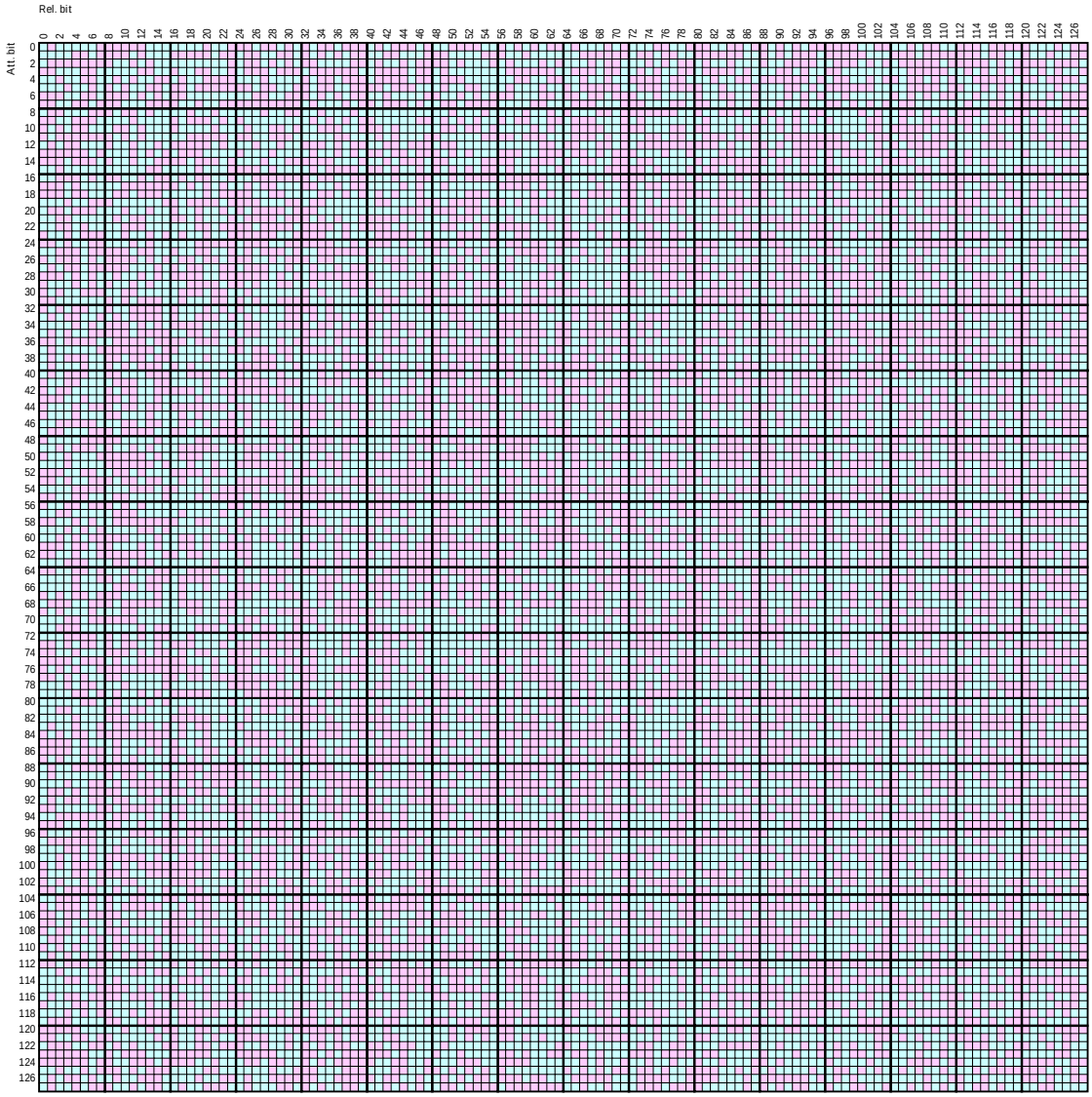
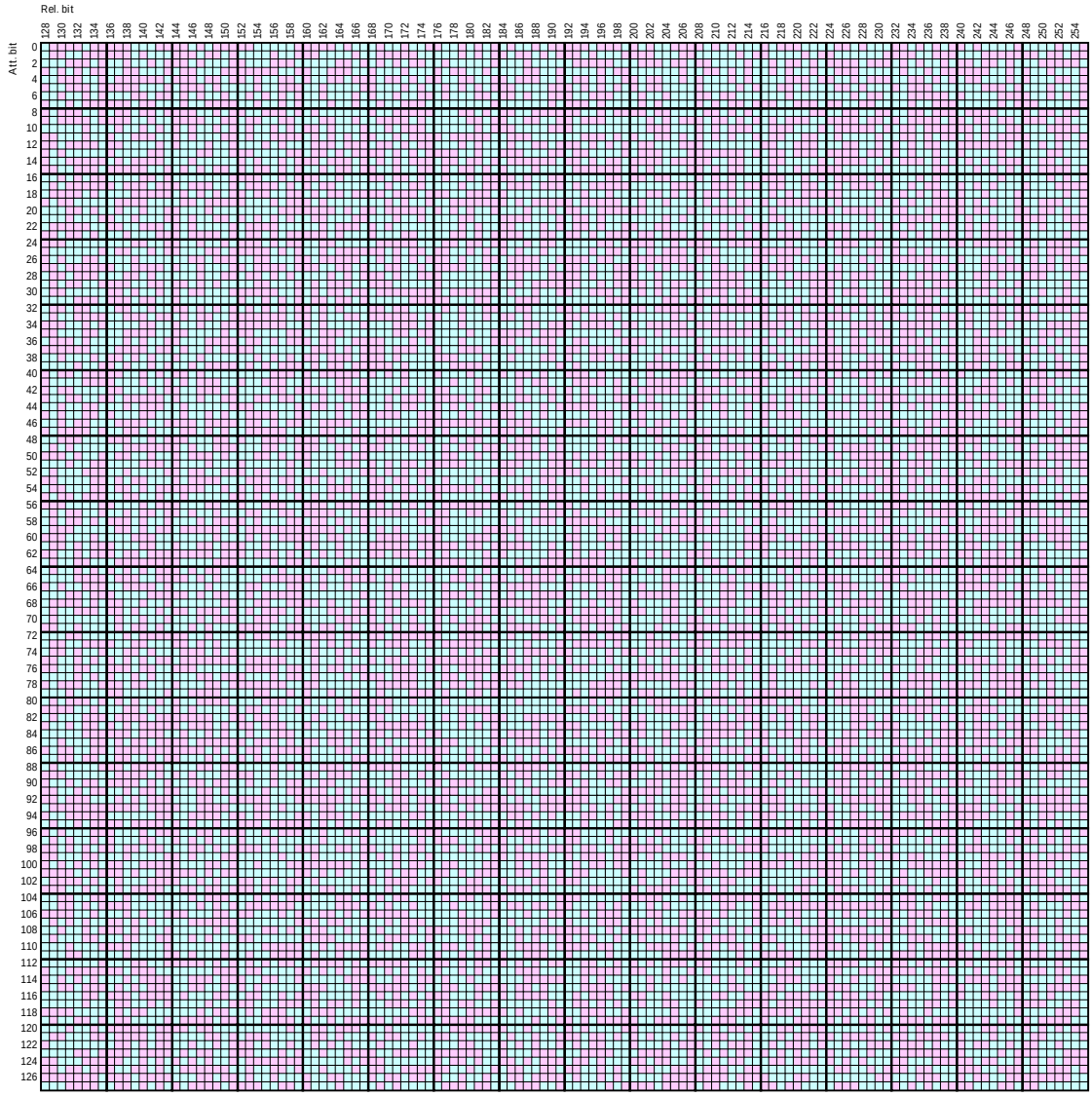


図 B.1.7 UNIE 鍵ｽｹｼﾞｭｰﾗ 秘密鍵と拡大鍵の相関(Hw=1) AVA(1/2)



※拡大鍵長が 256bit を越えるため、拡大鍵の上位 256bit のみを
グラフ表示している。

図 B.1.8 UNIE 鍵ｽｹｼﾞｭｰﾗ 秘密鍵と拡大鍵の相関(Hw=1) AVA(2/2)

B 結果グラフ

B.2 FEAL-NX

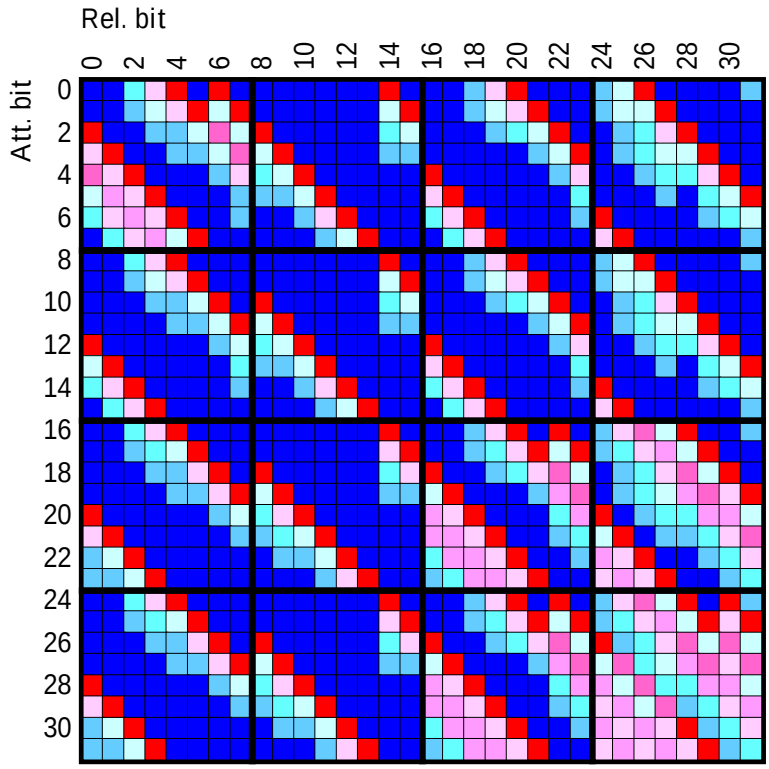


図 B.2.1 FEAL ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVA

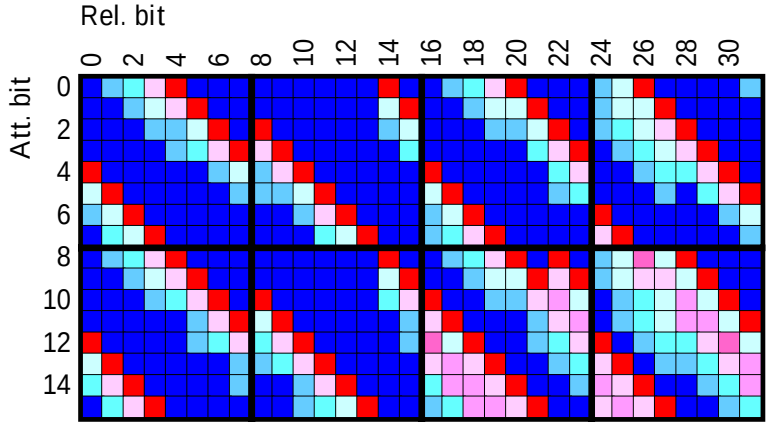


図 B.2.2 FEAL ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVA

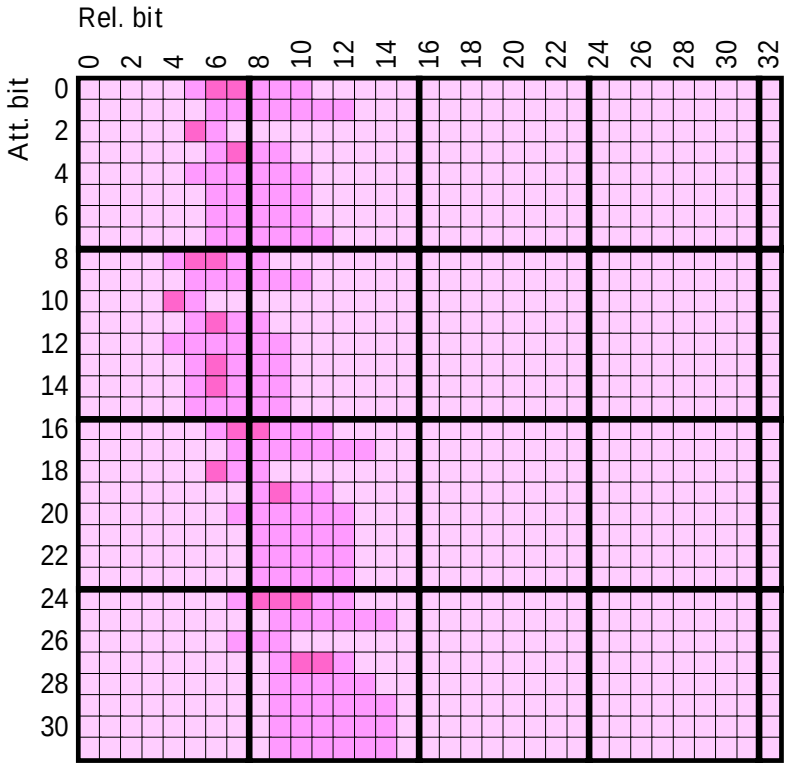


図 B.2.3 FEAL ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVD

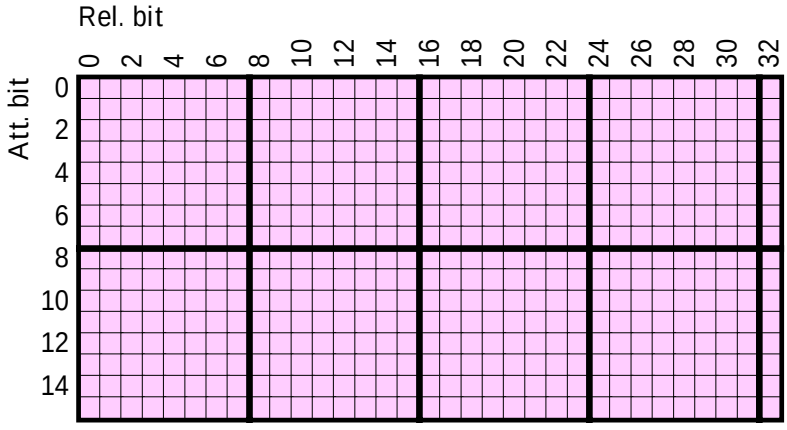


図 B.2.4 FEAL ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVD

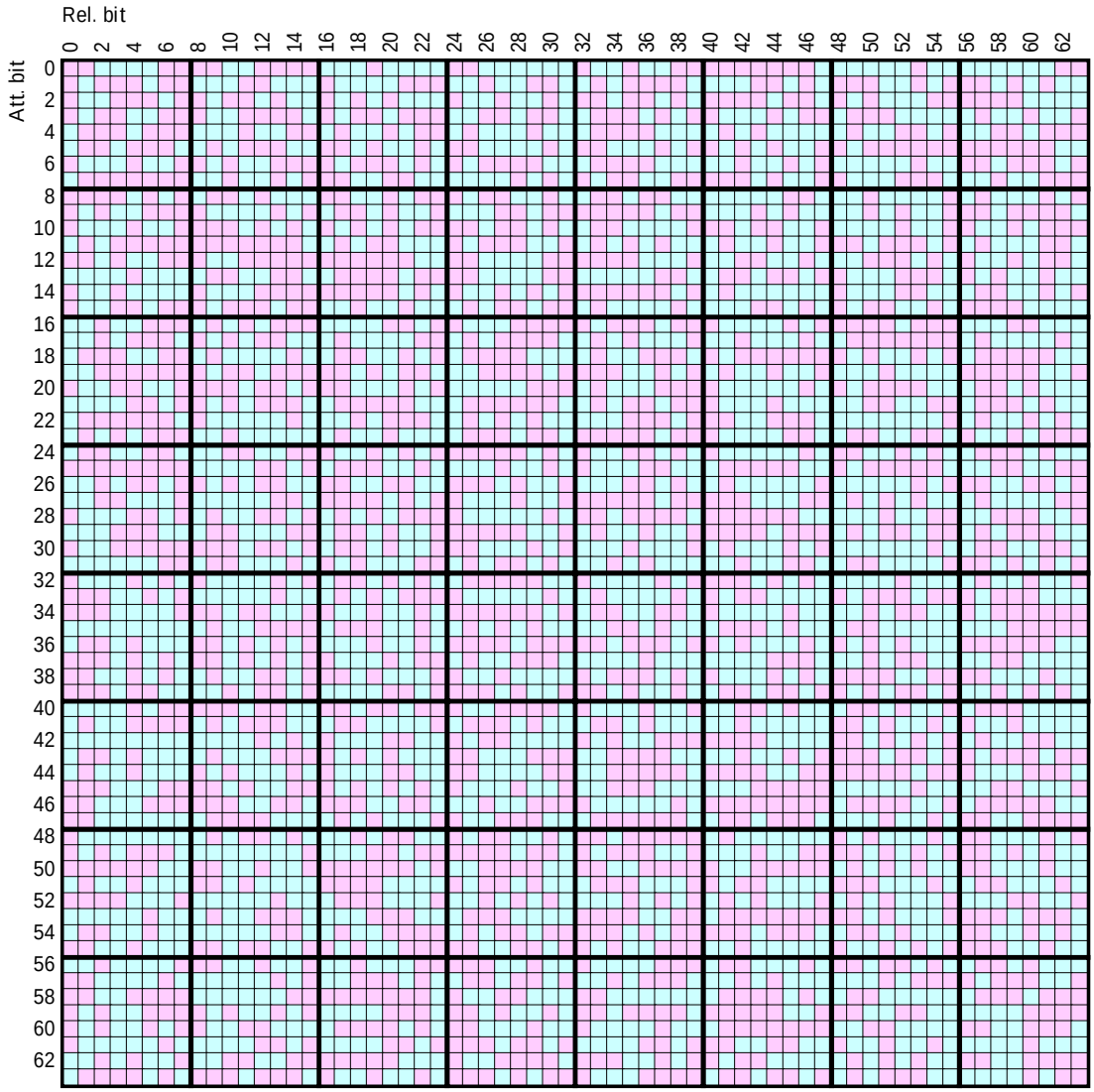


図 B.2.5 FEAL ﾃﾞｰﾀ攪拌部 段数経過(Hw=1) R4 AVA

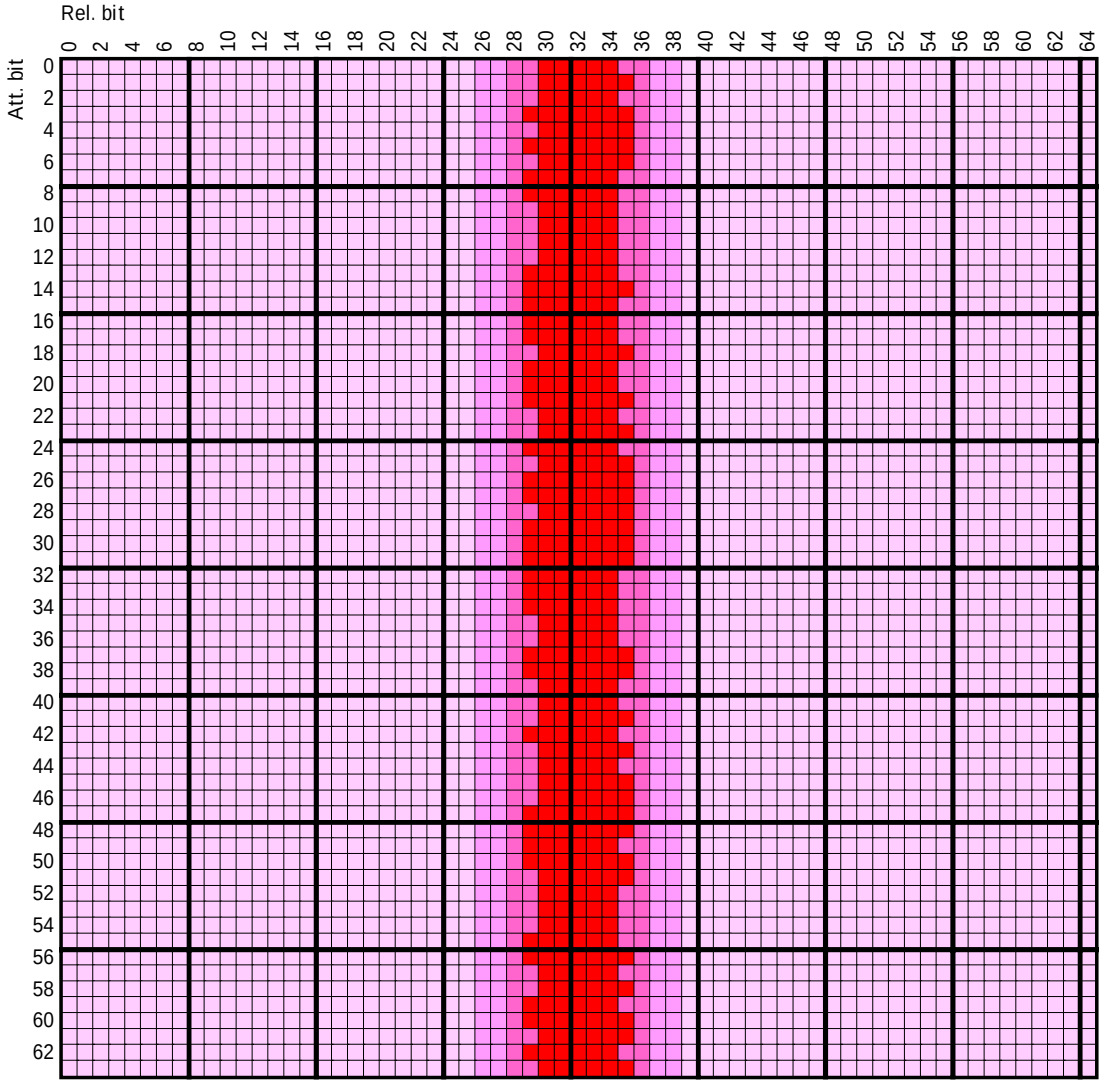


図 B.2.6 FEAL ﾃﾞｰﾀ攪拌部 段数経過(Hw=1) R4 AVD

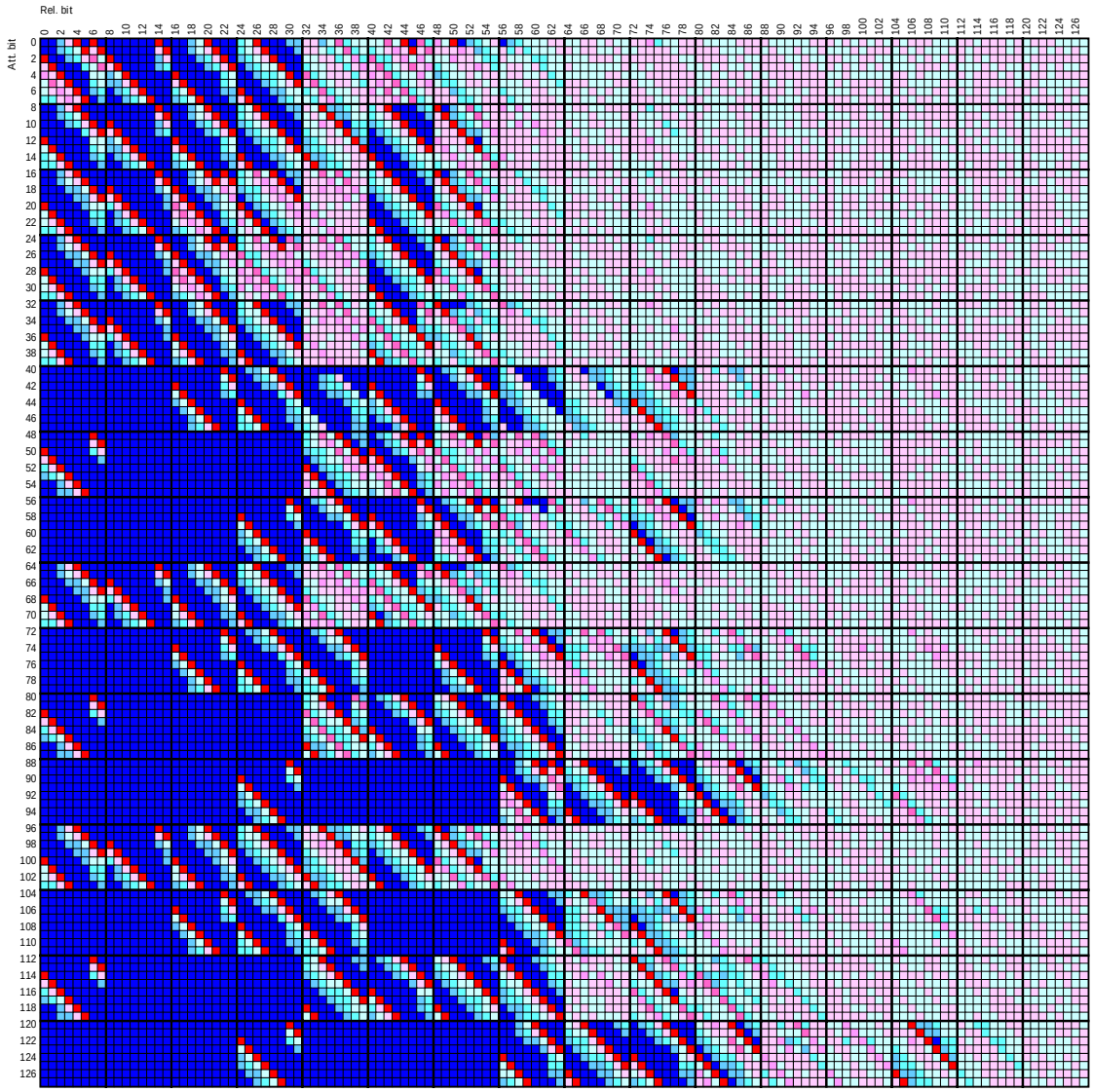
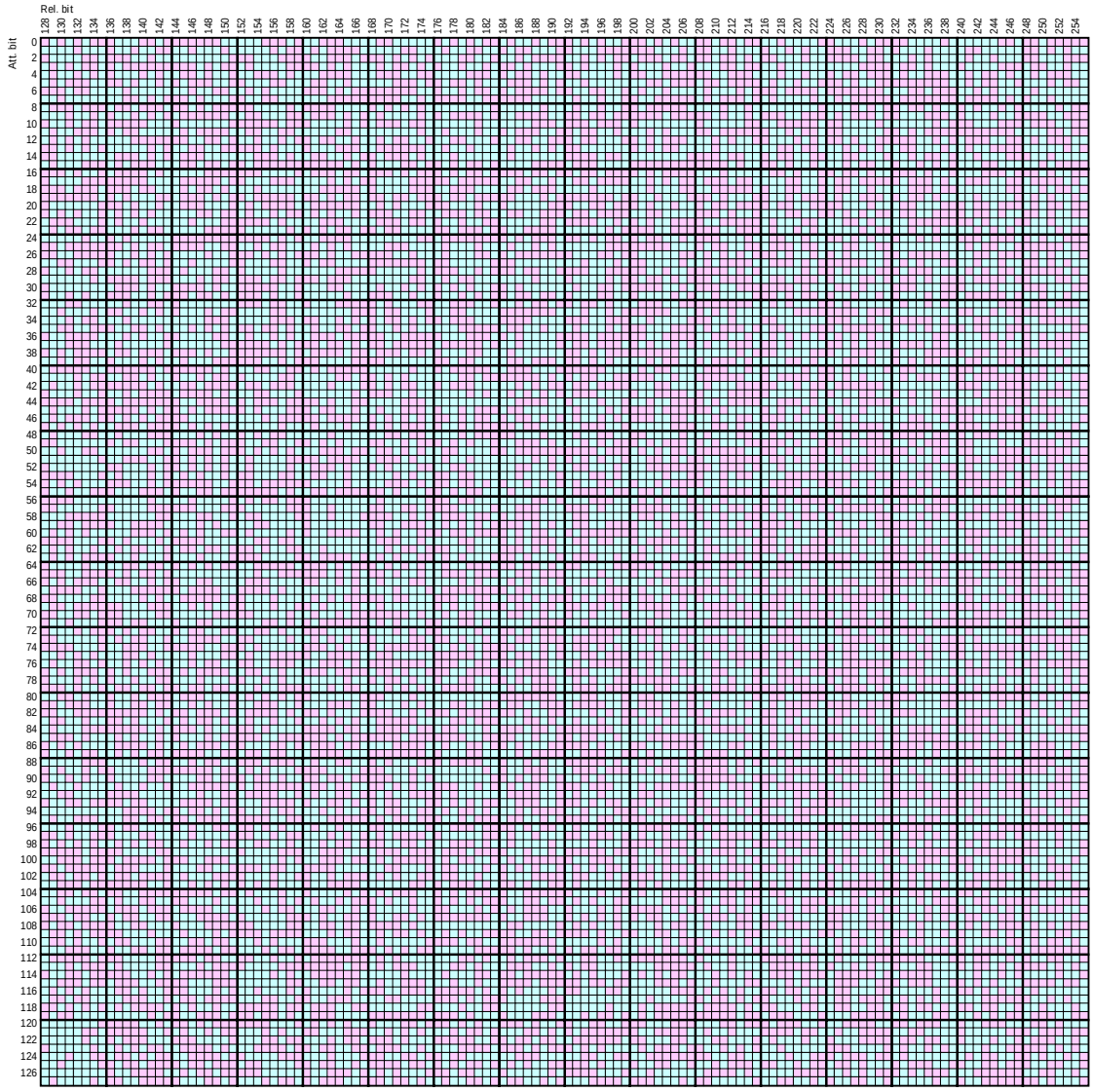


図 B.2.7 FEAL 鍵ｽｹｼﾞｭｰﾗ 秘密鍵と拡大鍵の相関(Hw=1) AVA(1/2)

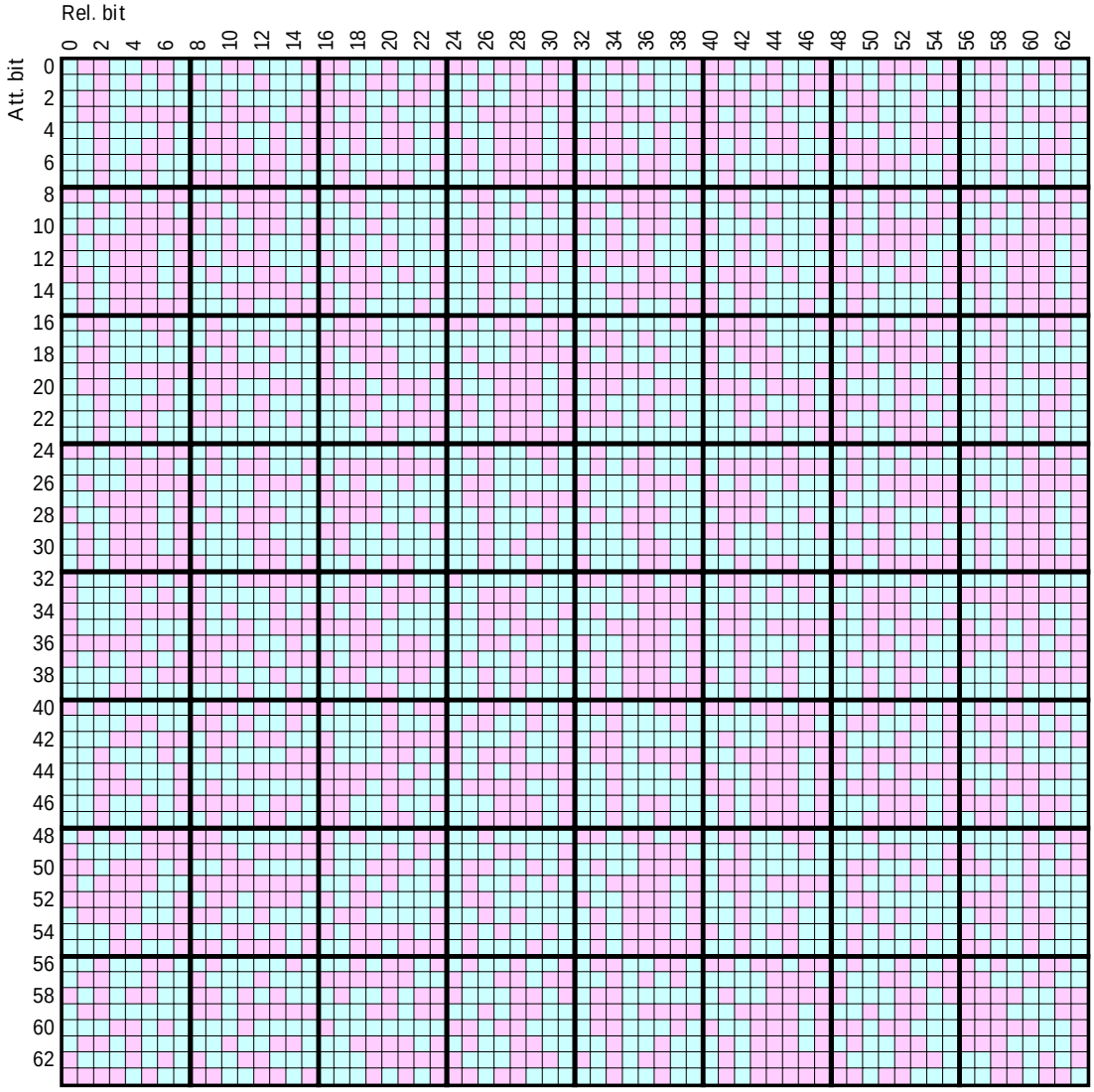


※拡大鍵長が 256bit を越えるため、拡大鍵の上位 256bit のみを
グラフ表示している。

図 B.2.8 FEAL 鍵ｽｹｼﾞｭｰﾗ 秘密鍵と拡大鍵の相関(Hw=1) AVA(2/2)

B 結果グラフ

B.3 Hierocrypt-L1



※ﾃﾞｰﾀ件数が他に比べて 1/4 である。同一のｽｹｰﾙで比較するために推測値として評価値を 4 倍した。

図 B.3.1 HiL1 ﾗｳﾝﾄﾞ関数　入力と出力の相関(Hw=1) AVA

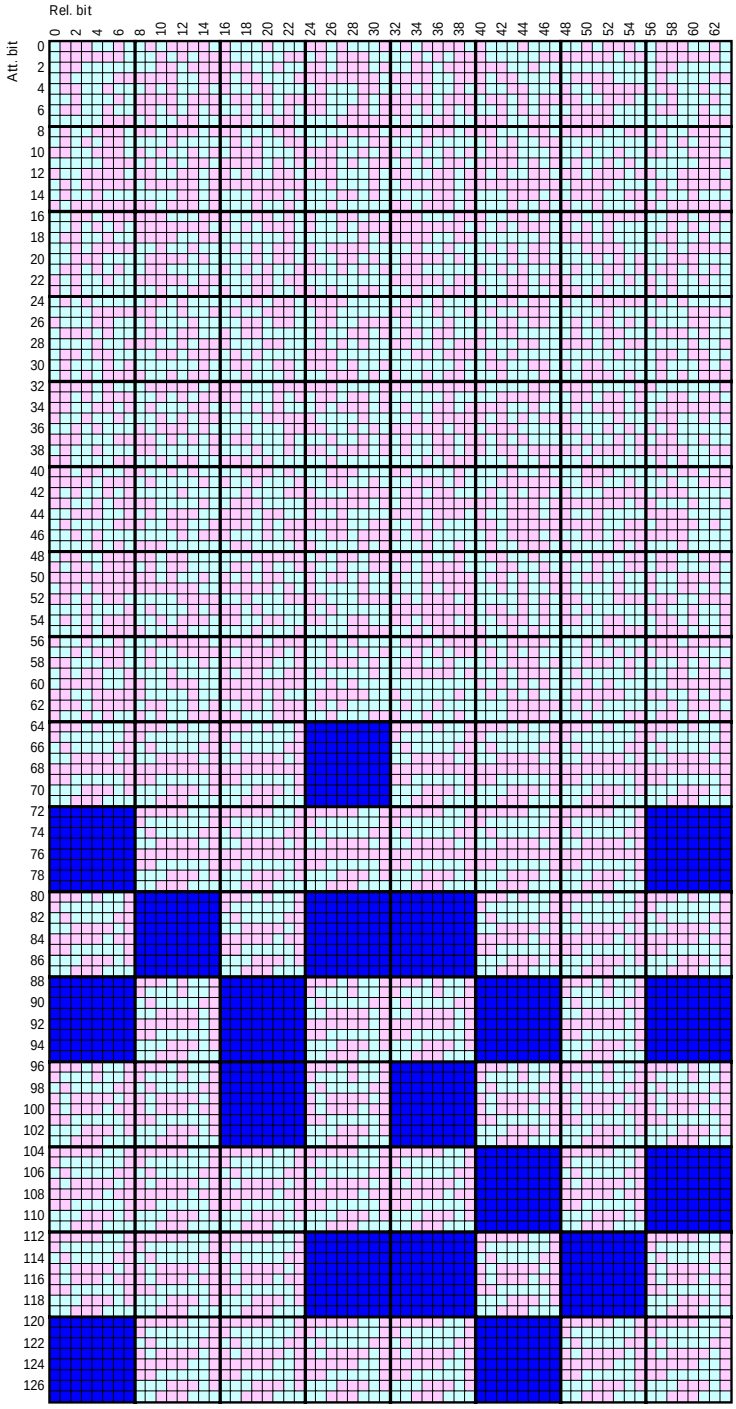
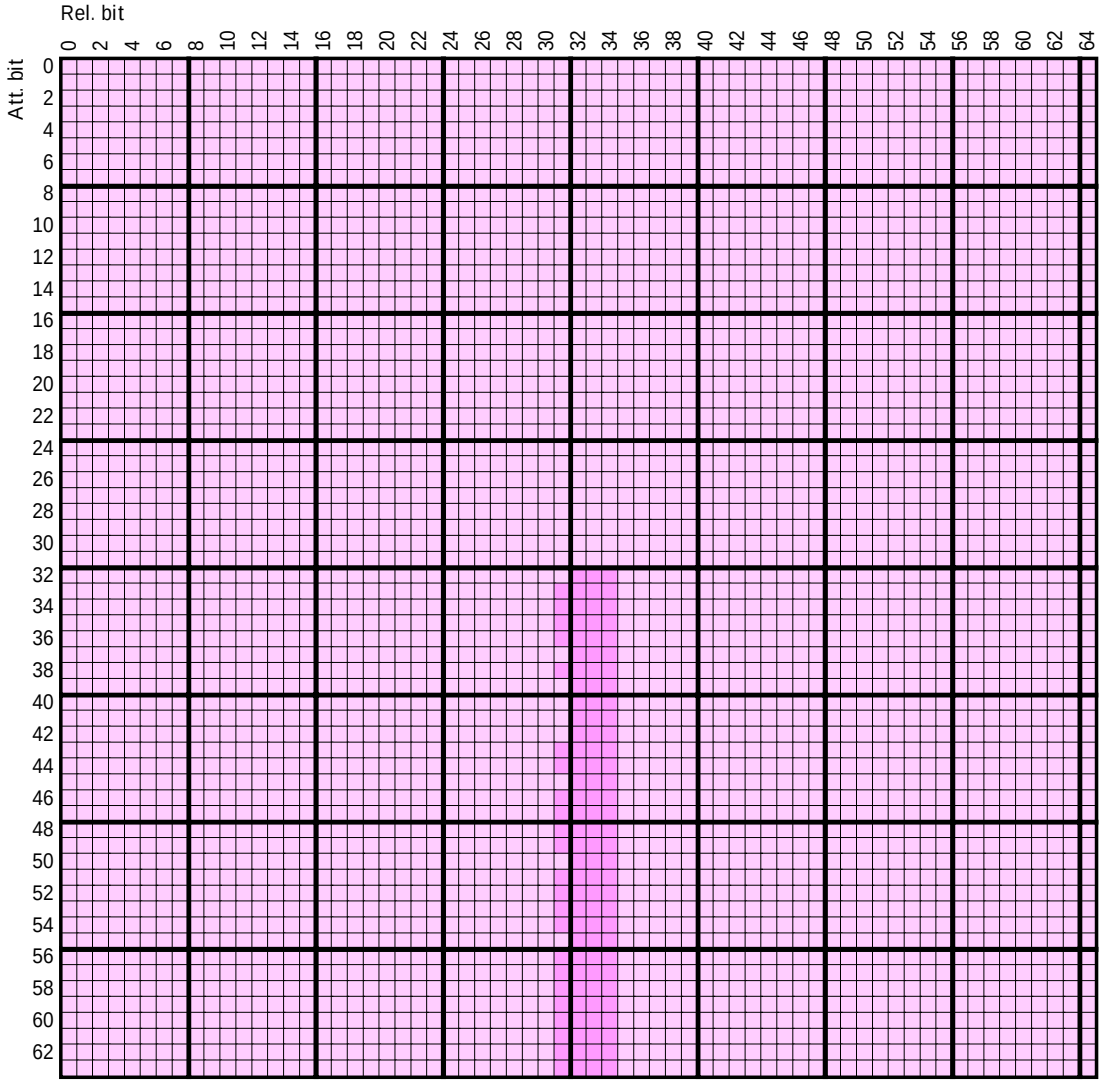


図 B.3.2 HiL1 ﾗｳﾝﾄﾞ関数　拡大鍵と出力の相関(Hw=1) AVA



※ﾃﾞｰﾀ件数が他に比べて 1/4 である。同一のｽｹｰﾙで比較するために推測値として評価値を 4 倍した。

図 B.3.3 HiL1 ﾗｳﾝﾄﾞ関数　入力と出力の相関(Hw=1) AVD

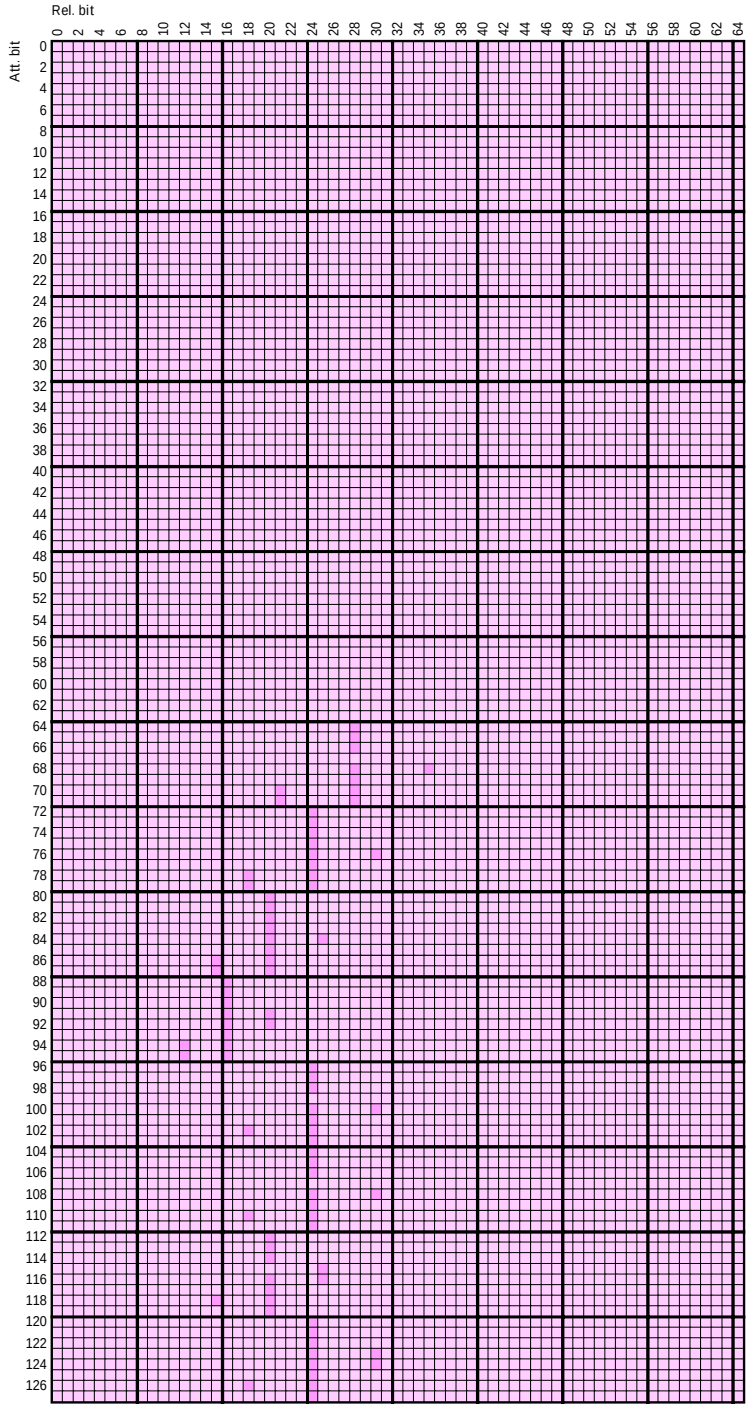


図 B.3.4 HiL1 ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1)　AVD

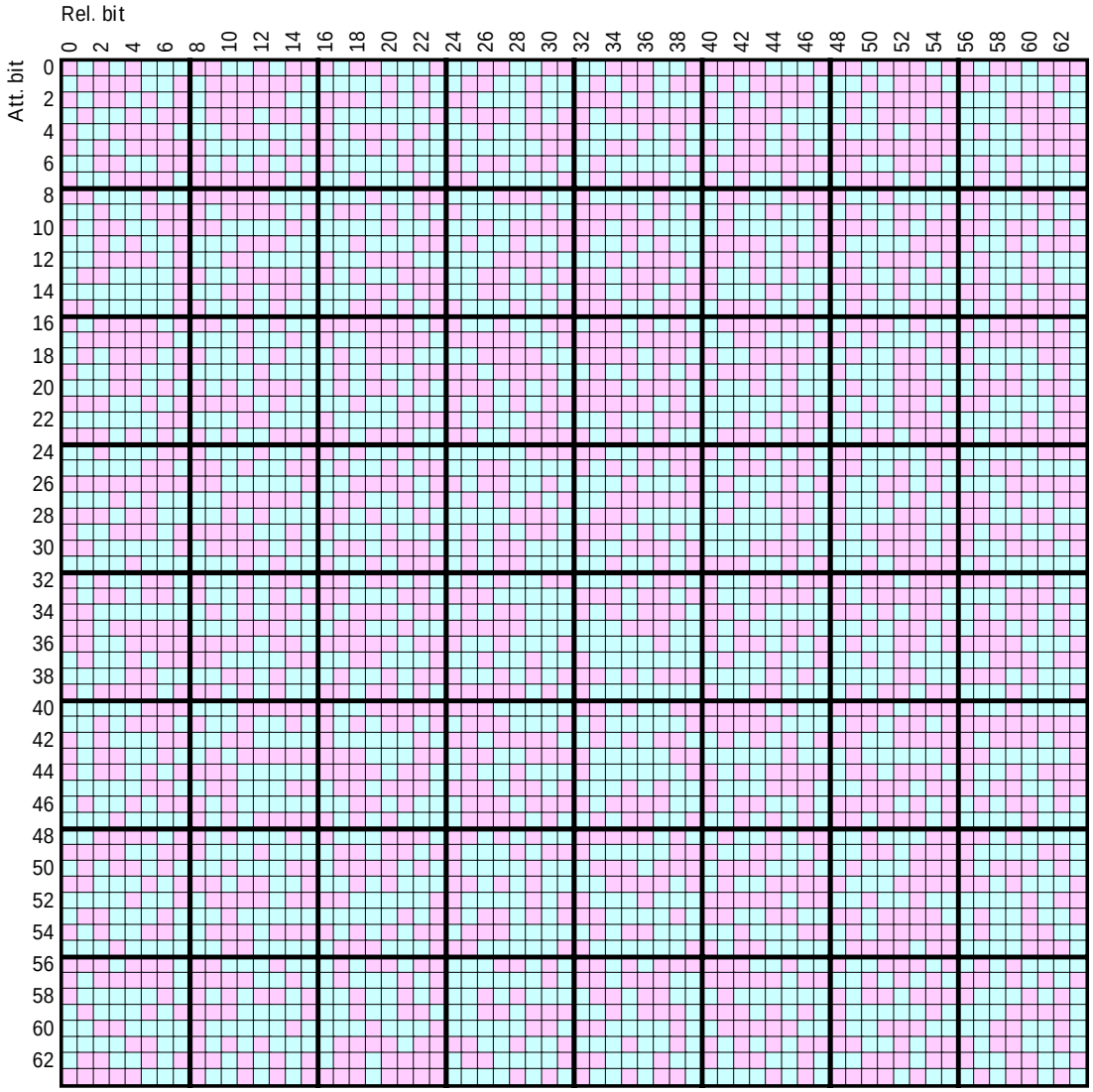


図 B.3.5 HiL1 ﾃﾞｰﾀ攪拌部 段数経過(Hw=1) R4　AVA

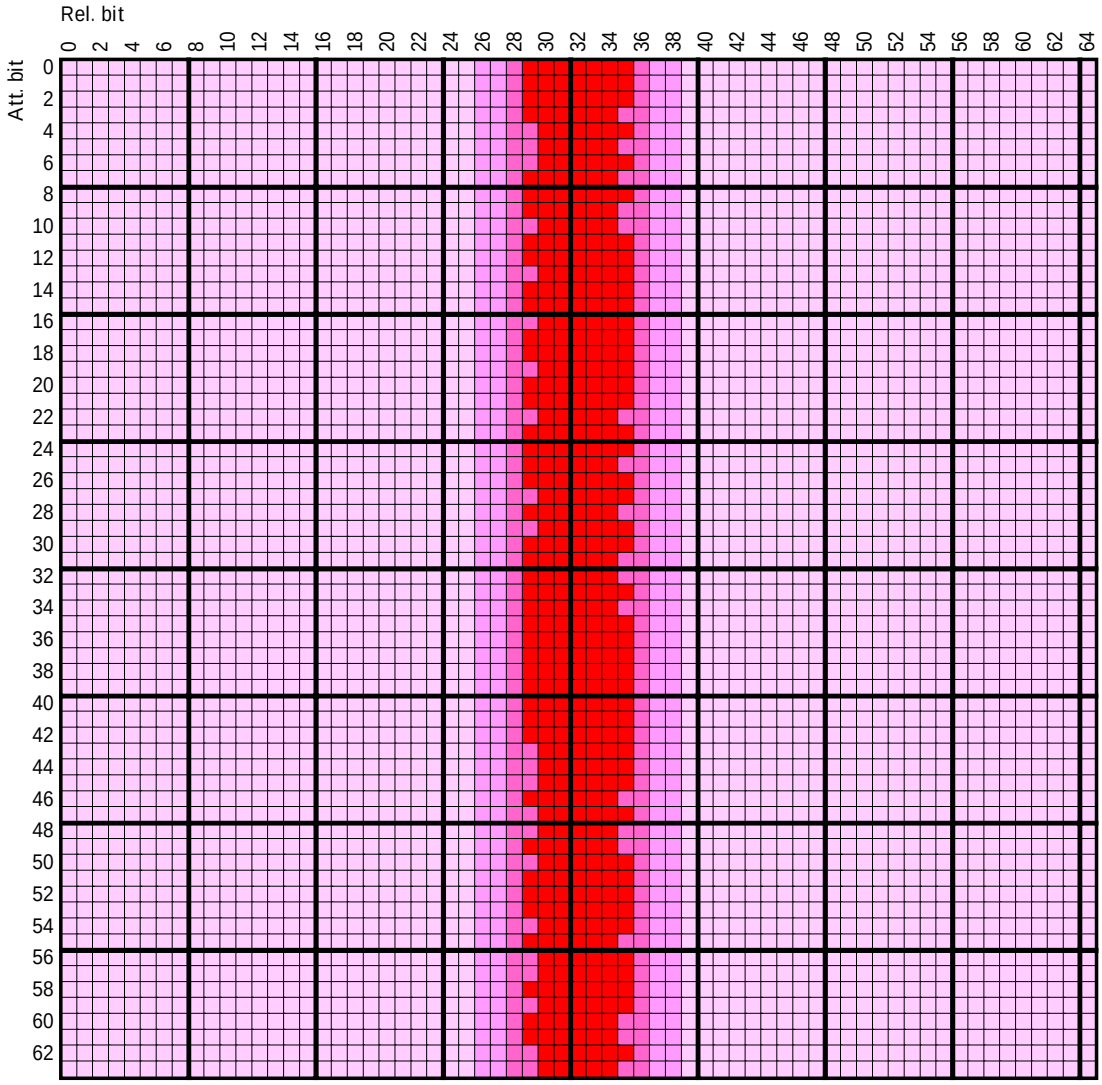


図 B.3.6 HiL1 ﾃﾞｰﾀ攪拌部 段数経過(Hw=1) R4　AVD

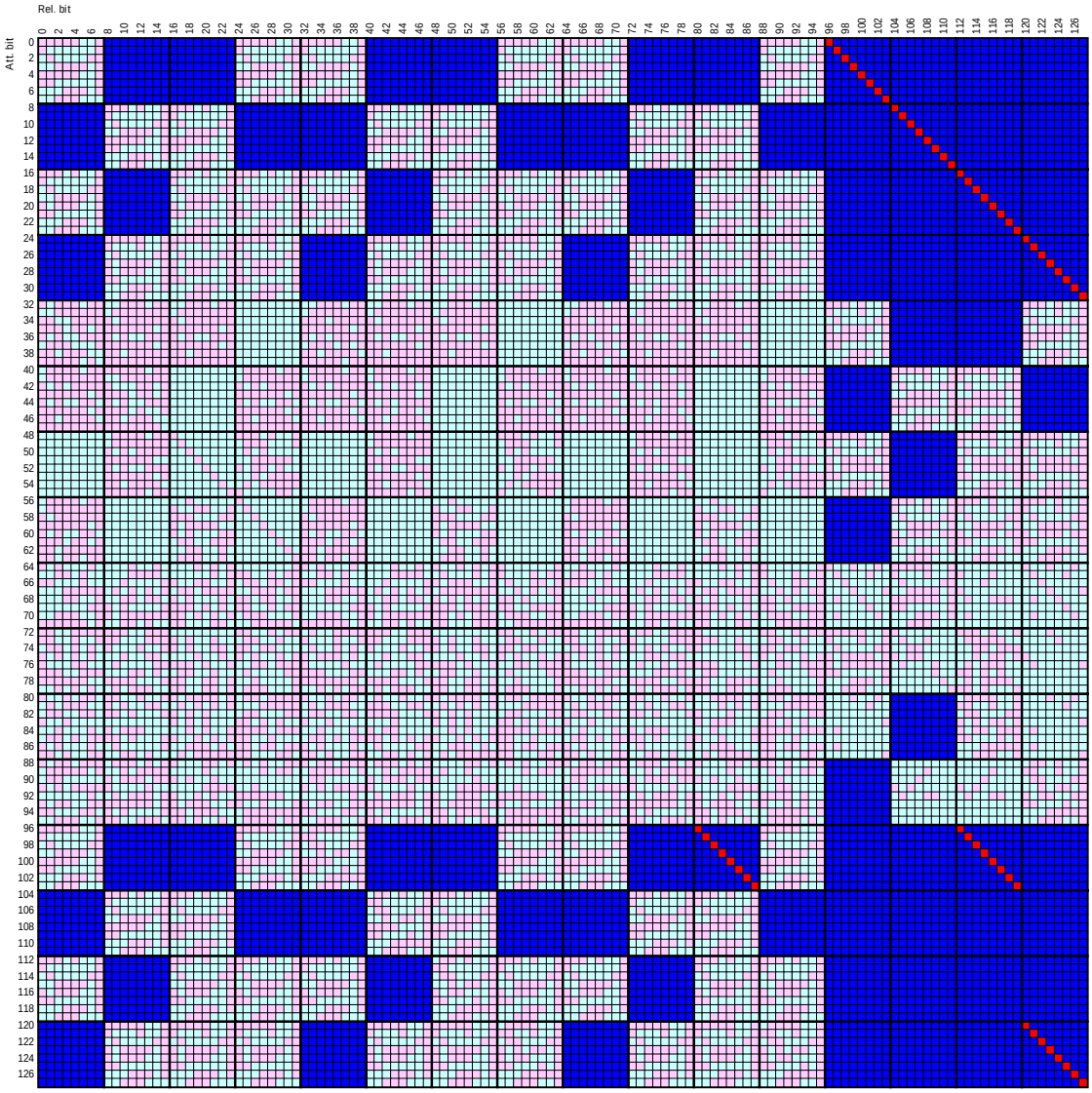
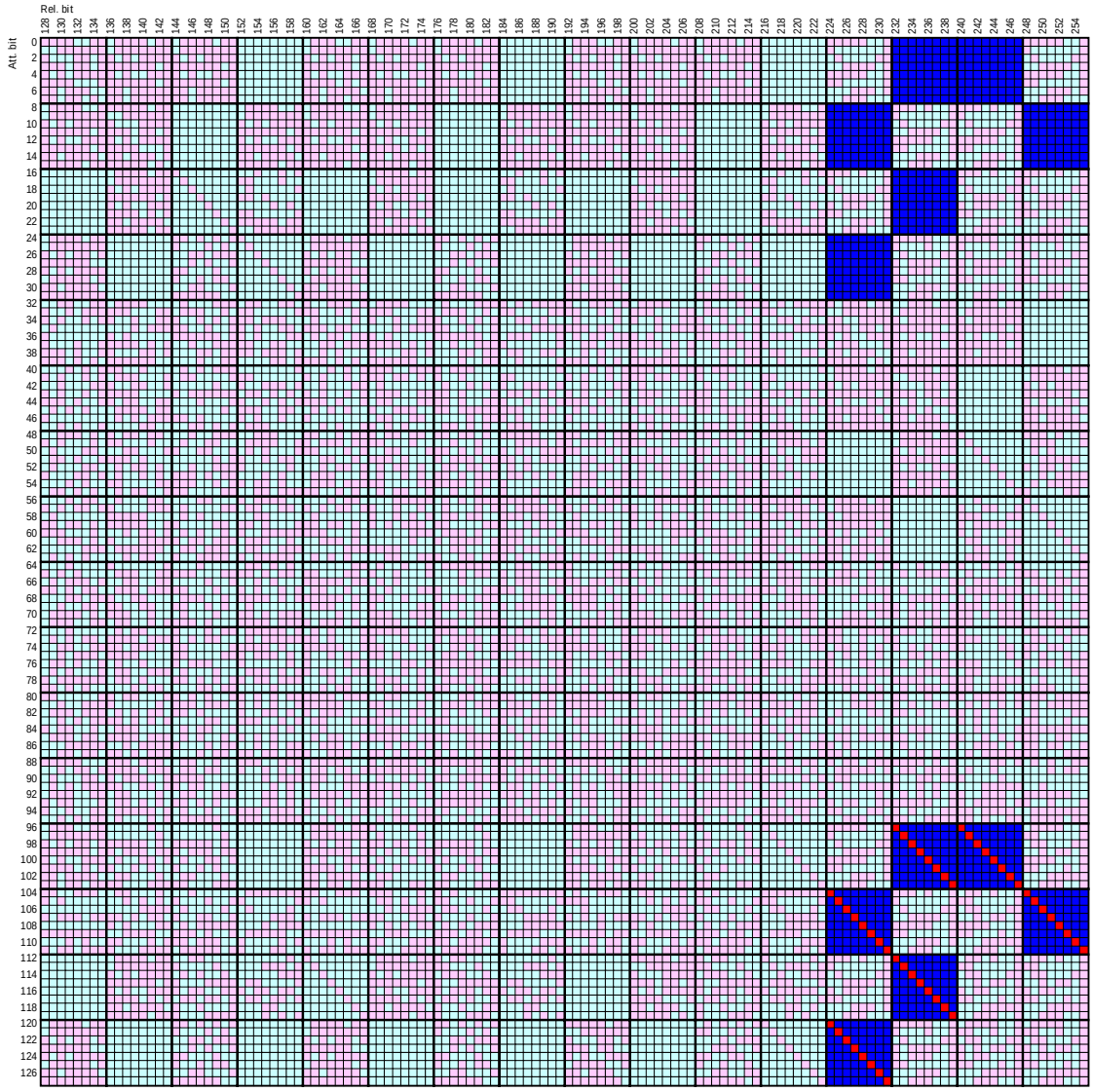


図 B.3.7 HiL1 鍵ｽｹｼﾞｭｰﾗ 秘密鍵と拡大鍵の相関(Hw=1) AVA(1/2)



※拡大鍵長が 256bit を越えるため、拡大鍵の上位 256bit のみを
グラフ表示している。

図 B.3.8 HiL1 鍵ｽｹｼﾞｭｰﾗ 秘密鍵と拡大鍵の相関(Hw=1) AVA(2/2)

B 結果グラフ

B.4 MISTY1

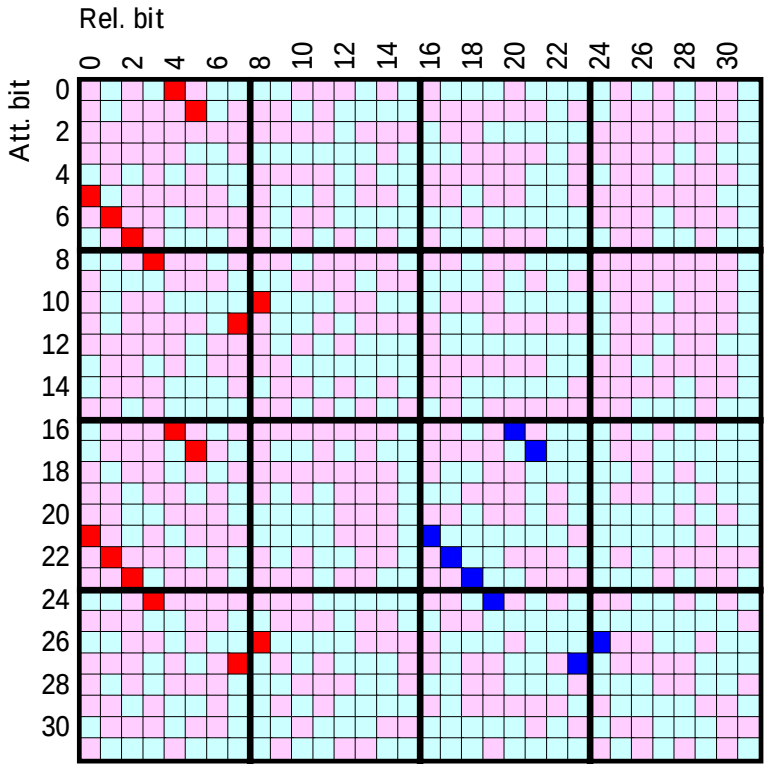


図 B.4.1 MIST ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVA

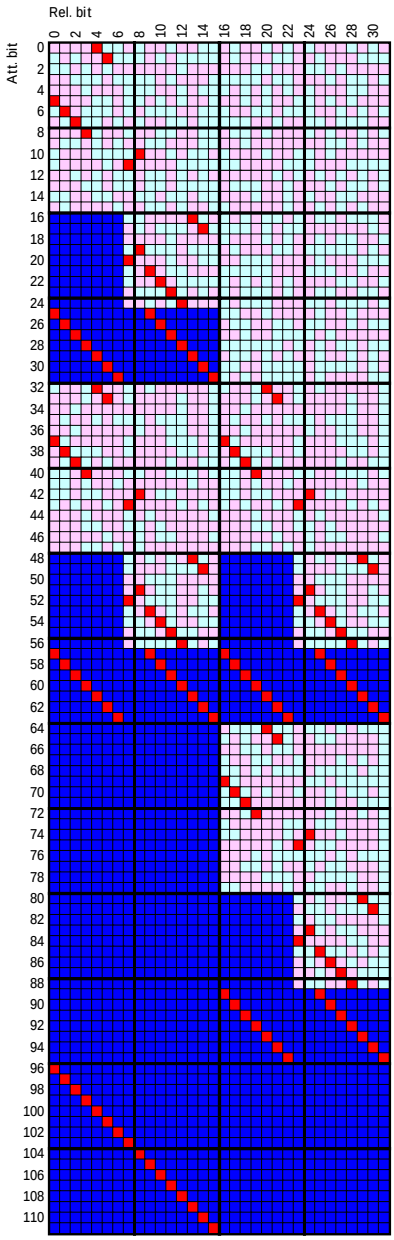


図 B.4.2 MIST ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVA

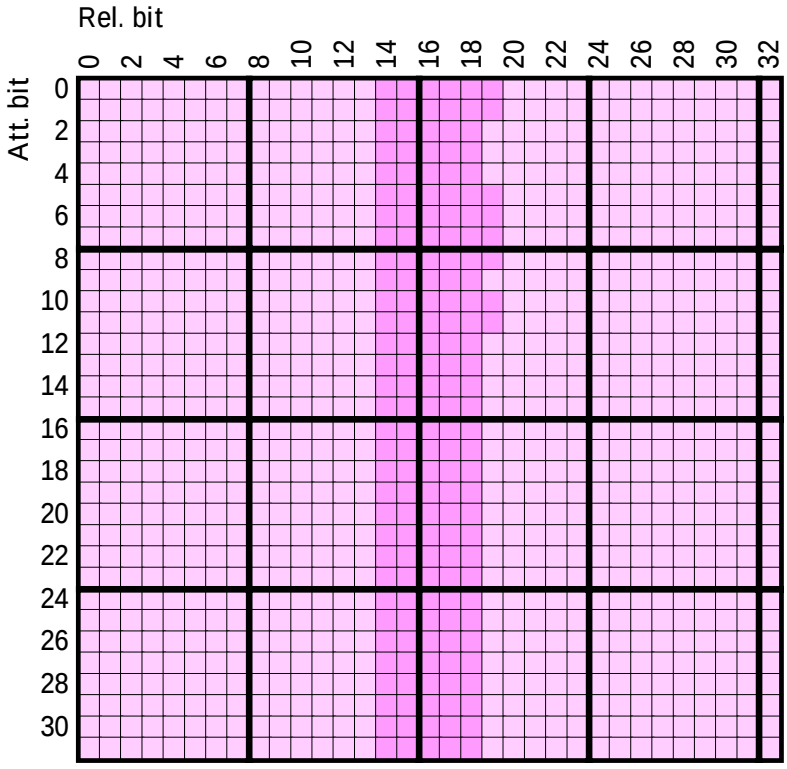


図 B.4.3 MIST ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVD

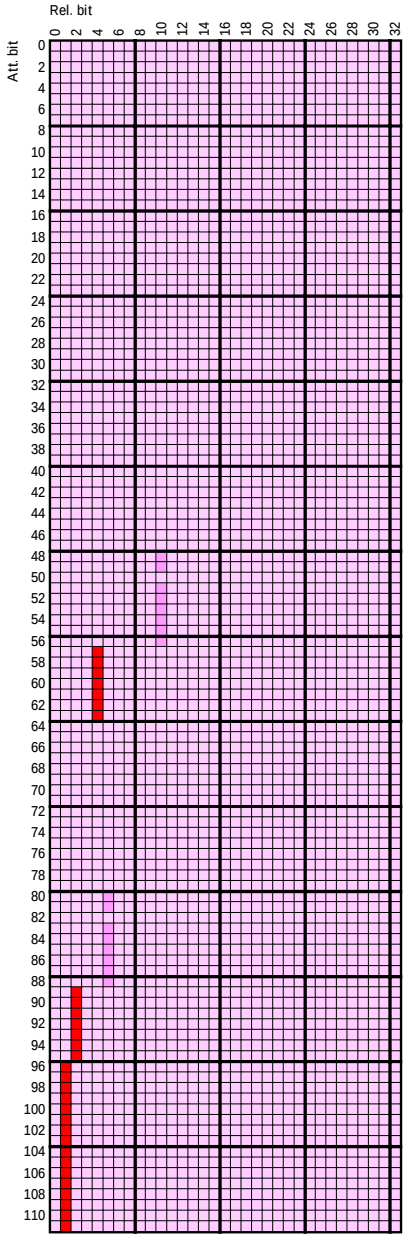


図 B.4.4 MIST ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVD

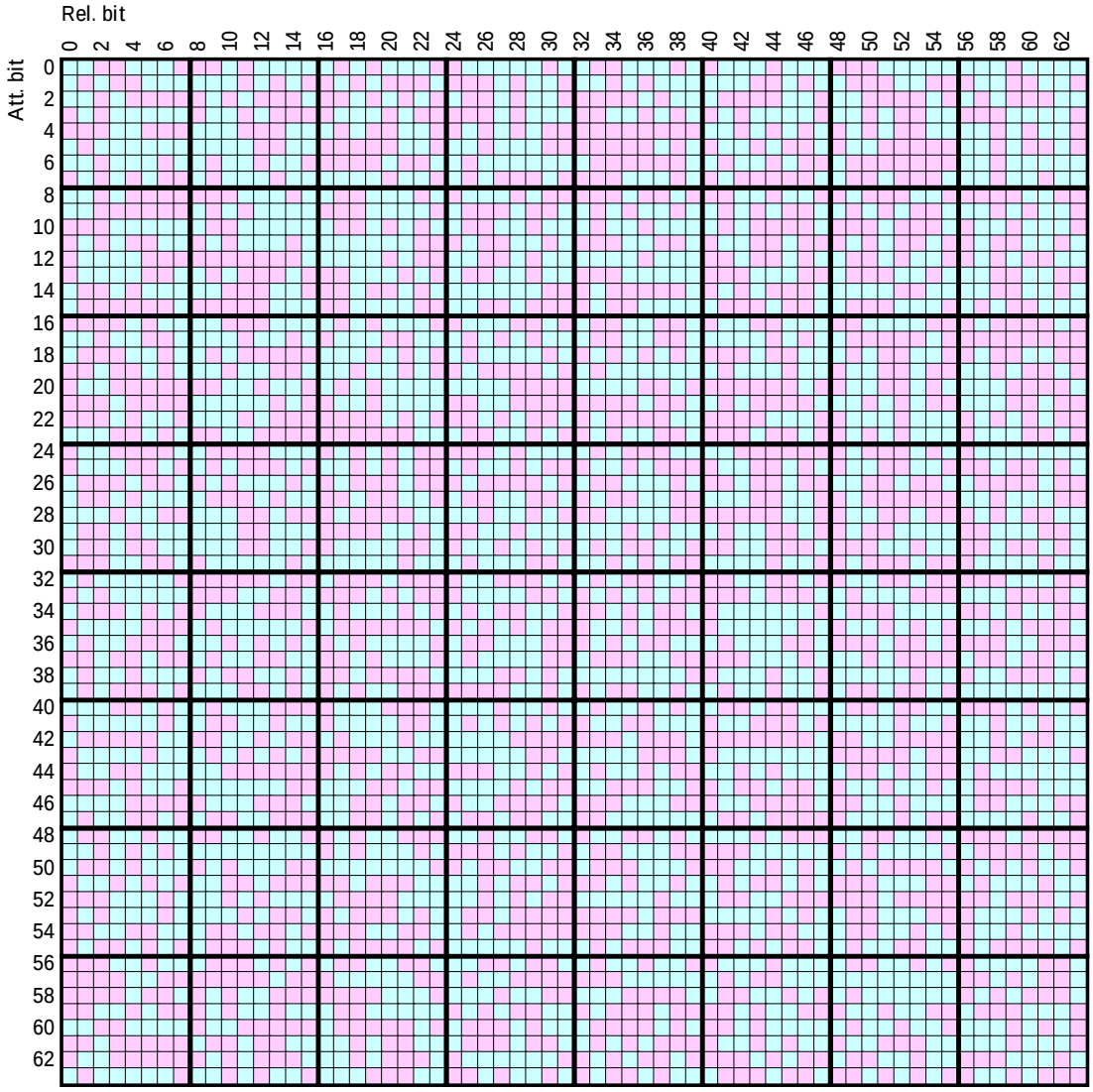


図 B.4.5 MIST ﾃﾞｰﾀ攪拌部 段数経過(Hw=1) R4 AVA

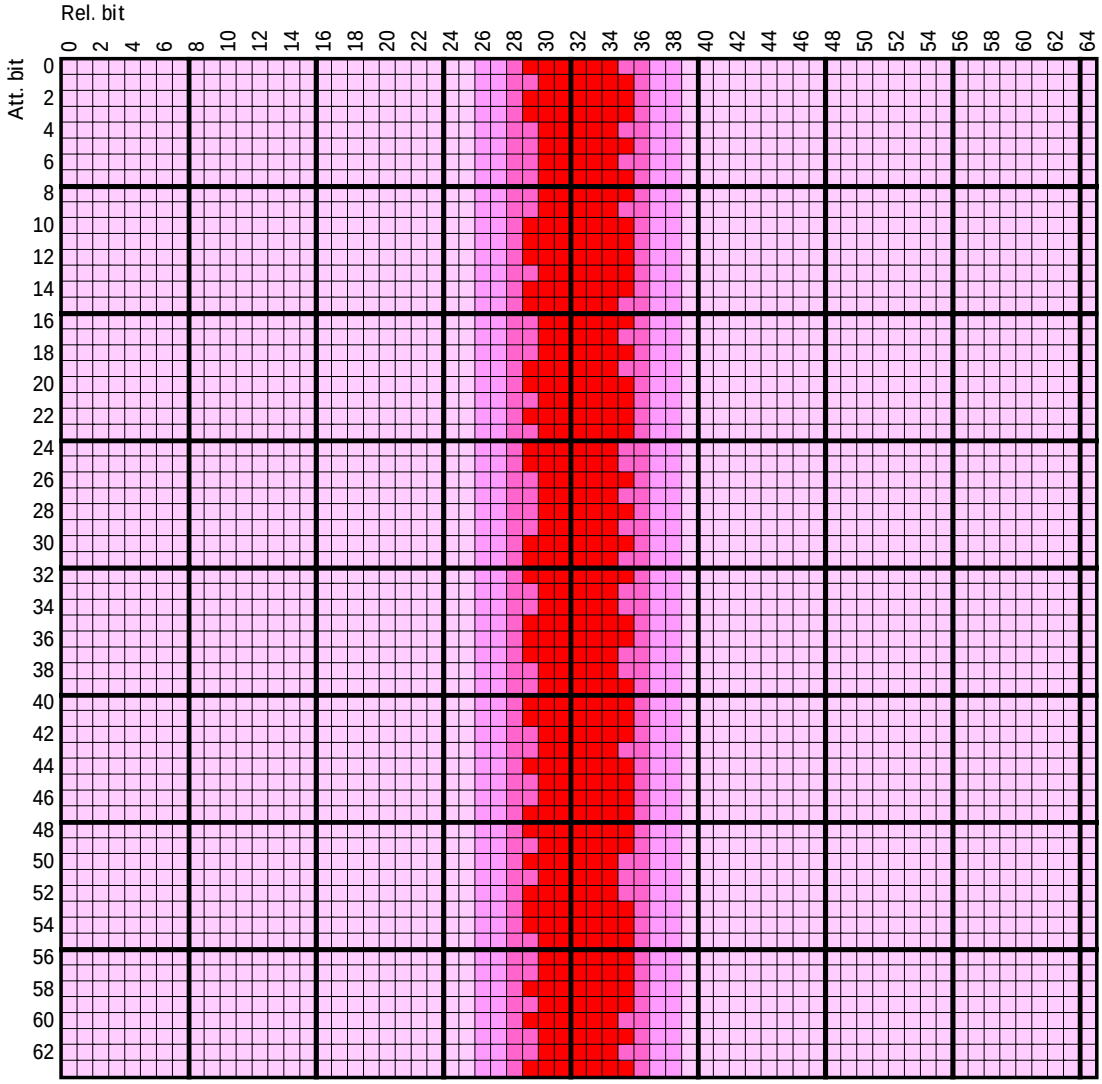


図 B.4.6 MIST ﾃﾞｰﾀ攪拌部 段数経過(Hw=1) R4 AVD

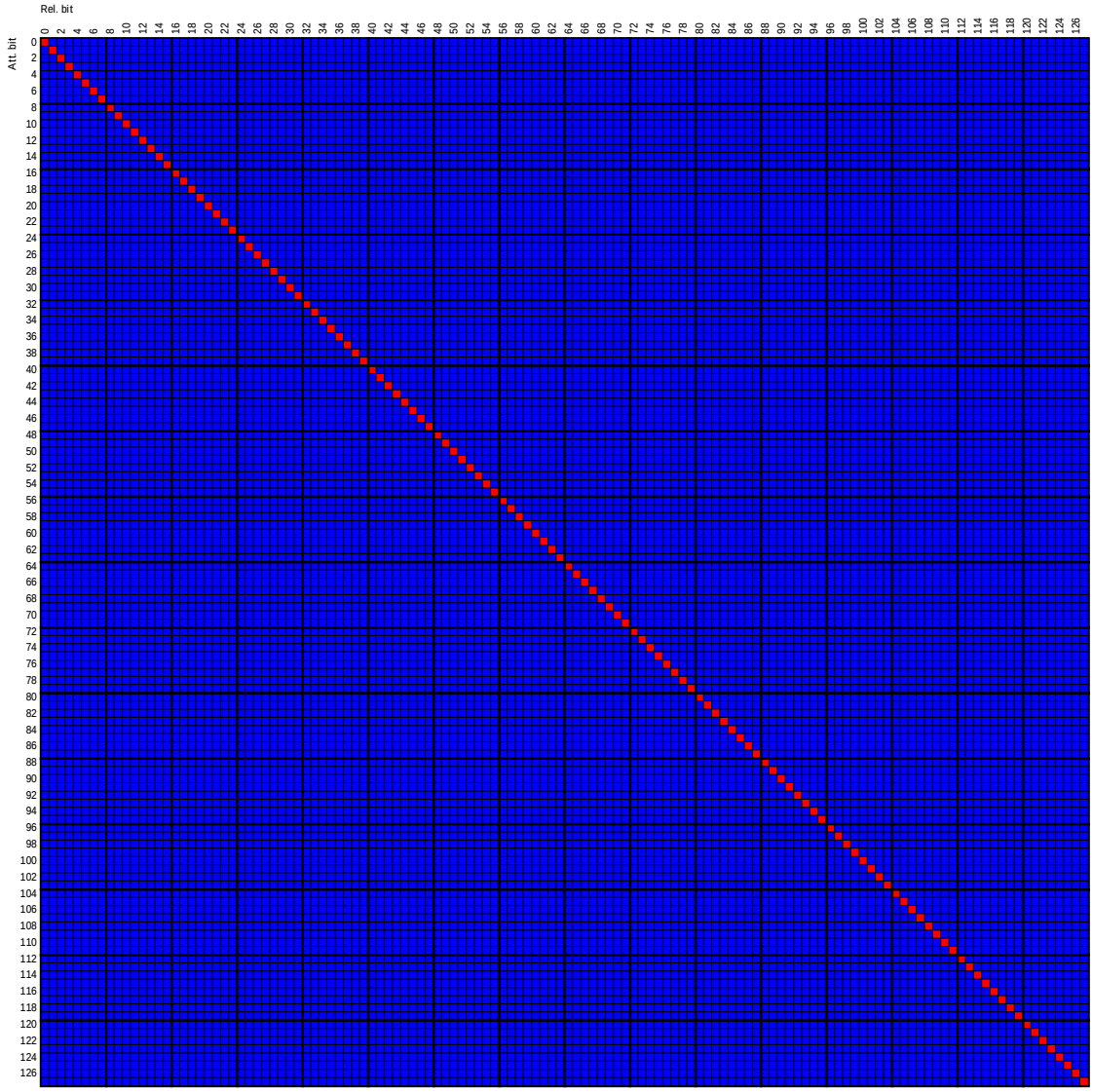
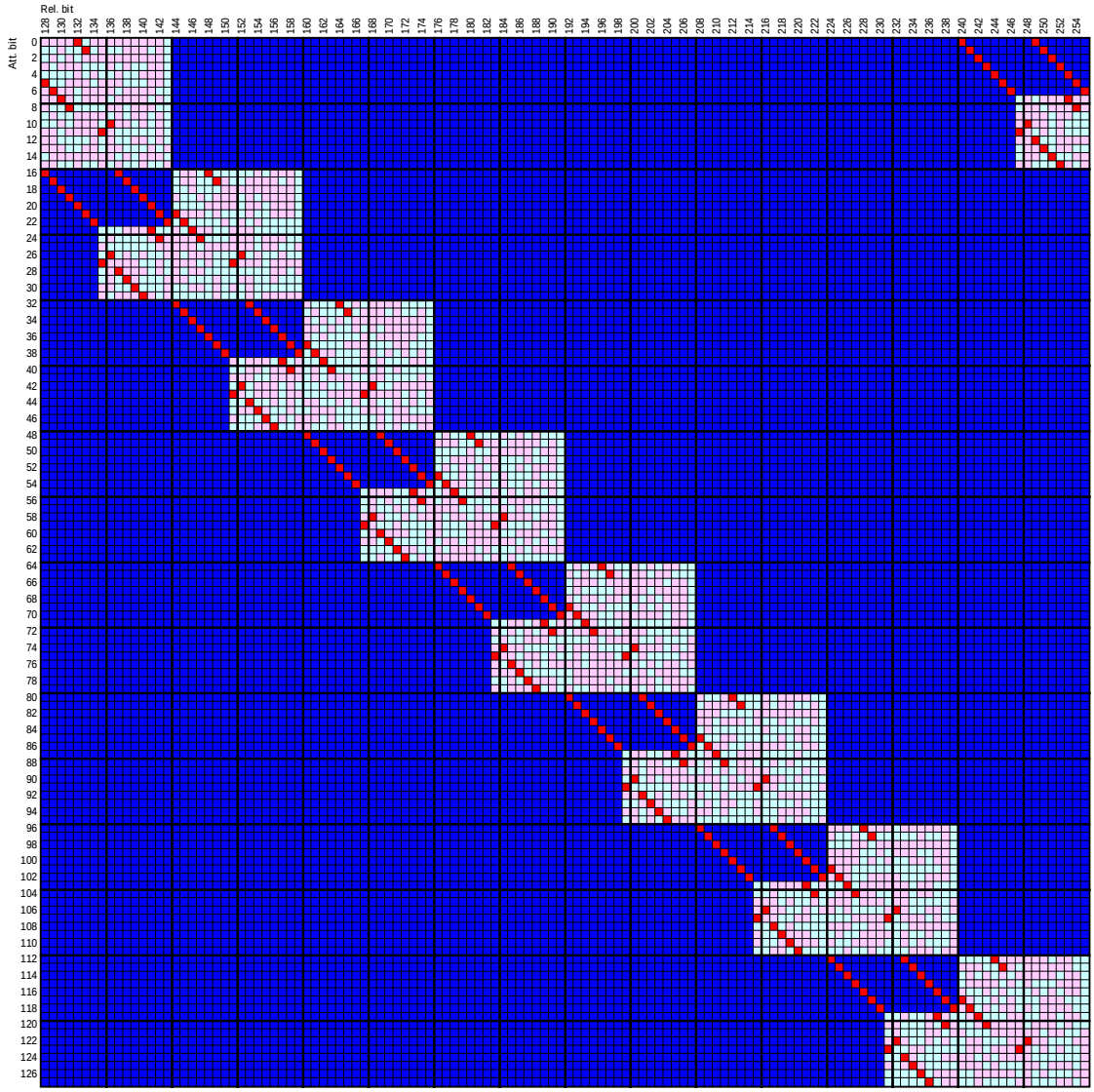


図 B.4.7 MIST 鍵ｽｹｼﾞｭｰﾗ 秘密鍵と拡大鍵の相関(Hw=1) AVA(1/2)



※拡大鍵長が 256bit を越えるため、拡大鍵の上位 256bit のみを
グラフ表示している。

図 B.4.8 MIST 鍵ｽｹｼﾞｭｰﾗ 秘密鍵と拡大鍵の相関(Hw=1) AVA(2/2)

B 結果グラフ

B.5 Camellia

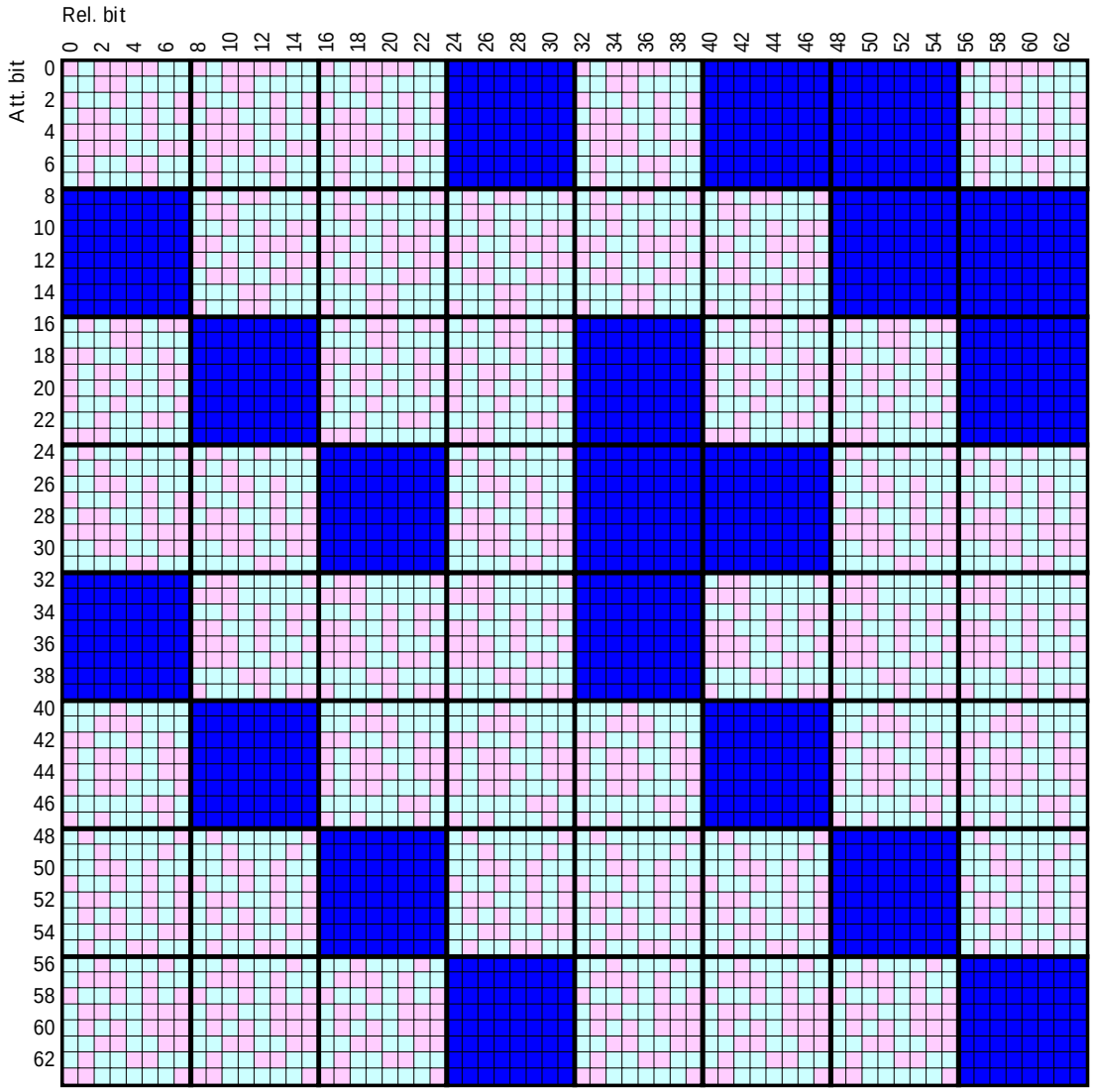


図 B.5.1 Came ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVA

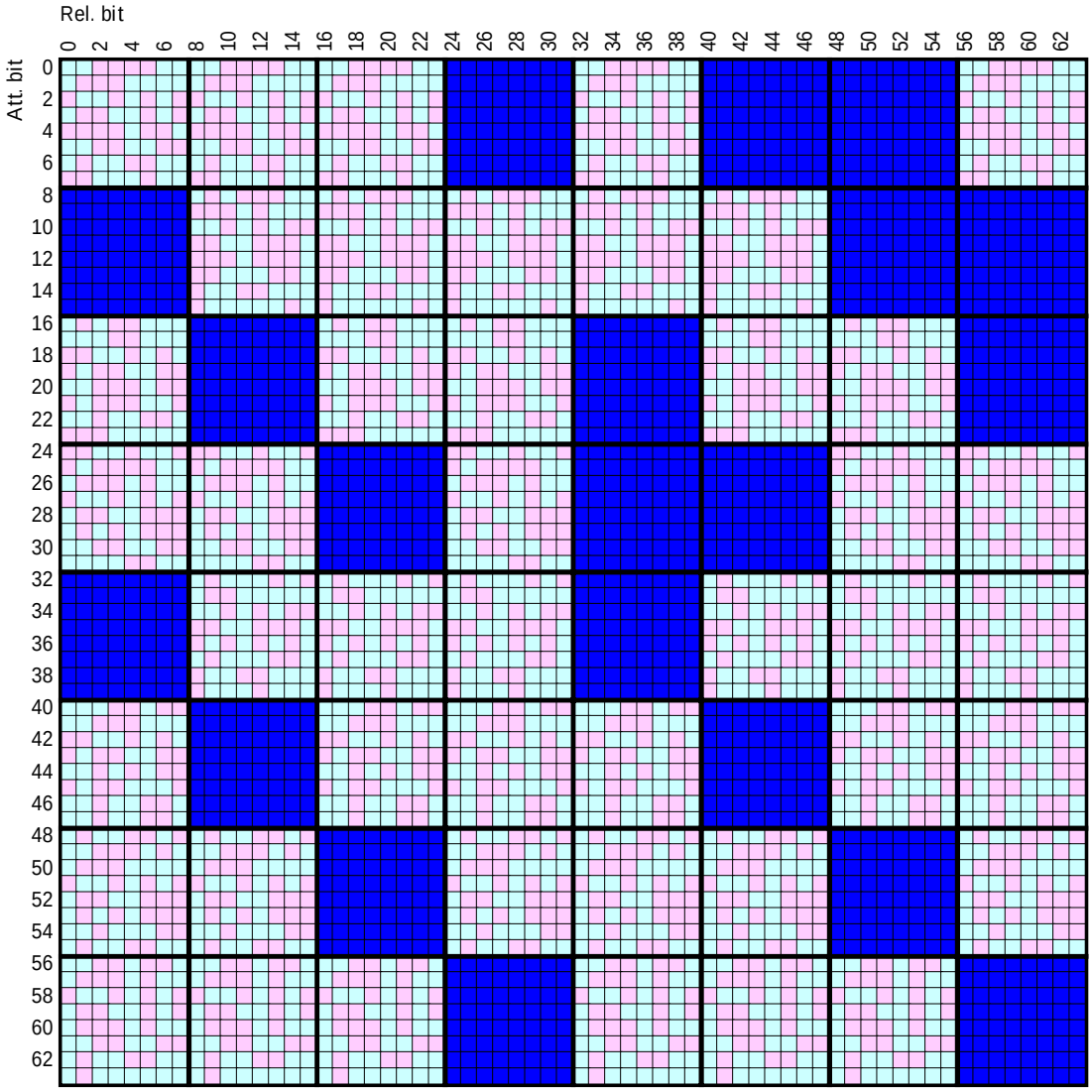


図 B.5.2 Came ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVA

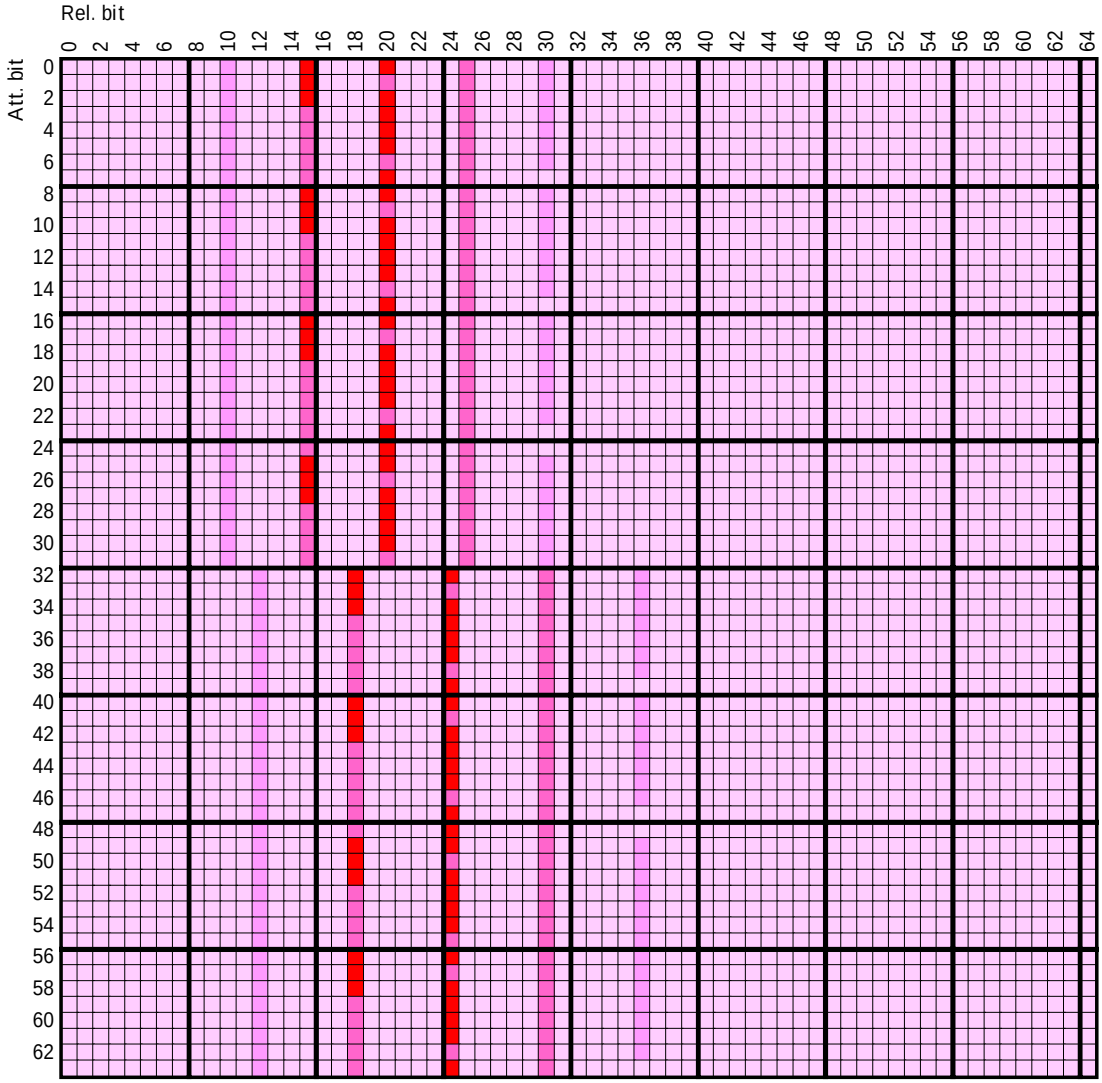


図 B.5.3 Came ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVD

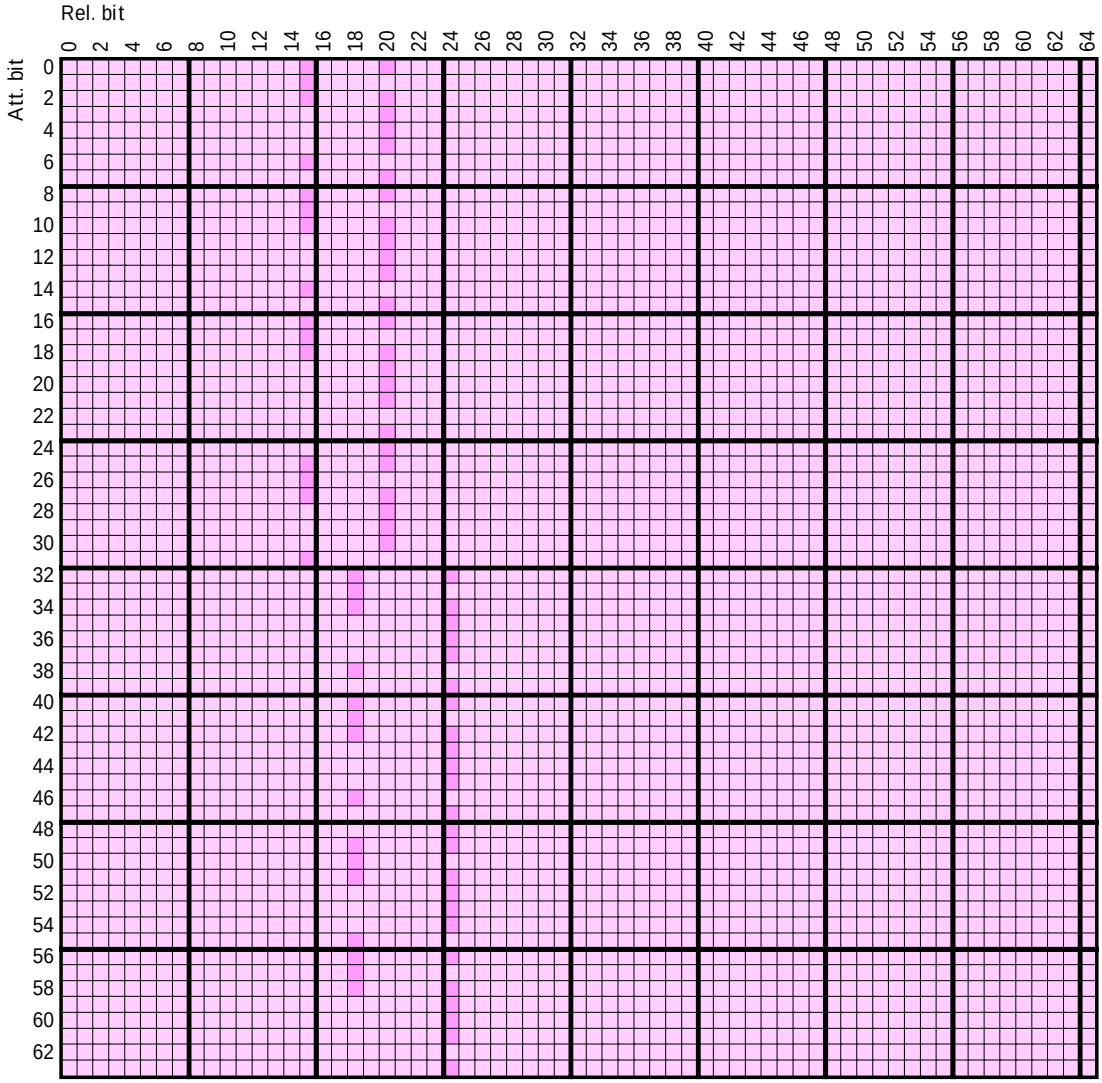


図 B.5.4 Came ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVD

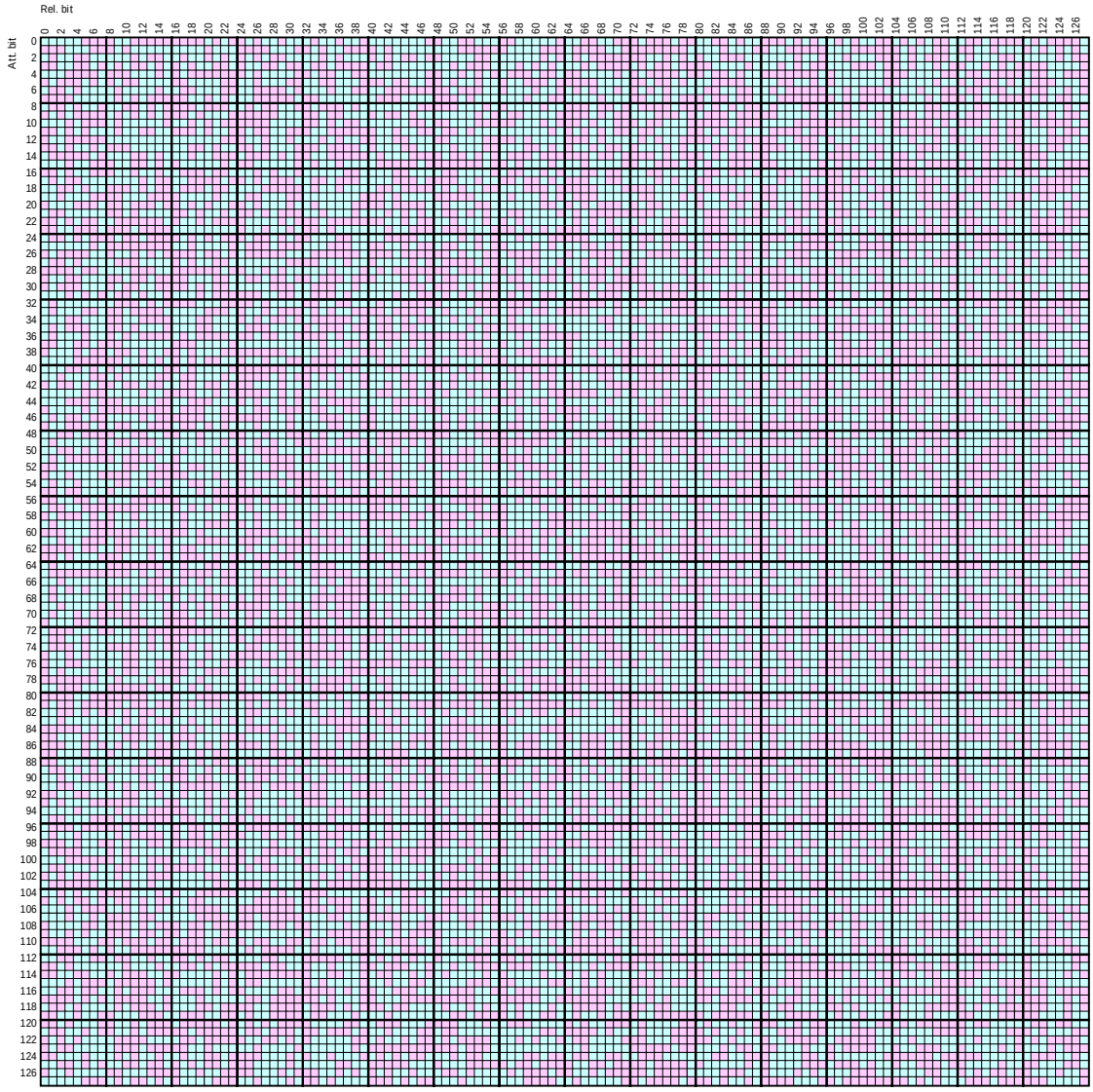


図 B.5.5 Came ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVA

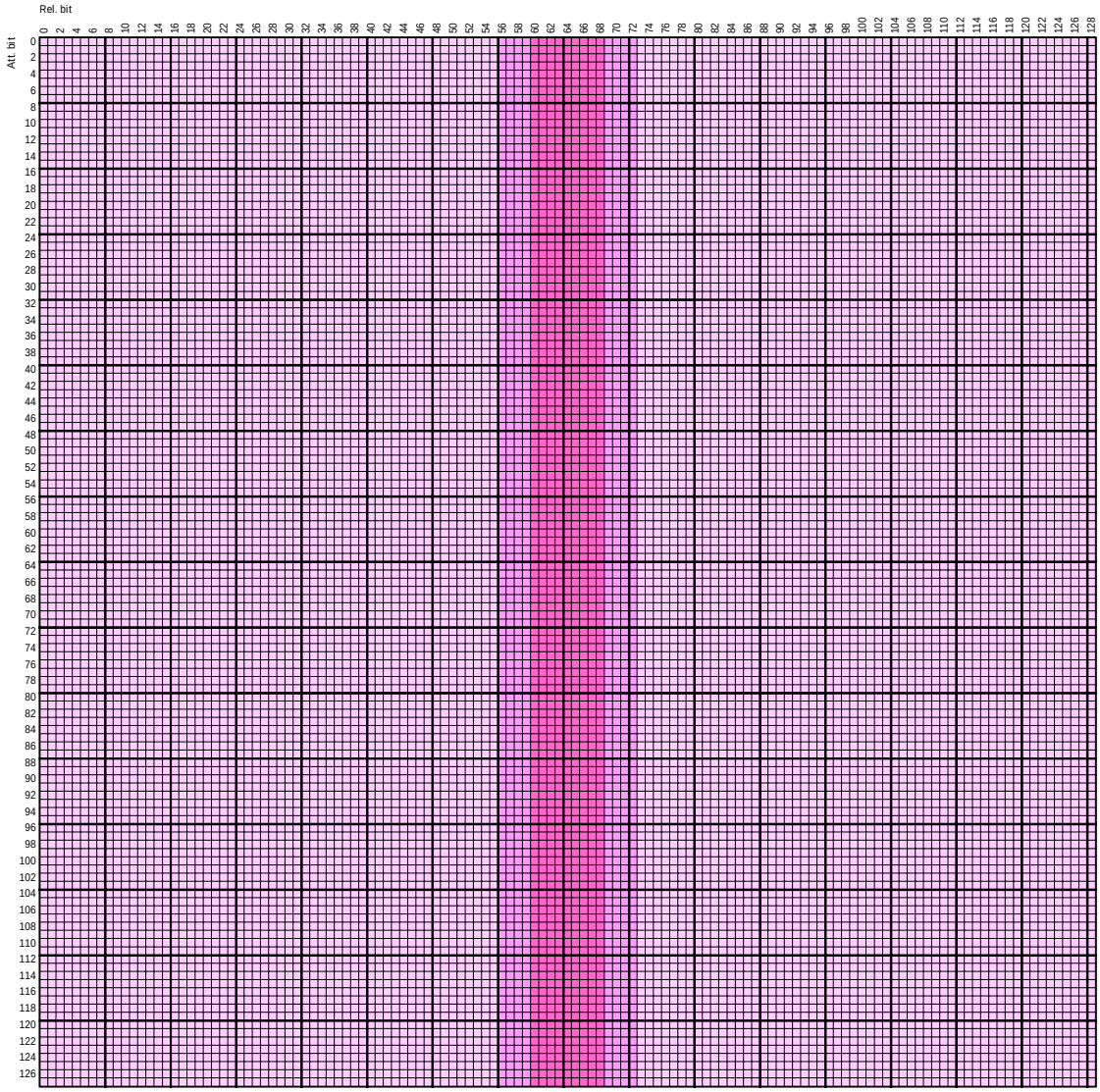


図 B.5.6 Came ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVD

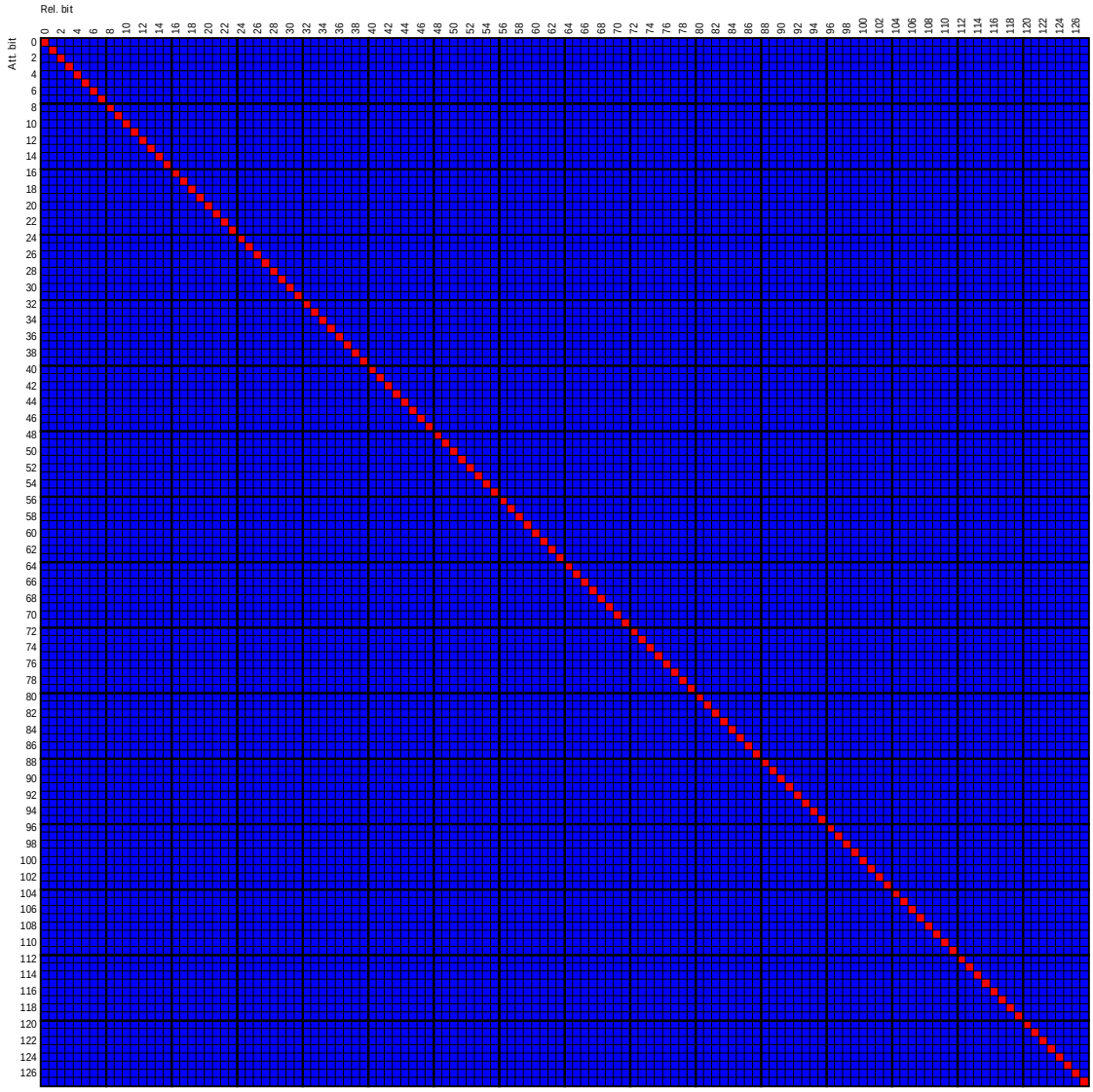
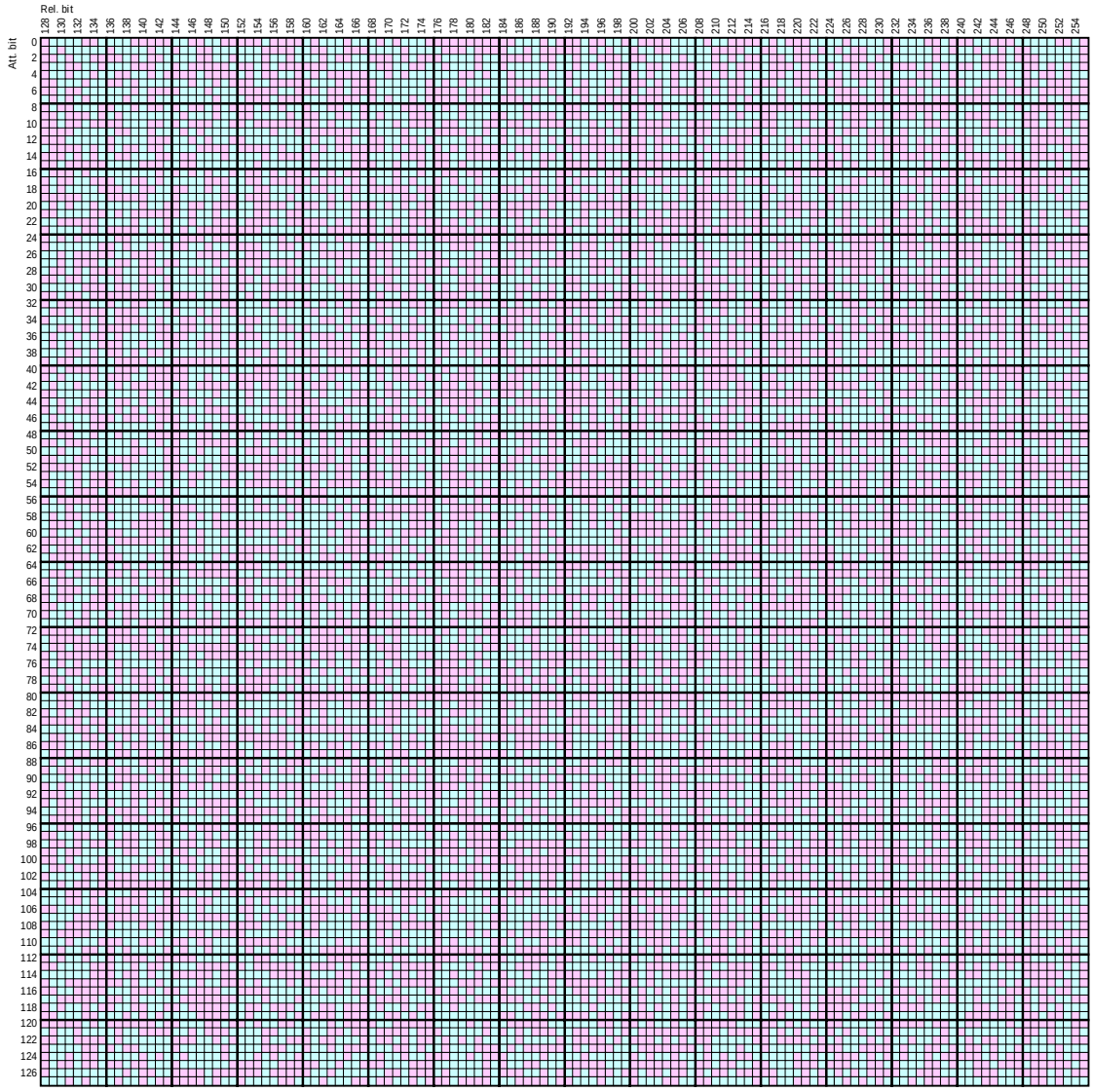


図 B.5.7 Came 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(1/2)



※拡大鍵長が 256bit を越えるため、拡大鍵の上位 256bit のみを
グラフ表示している。

図 B.5.8 Came 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(2/2)

B 結果グラフ
B.6 CIPHERUNICORN-A

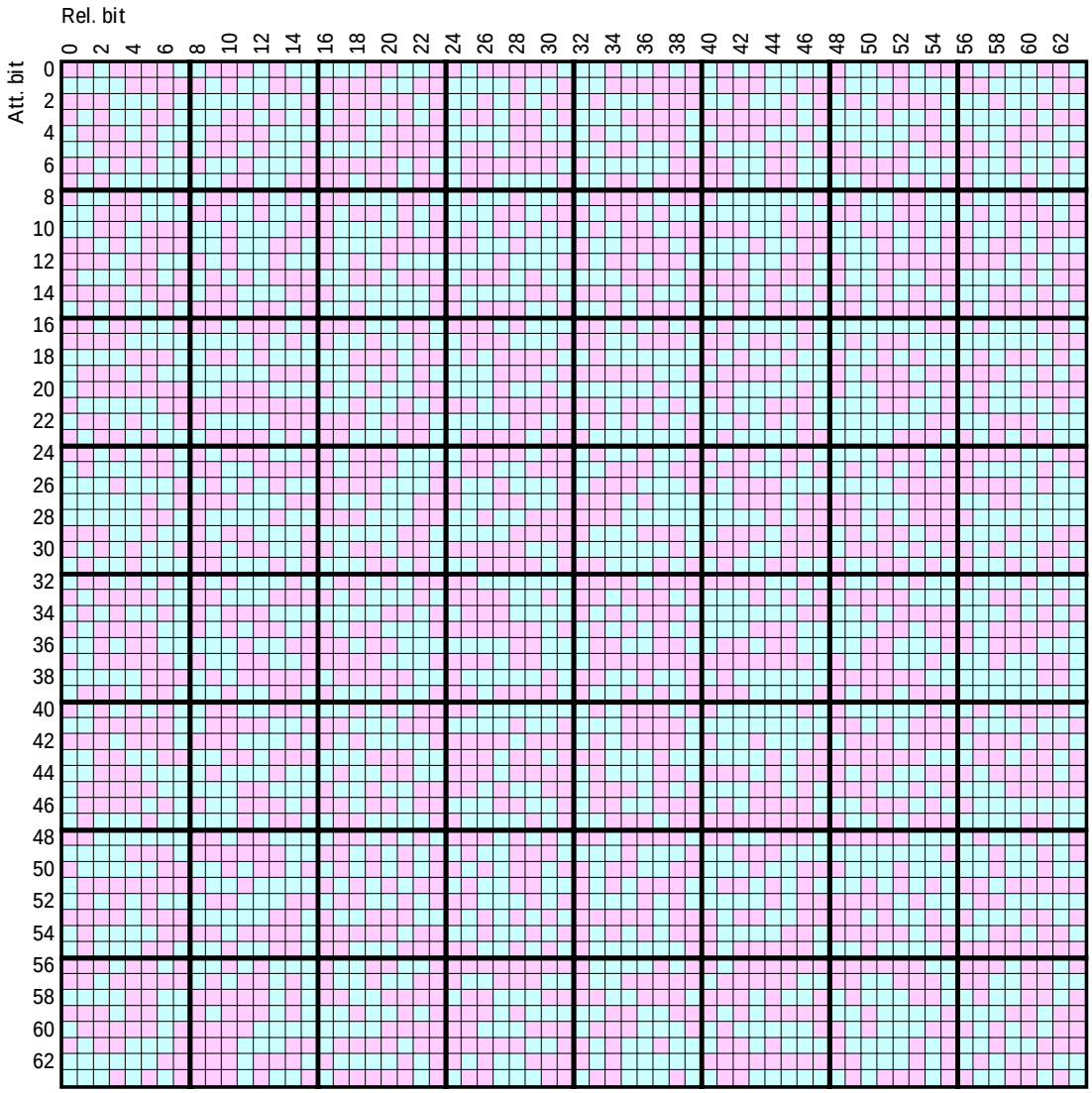


図 B.6.1 UNIA ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVA

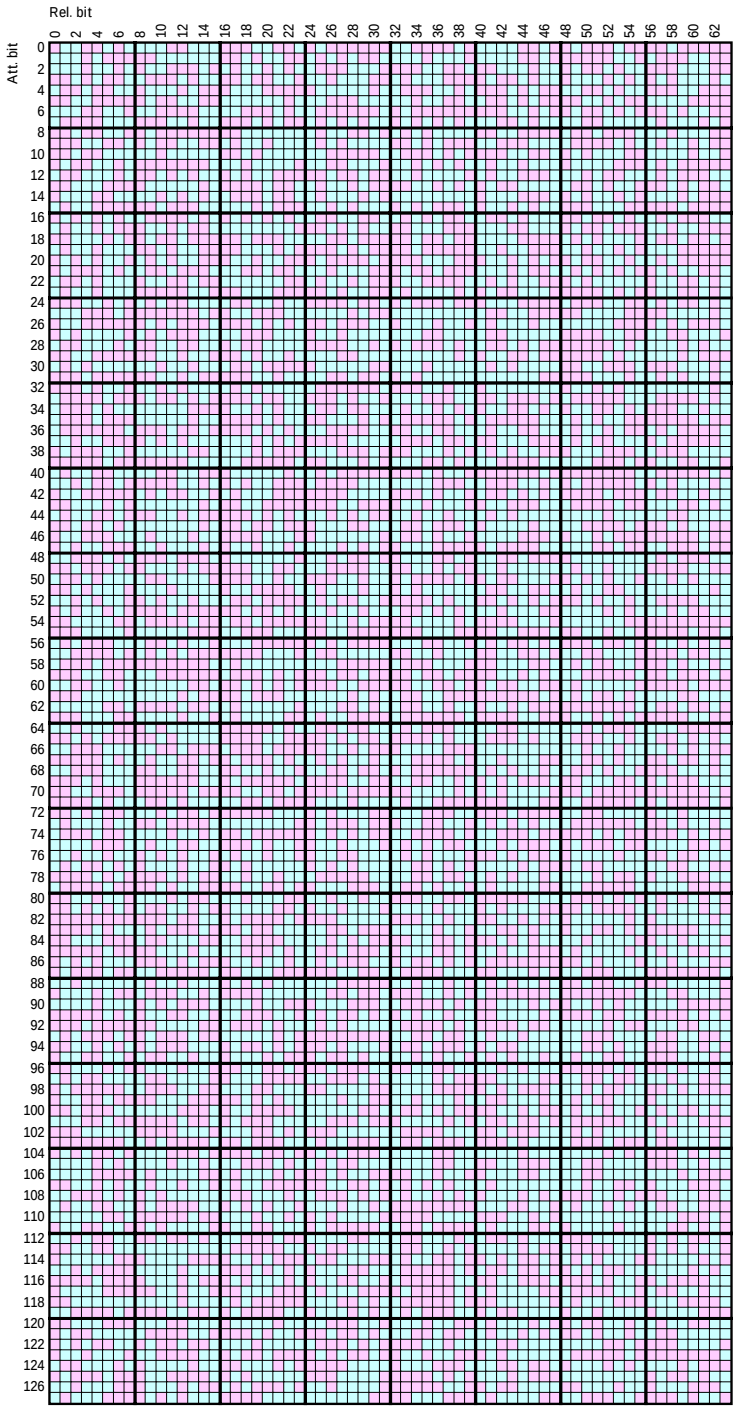


図 B.6.2 UNIA ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVA

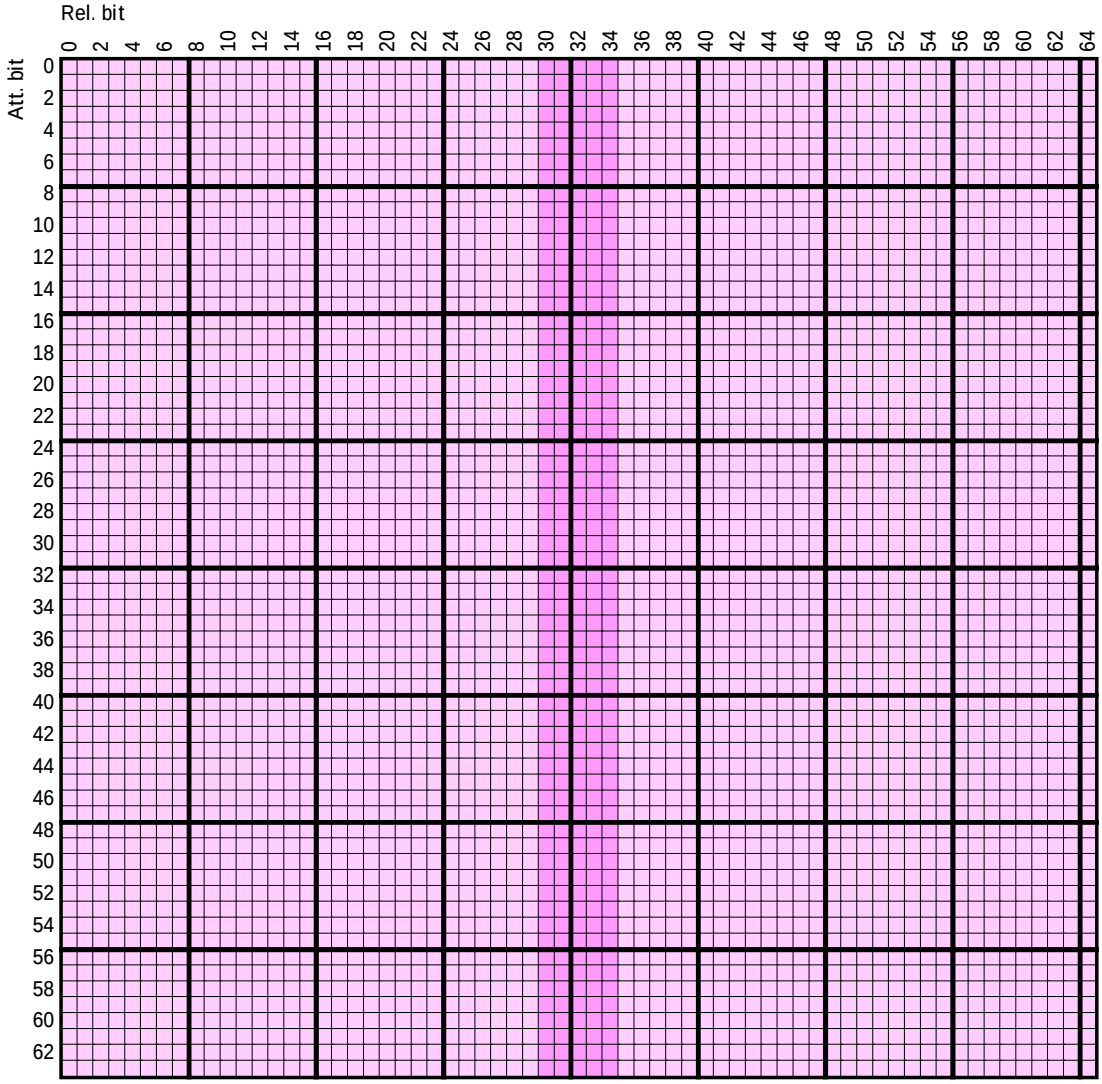


図 B.6.3 UNIA ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVD

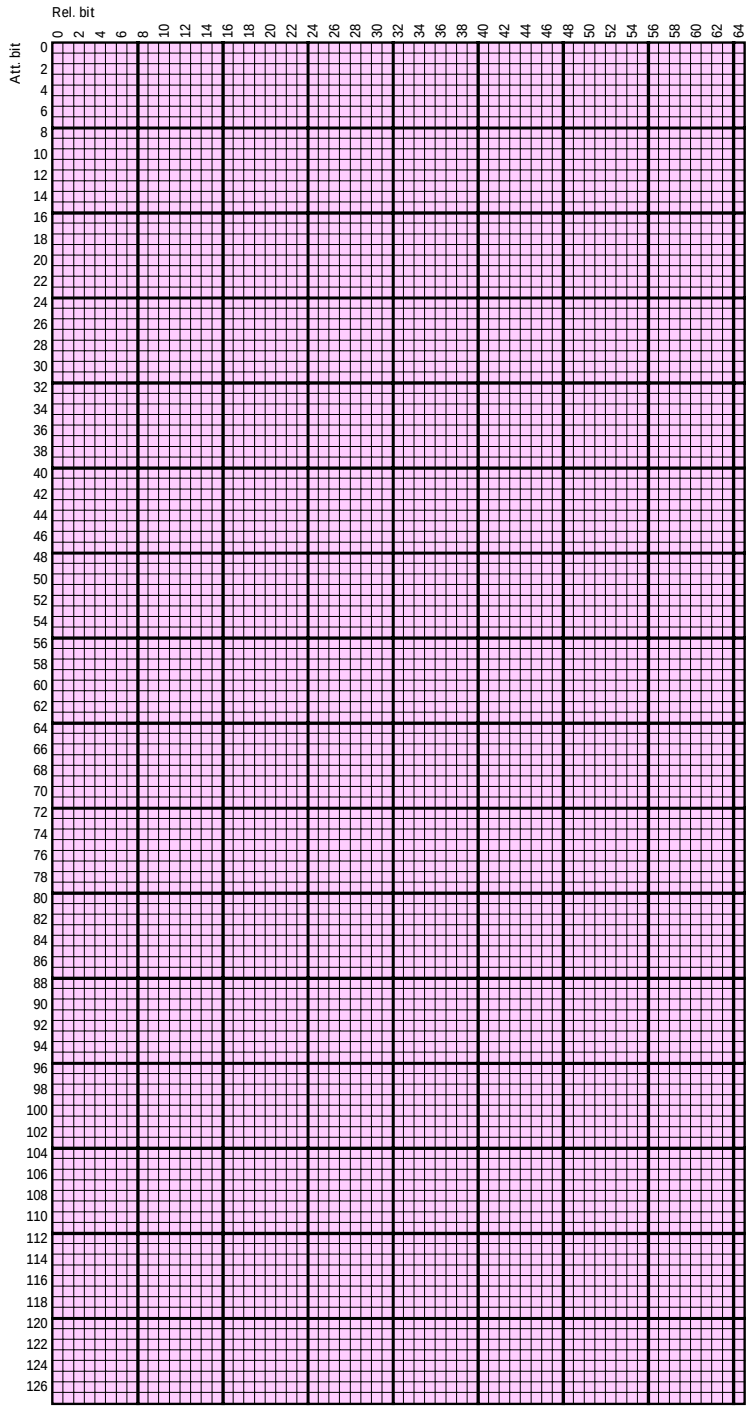


図 B.6.4 UNIA ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVD

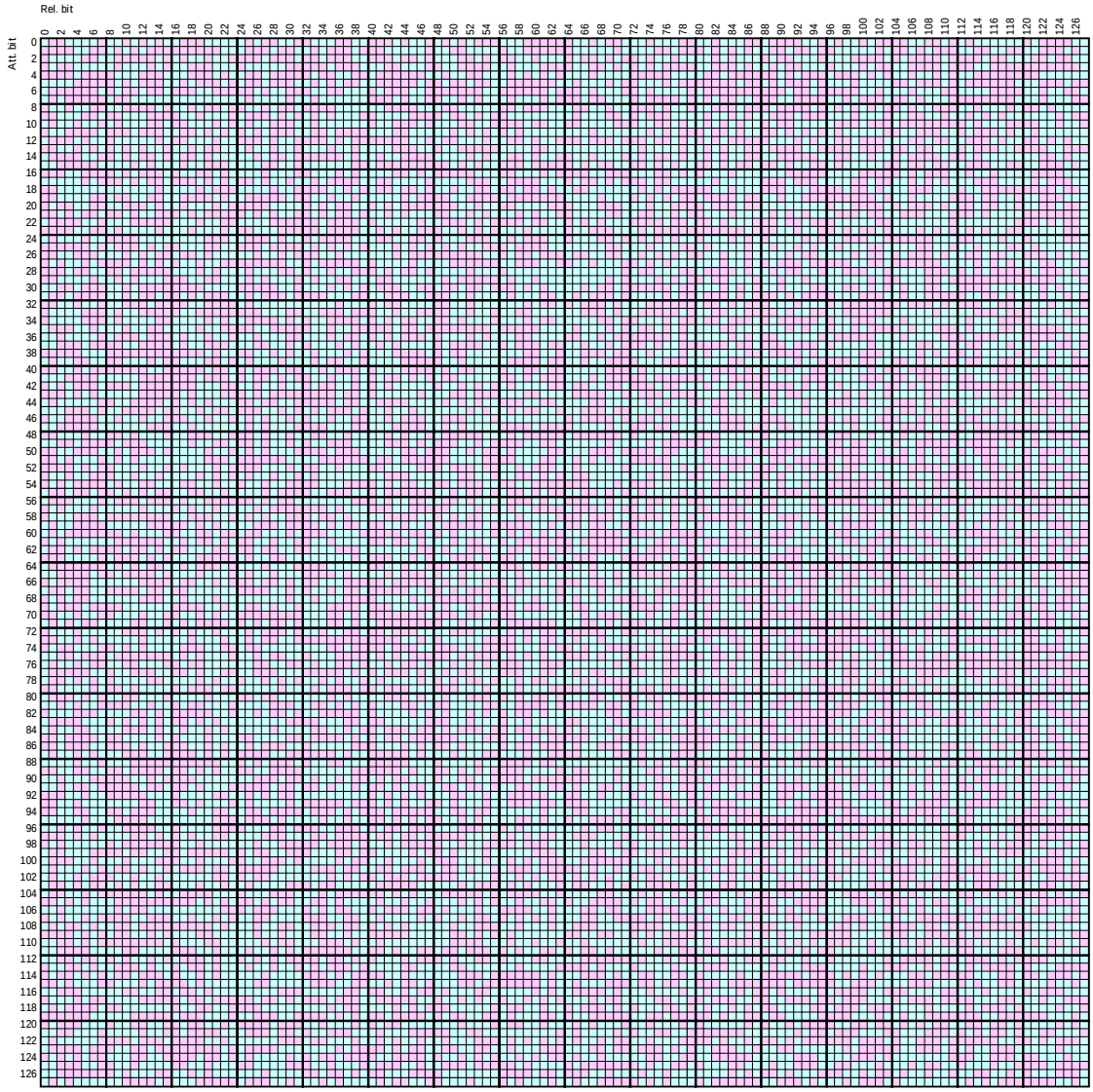


図 B.6.5 UNIA ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVA

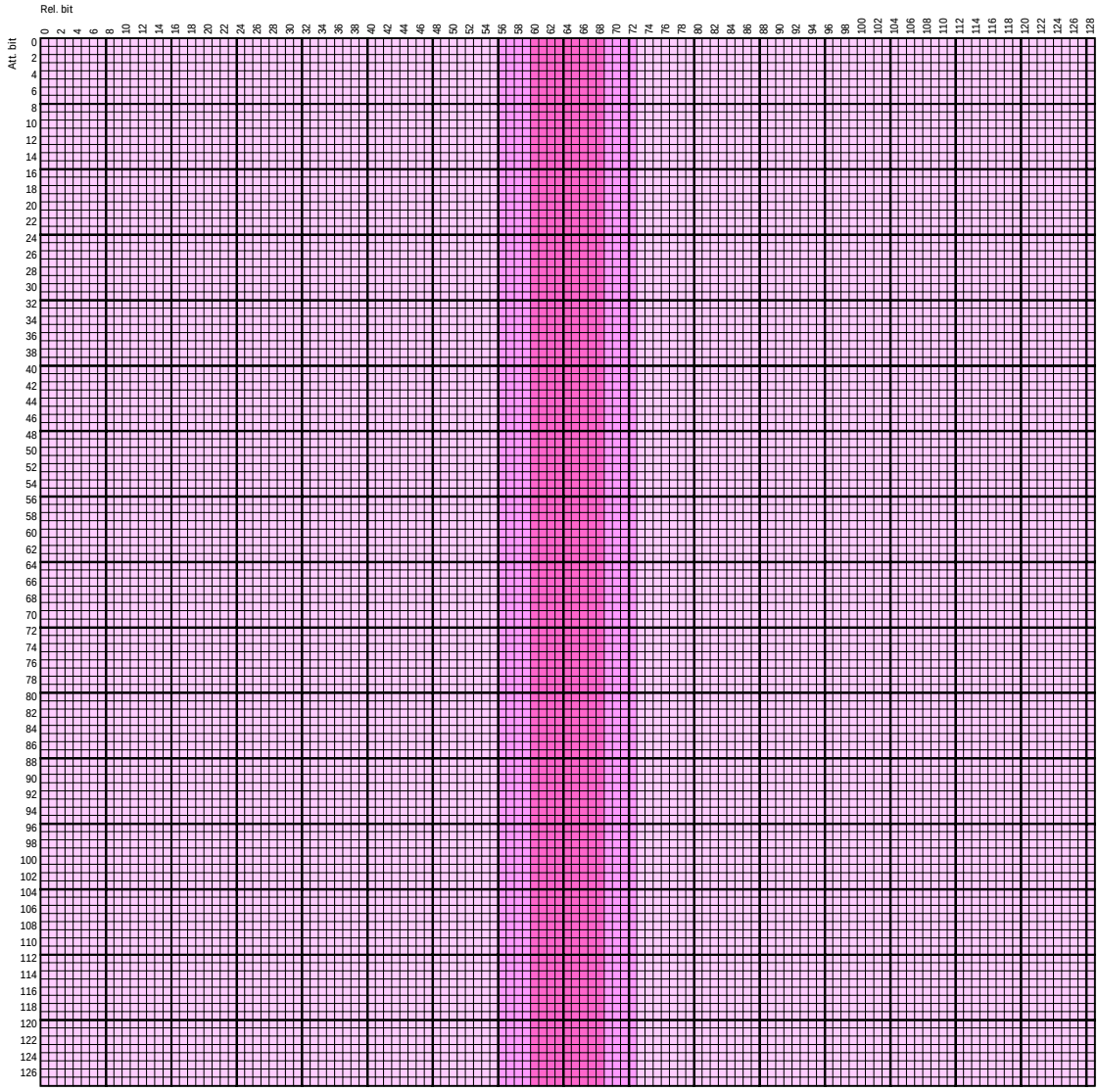


図 B.6.6 UNIA ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVD

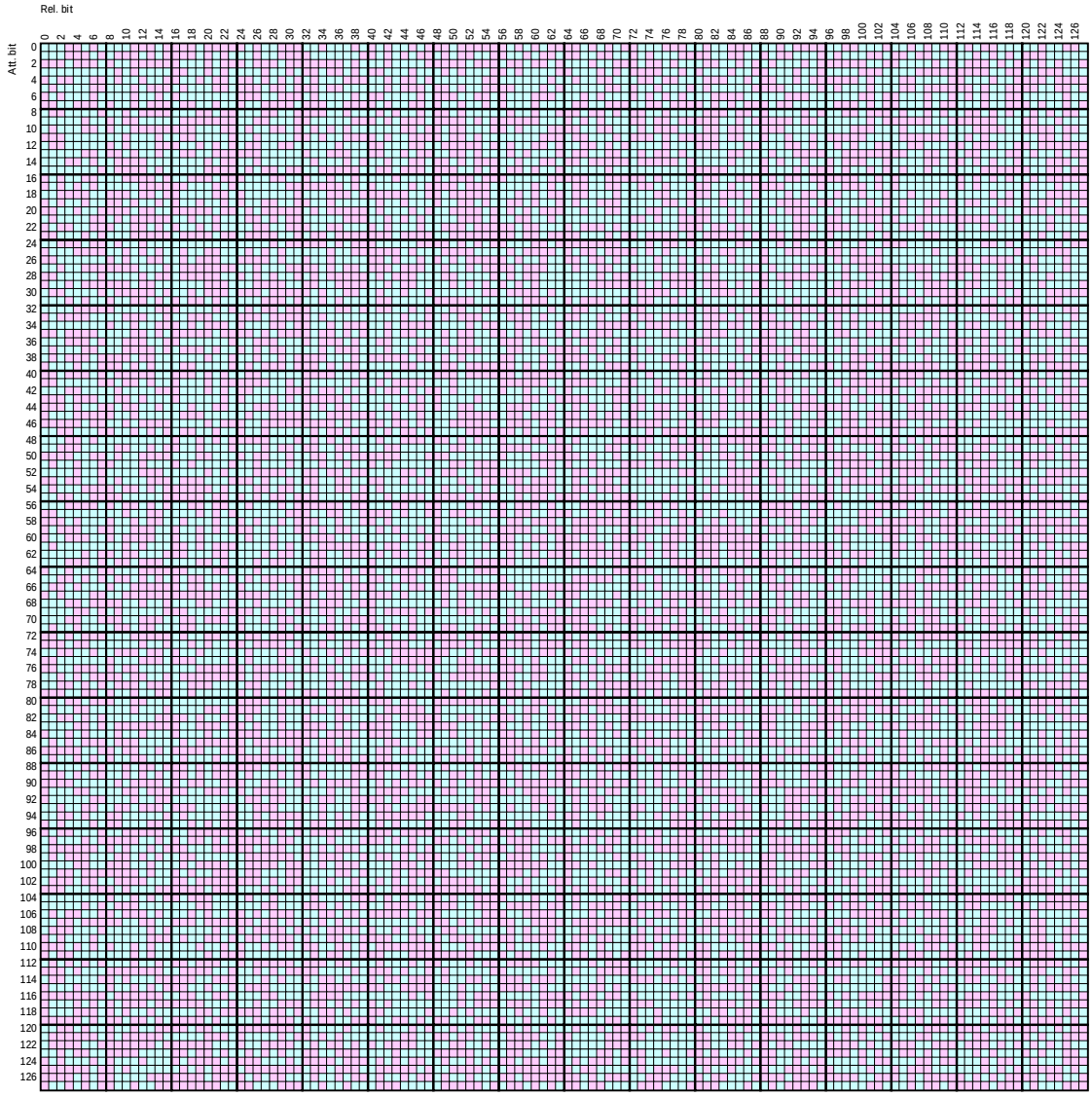
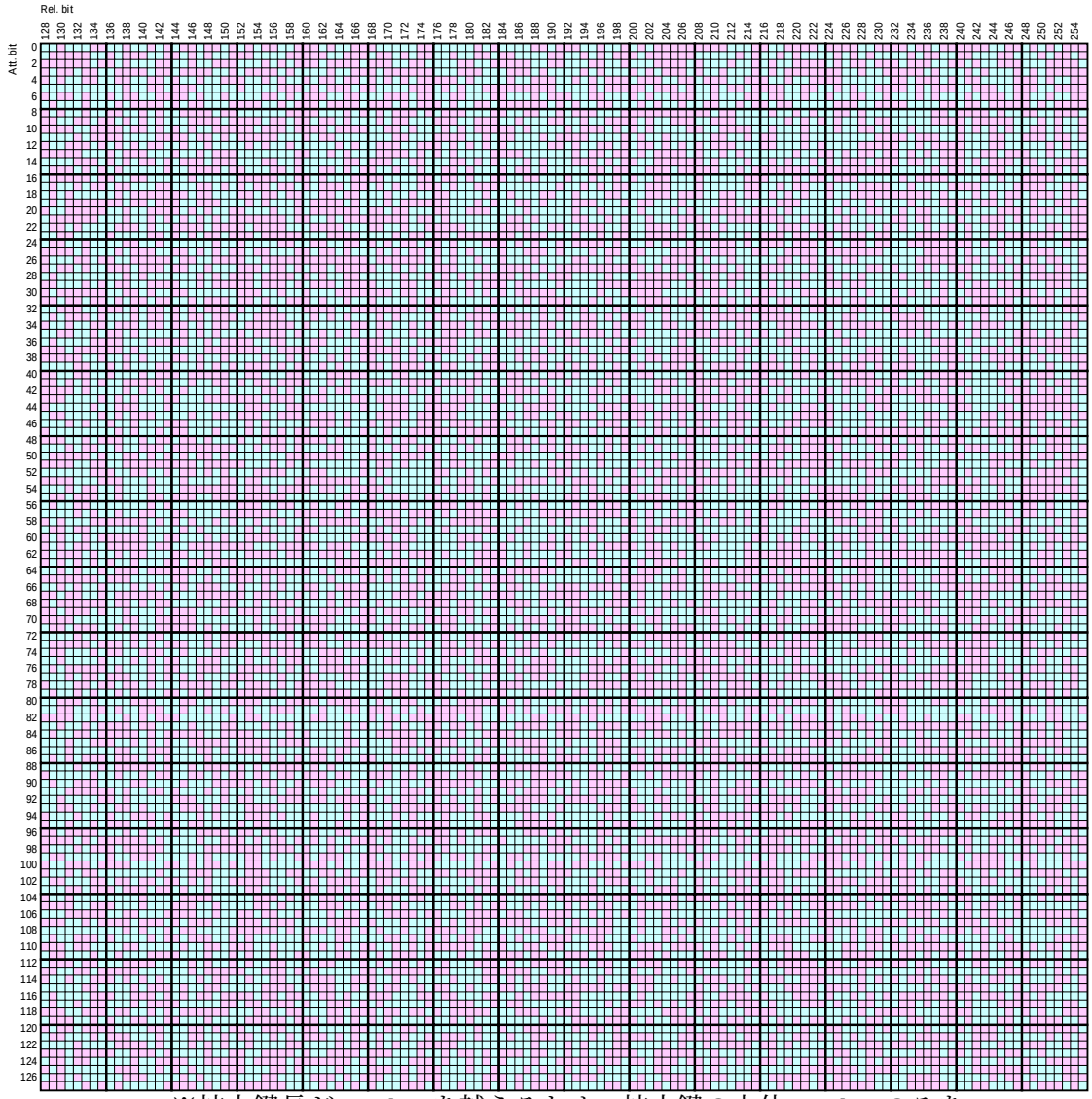


図 B.6.7 UNIA 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(1/2)

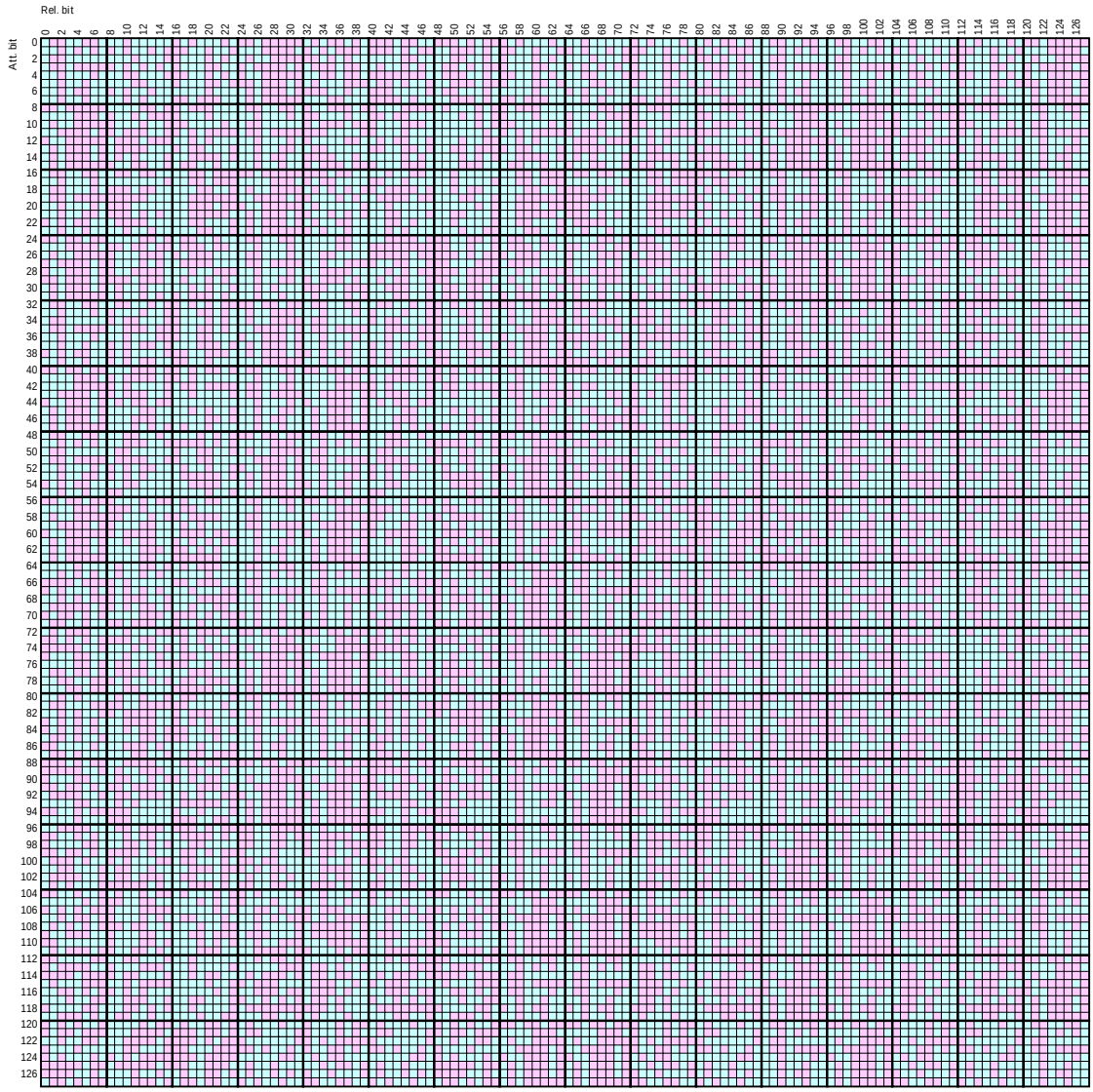


※拡大鍵長が 256bit を越えるため、拡大鍵の上位 256bit のみを
グラフ表示している。

図 B.6.8 UNIA 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(2/2)

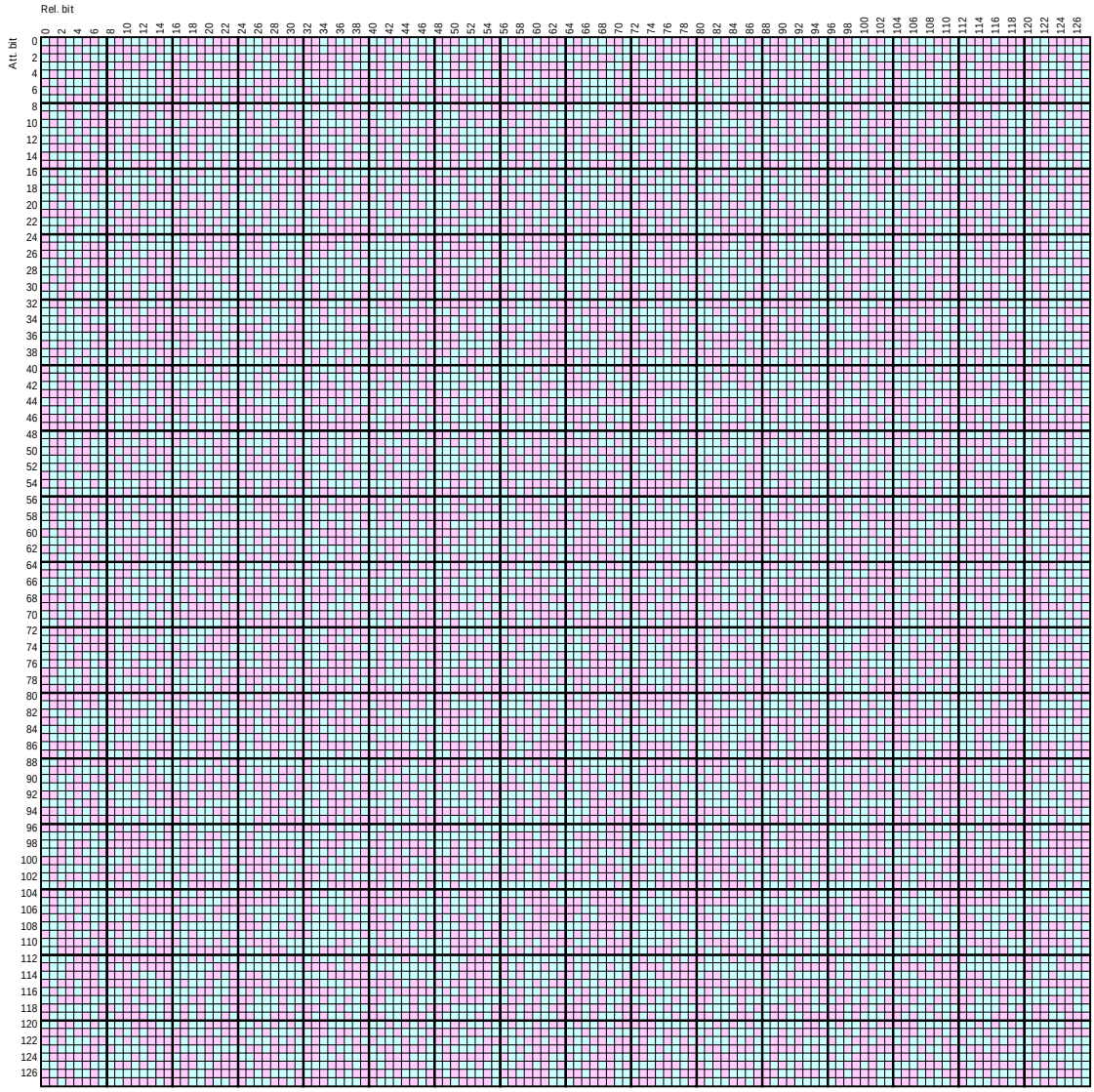
B 結果グラフ

B.7 Hierocrypt-3



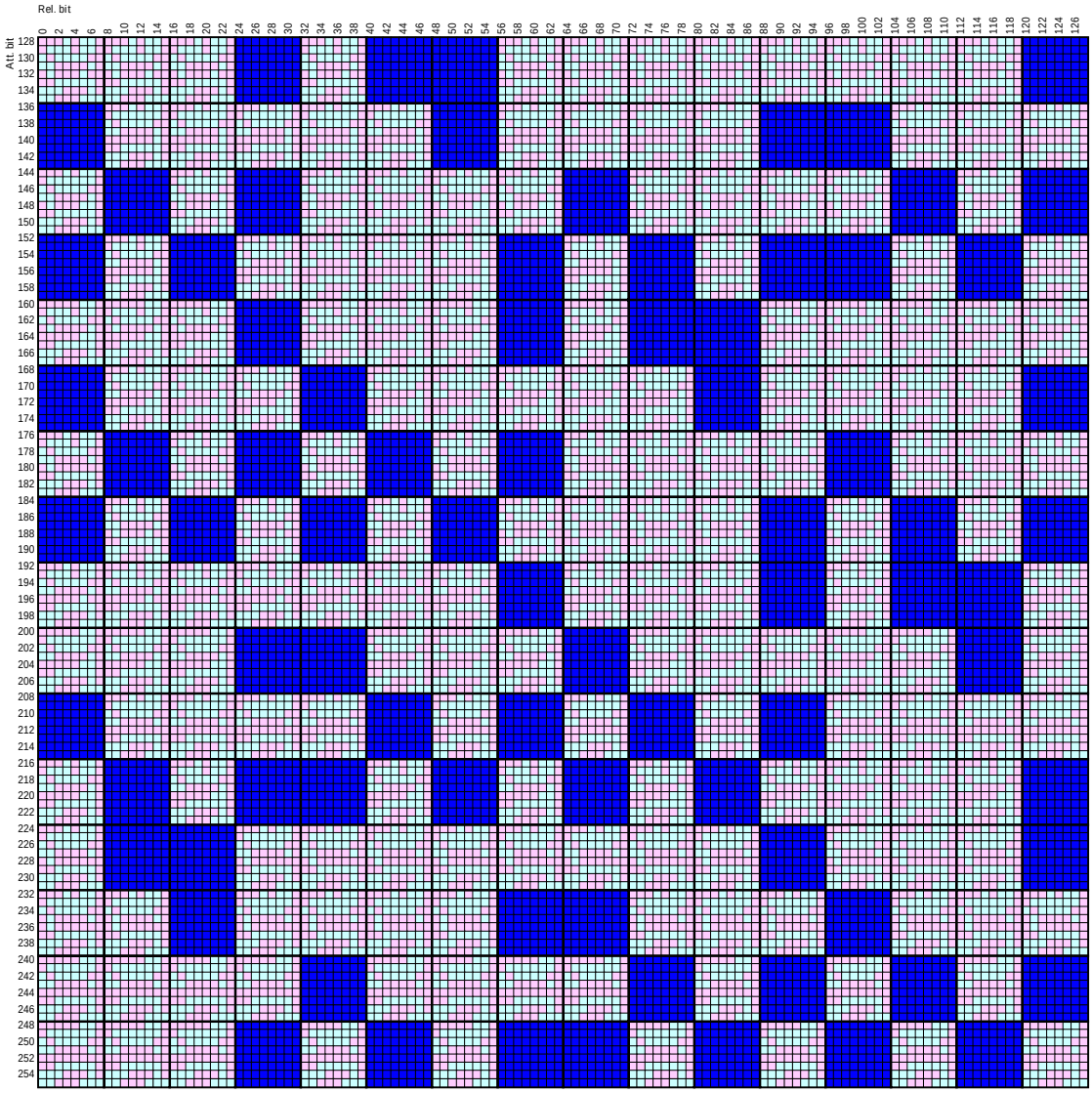
※ﾃﾞｰﾀ件数が他に比べて 1/4 である。同一のｽｹｰﾙで比較するために推測値として評価値を 4 倍した。

図 B.7.1 Hi3 ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVA



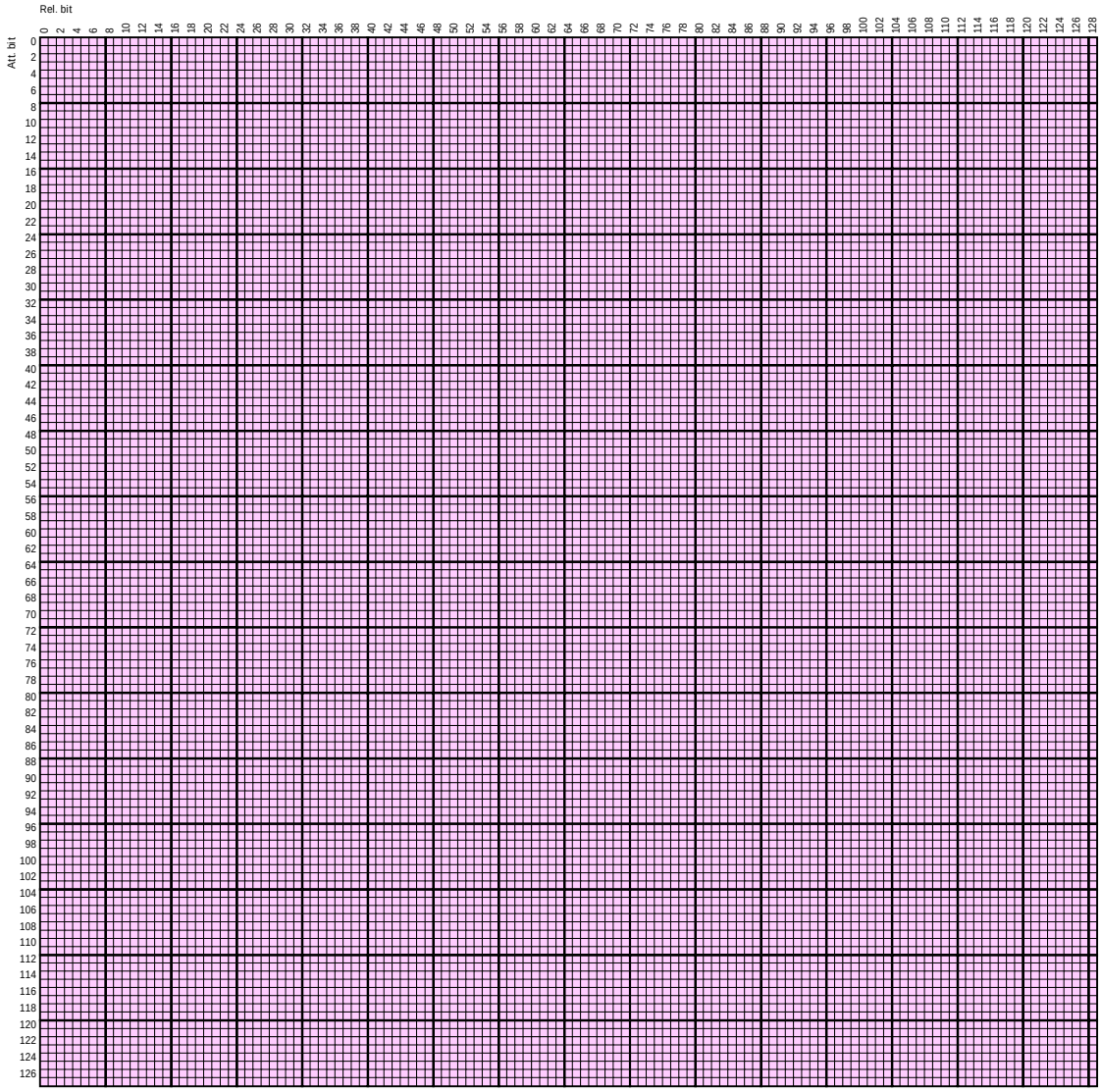
※ﾃﾞｰﾀ件数が他に比べて 1/4 である。同一のｽｹｰﾙで比較するために推測値として評価値を 4 倍した。

図 B.7.2 Hi3 ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVA(1/2)



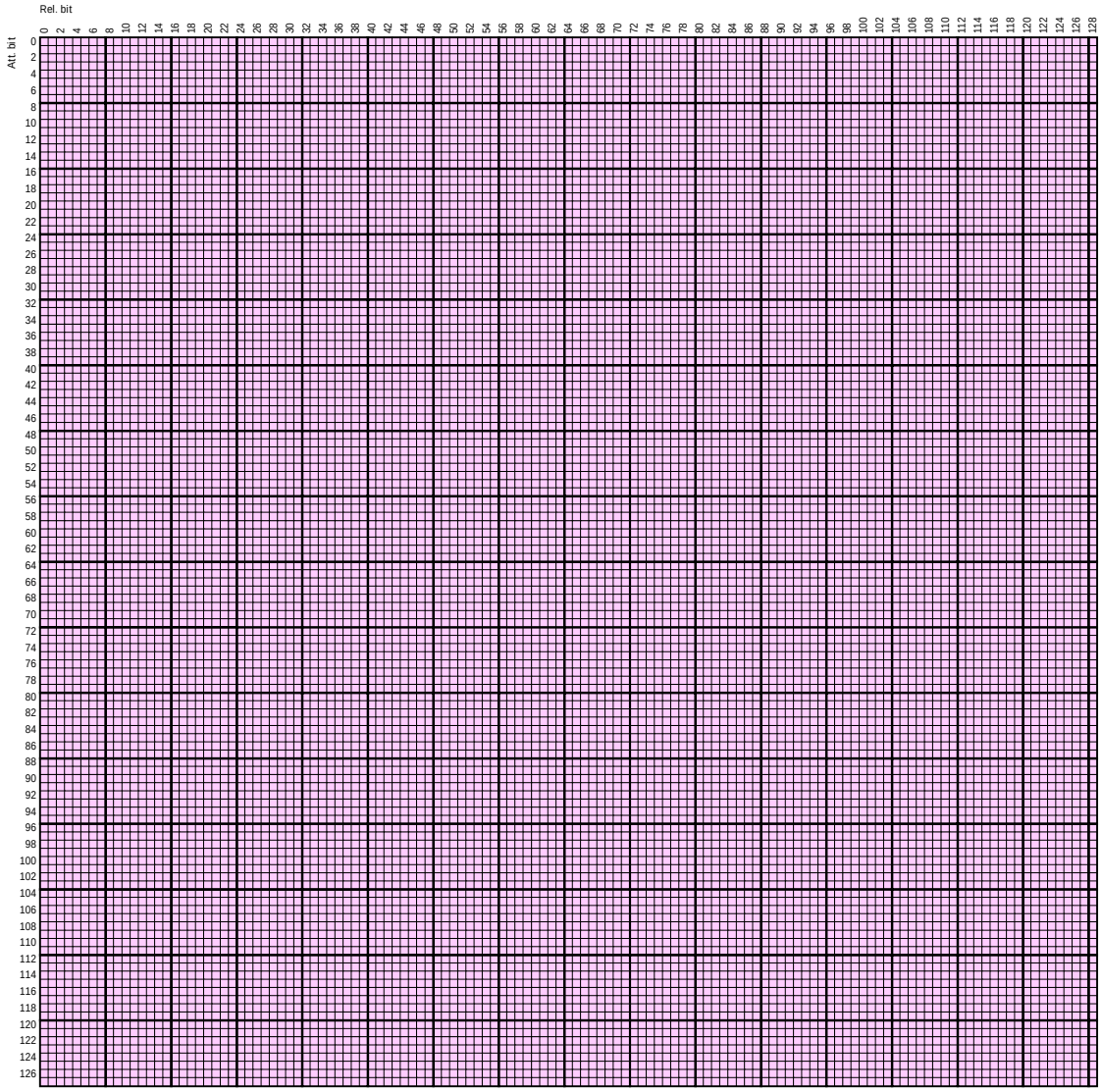
※ﾃﾞｰﾀ件数が他に比べて 1/4 である。同一のｽｹｰﾙで比較するために推測値として評価値を 4 倍した。

図 B.7.3 Hi3 ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVA(2/2)



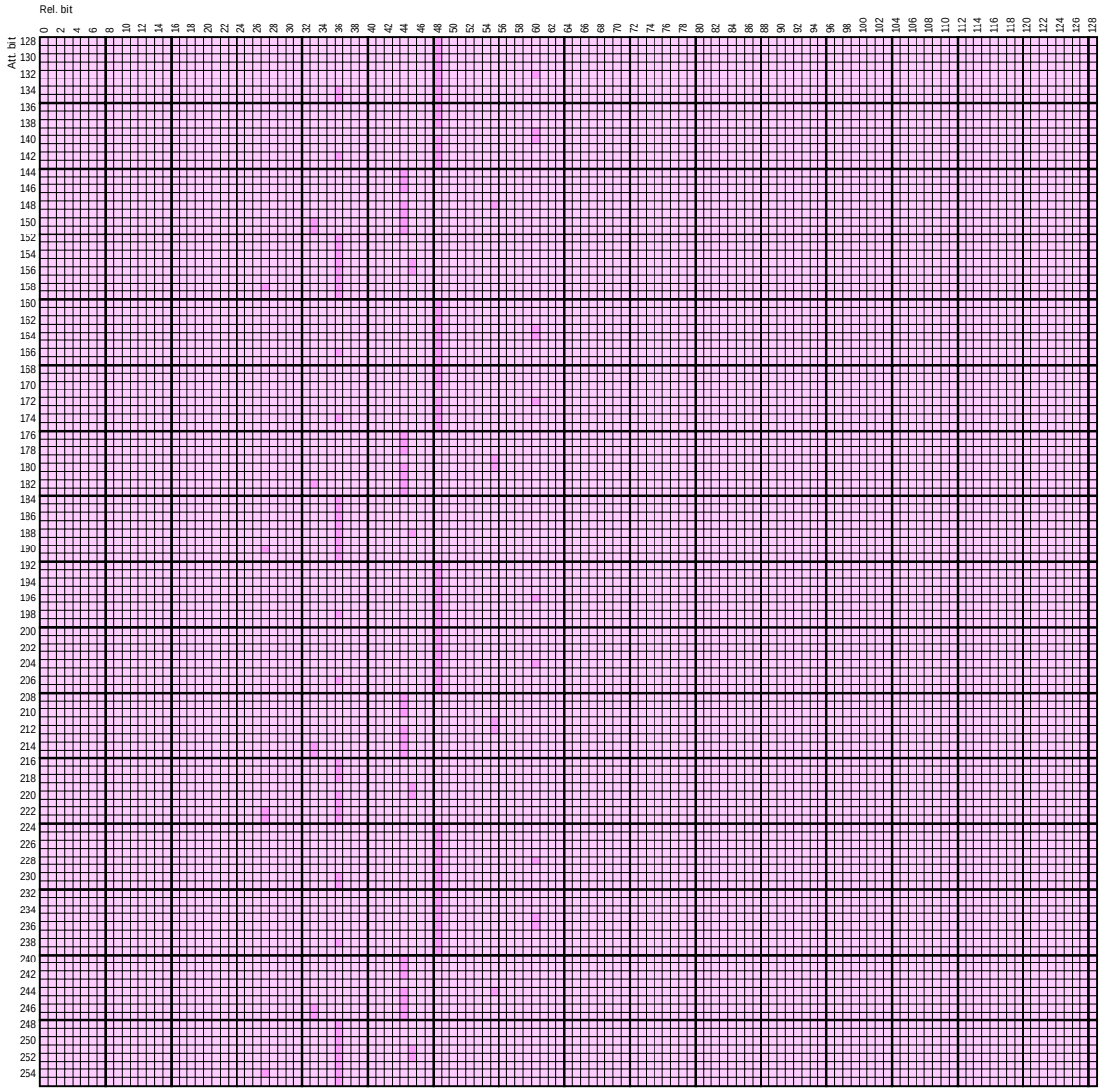
※ﾃﾞｰﾀ件数が他に比べて 1/4 である。同一のｽｹｰﾙで比較するために推測値として評価値を 4 倍した。

図 B.7.4 Hi3 ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVD



※ﾃﾞｰﾀ件数が他に比べて 1/4 である。同一のｽｹｰﾙで比較するために推測値として評価値を 4 倍した。

図 B.7.5 Hi3 ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVD(1/2)



※ﾃﾞｰﾀ件数が他に比べて 1/4 である。同一のｽｹｰﾙで比較するために推測値として評価値を 4 倍した。

図 B.7.6 Hi3 ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVD(2/2)

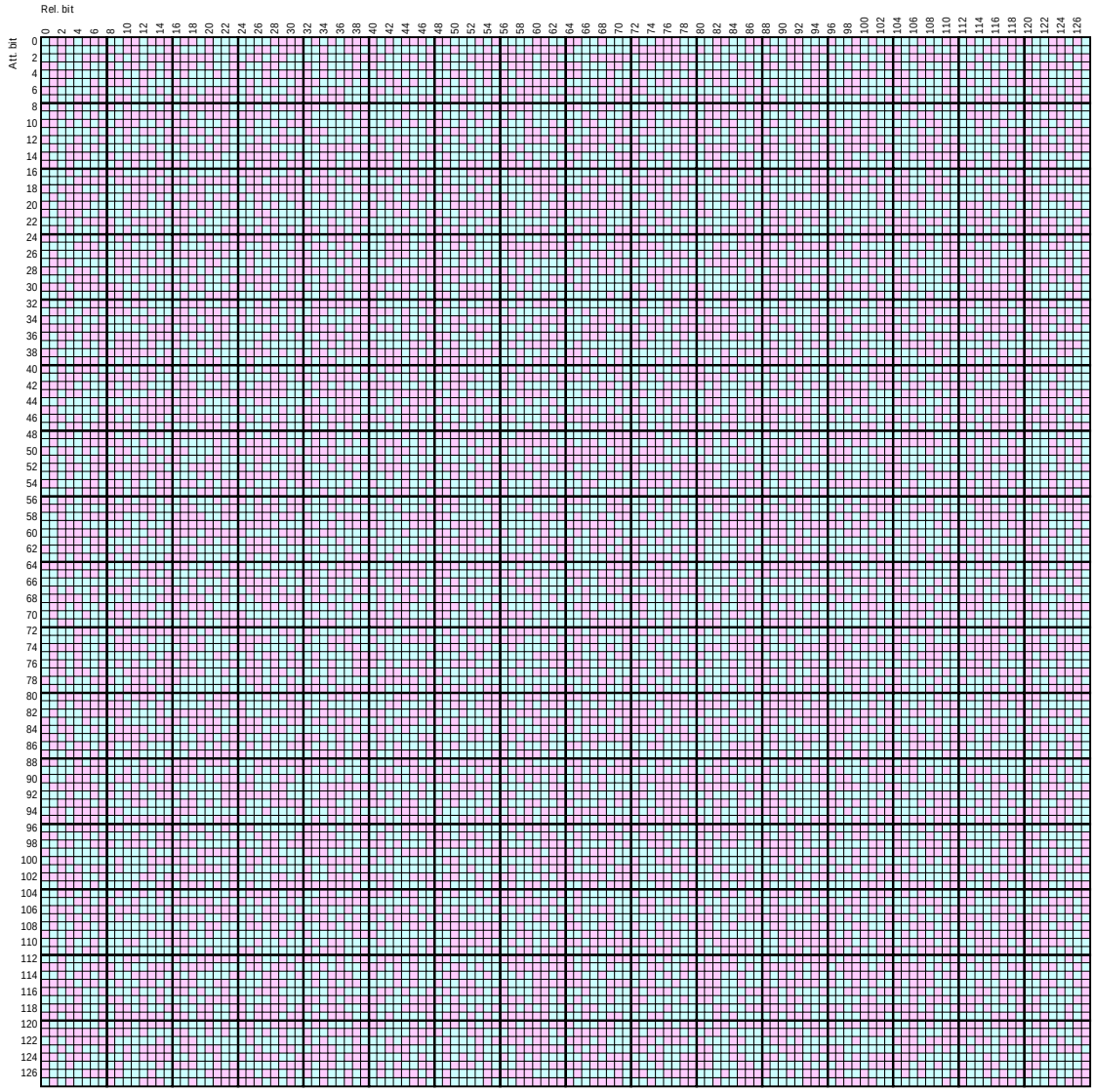


図 B.7.7 Hi3 ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVA

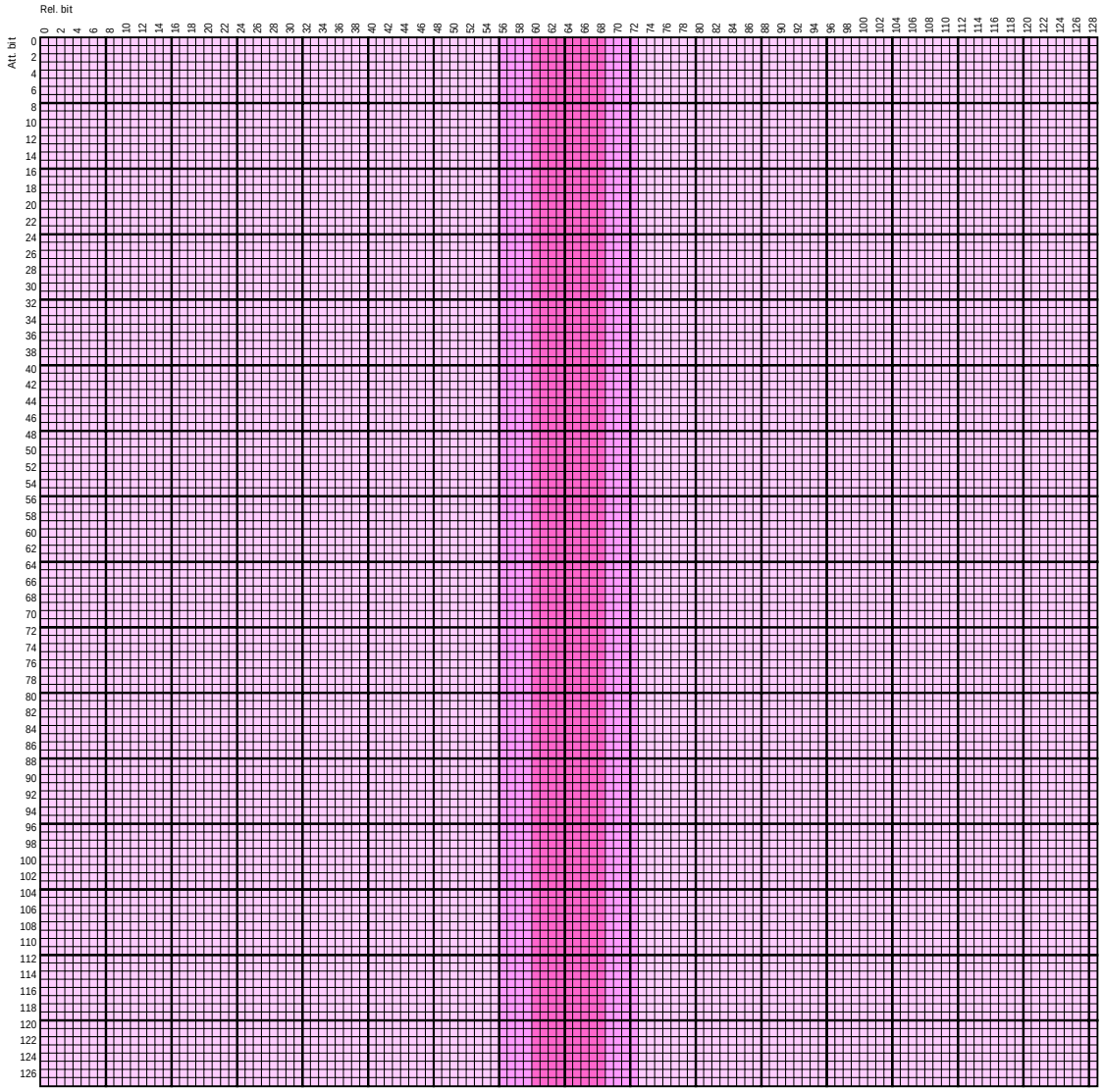


図 B.7.8 Hi3 ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVD

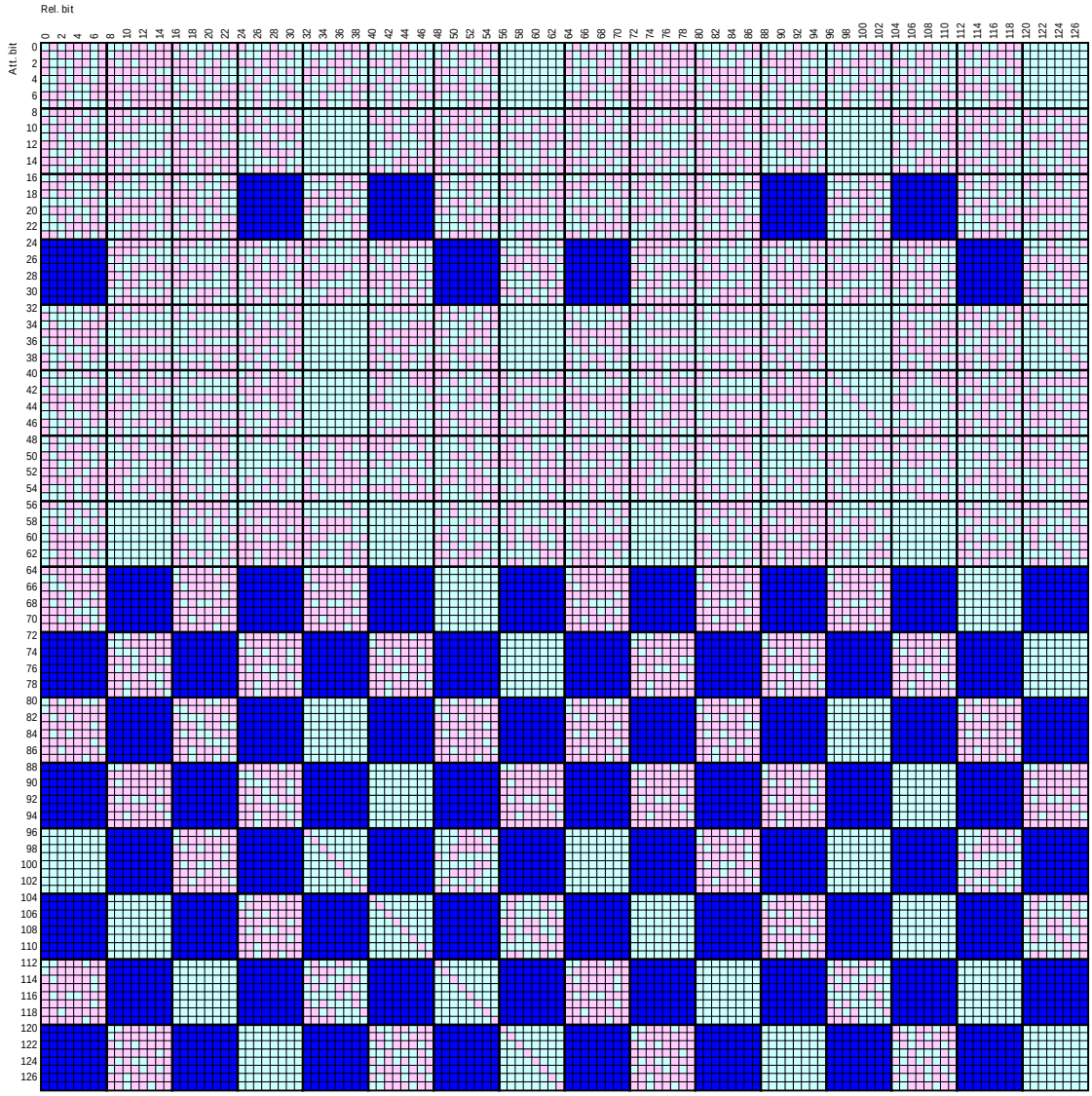
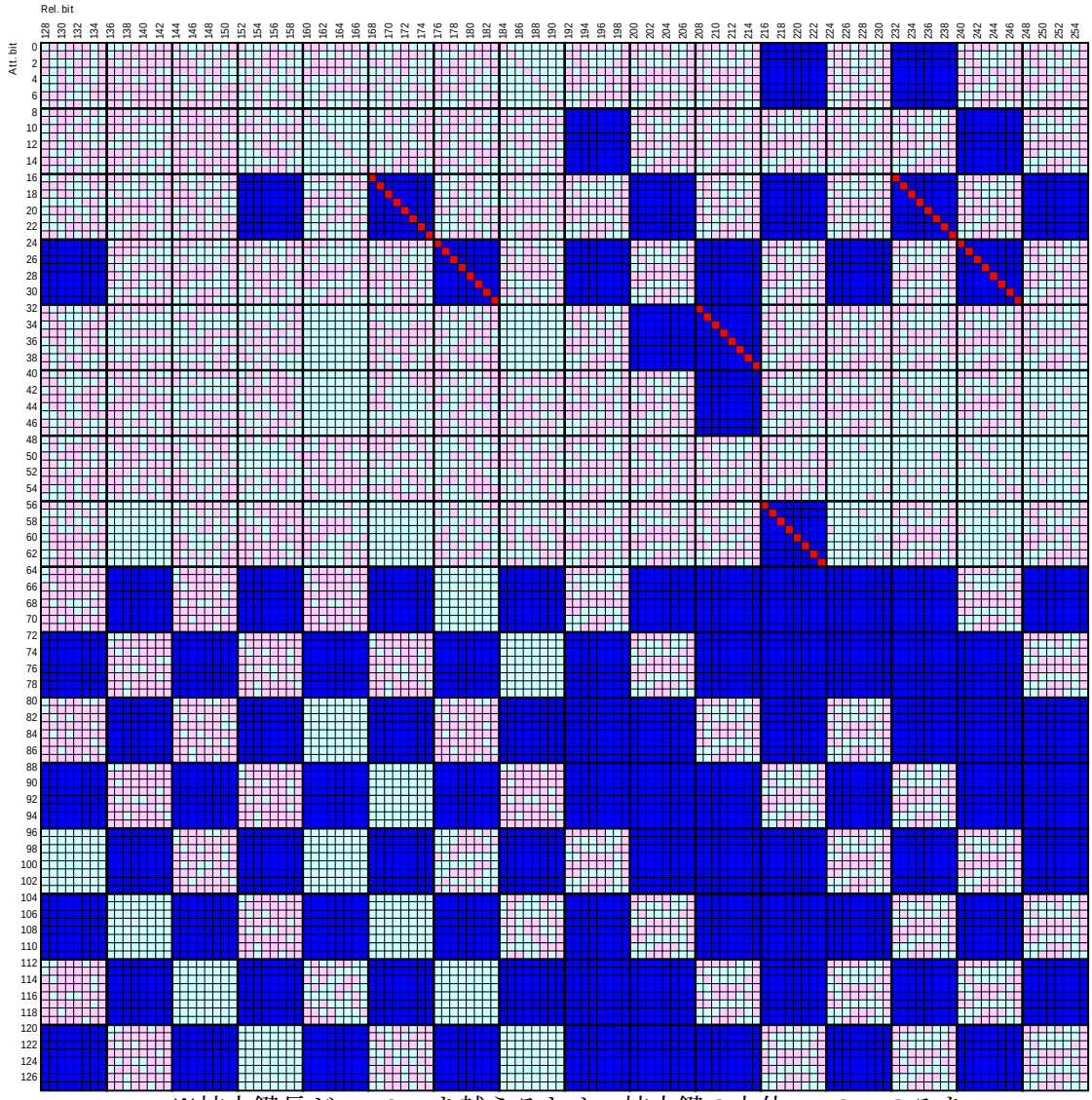


図 B.7.9 Hi3 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(1/2)



※拡大鍵長が 256bit を越えるため、拡大鍵の上位 256bit のみを
グラフ表示している。

図 B.7.10 Hi3 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(2/2)

B 結果グラフ
B.8 MARS

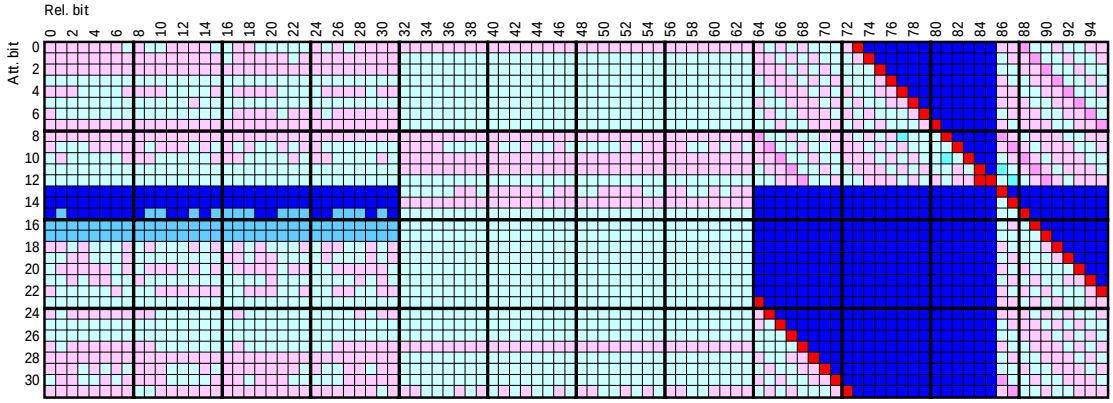


図 B.8.1 MARS ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVA

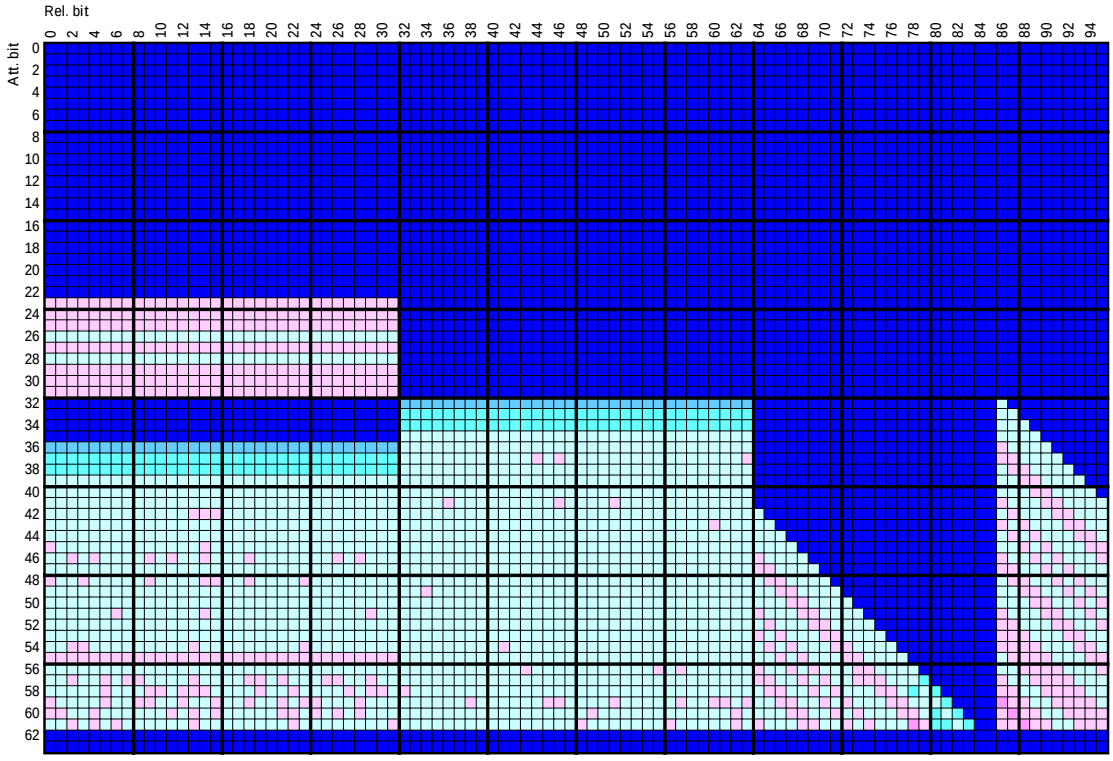


図 B.8.2 MARS ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVA

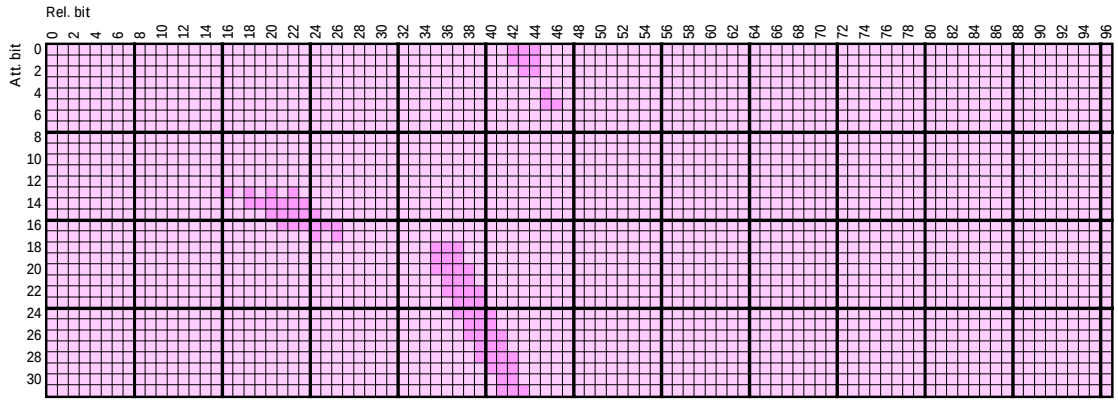


図 B.8.3 MARS ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVD

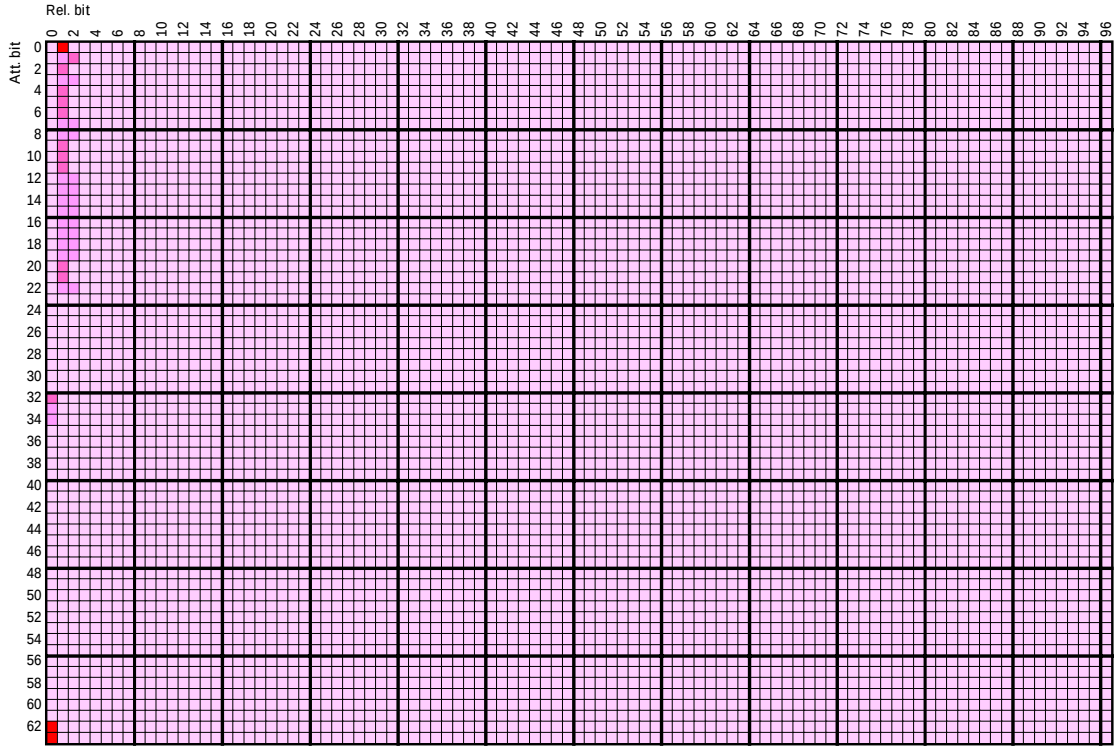


図 B.8.4 MARS ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVD

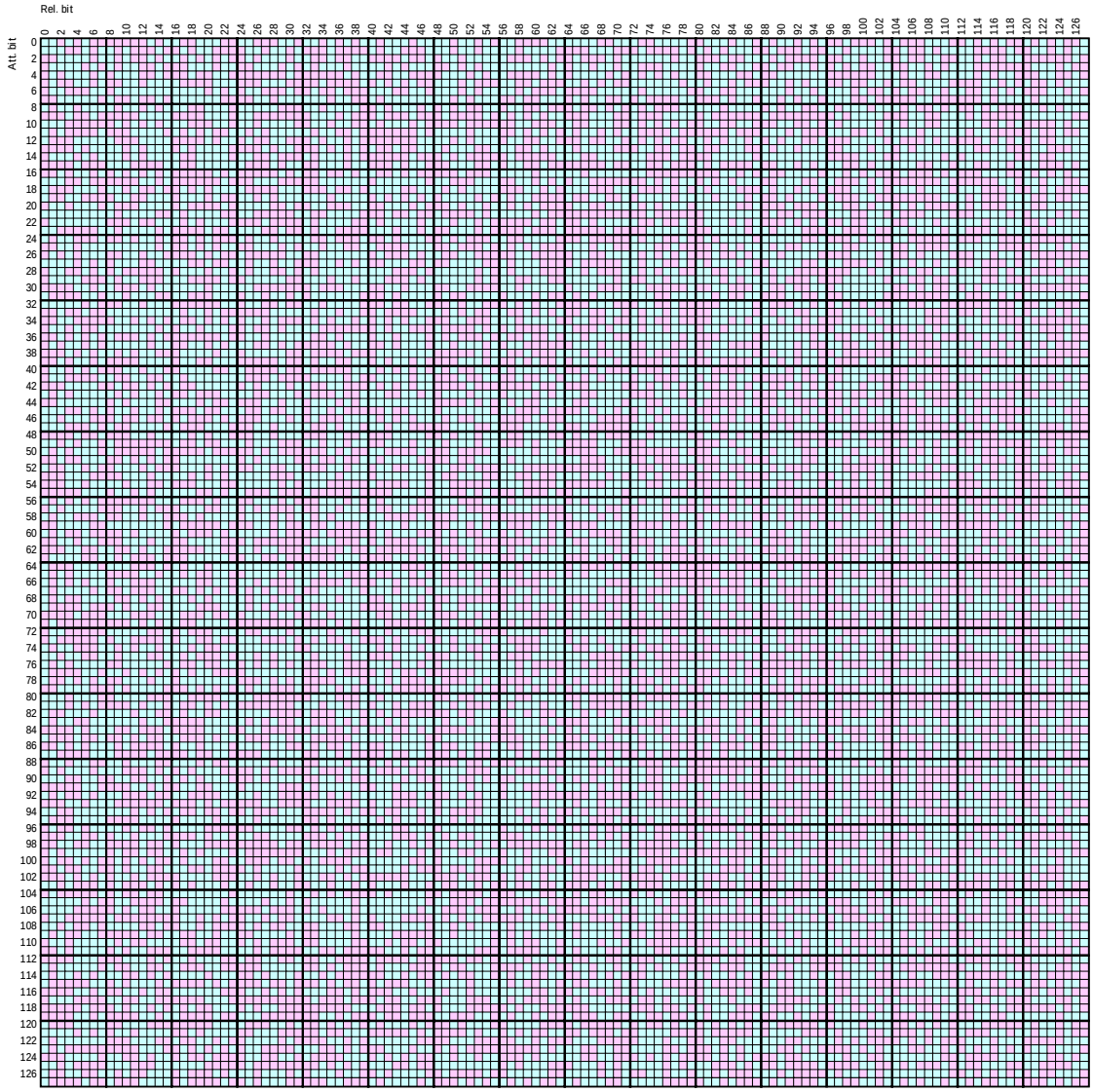


図 B.8.5 MARS ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVA

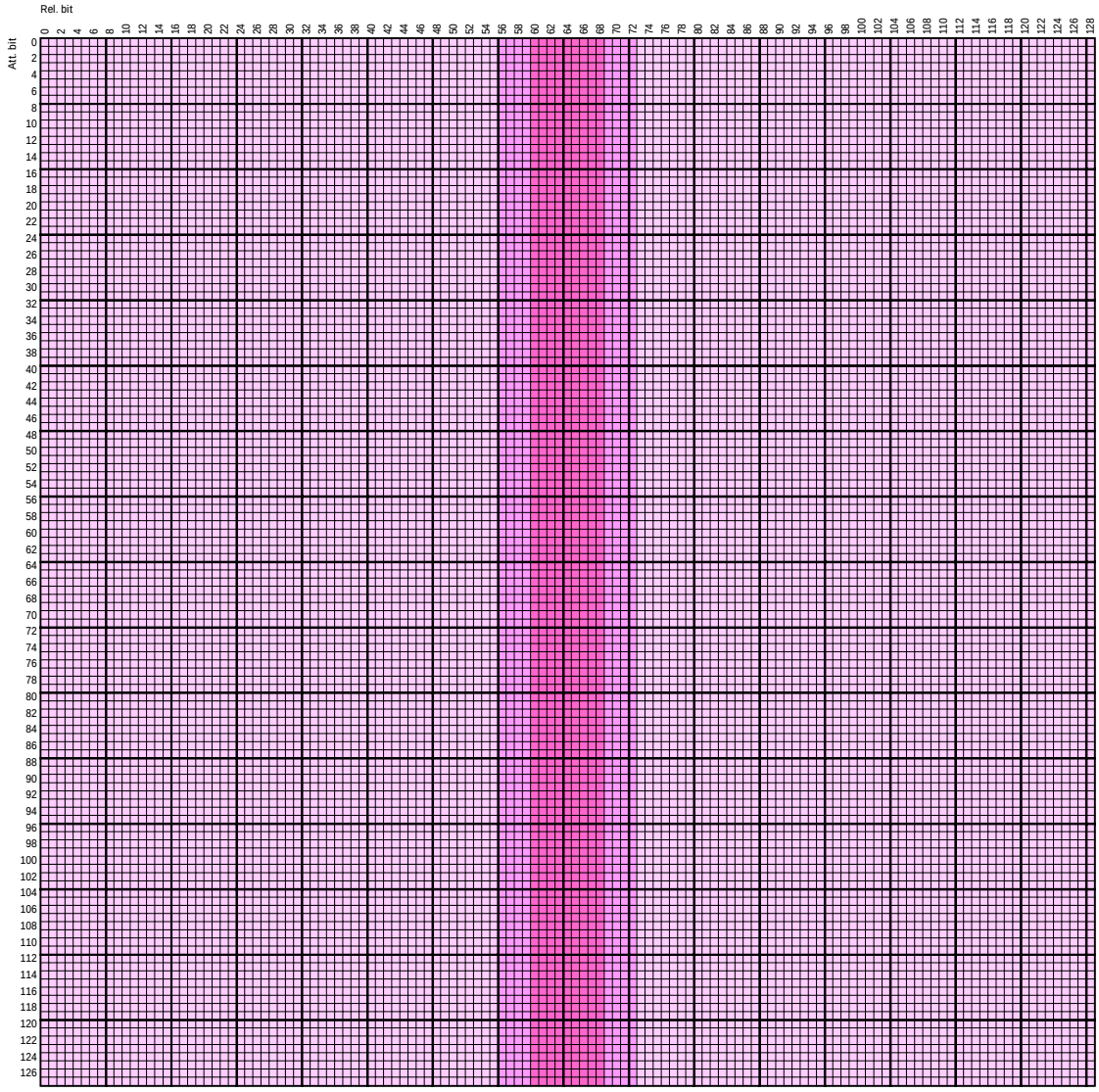


図 B.8.6 MARS ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVD

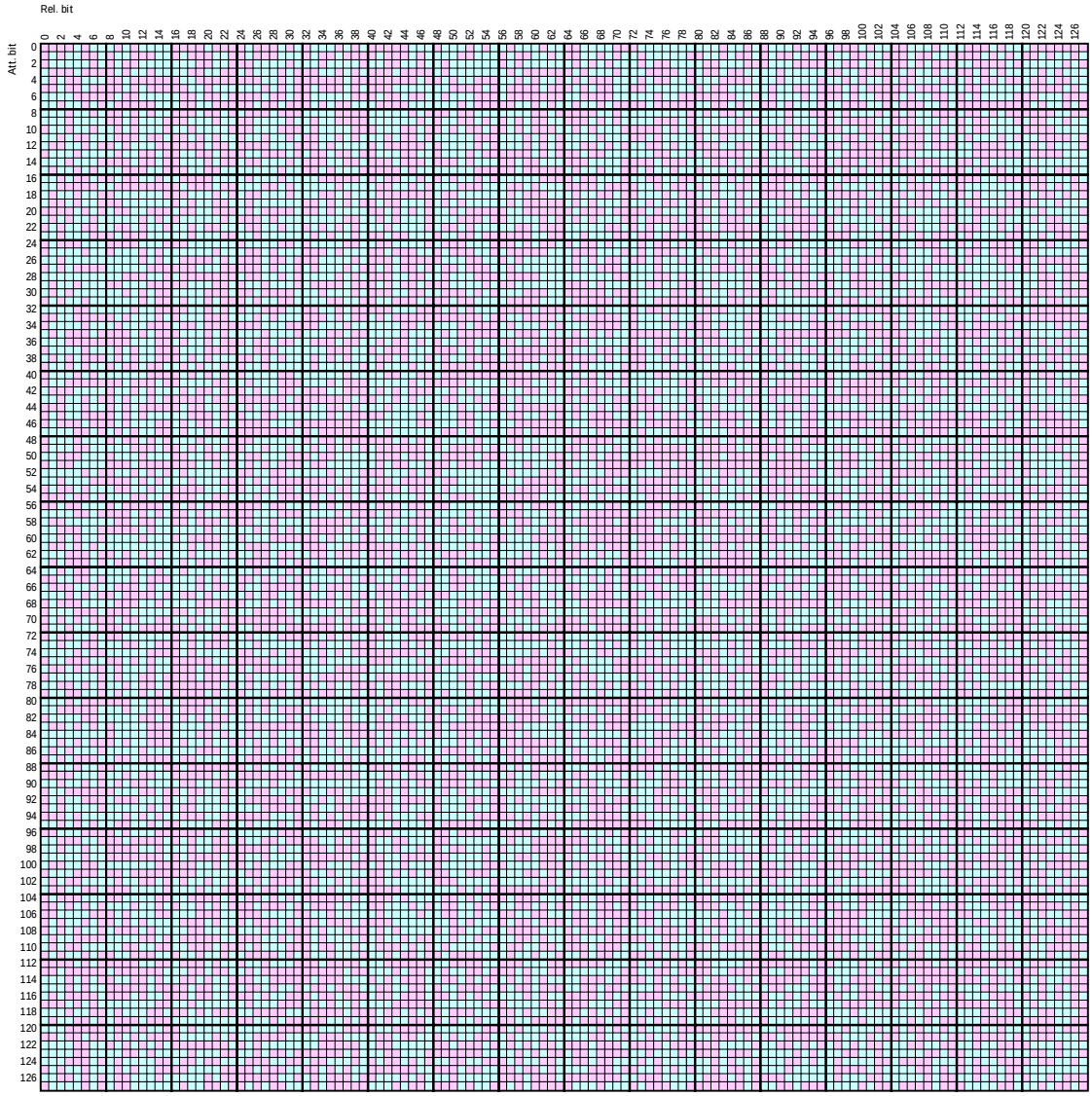
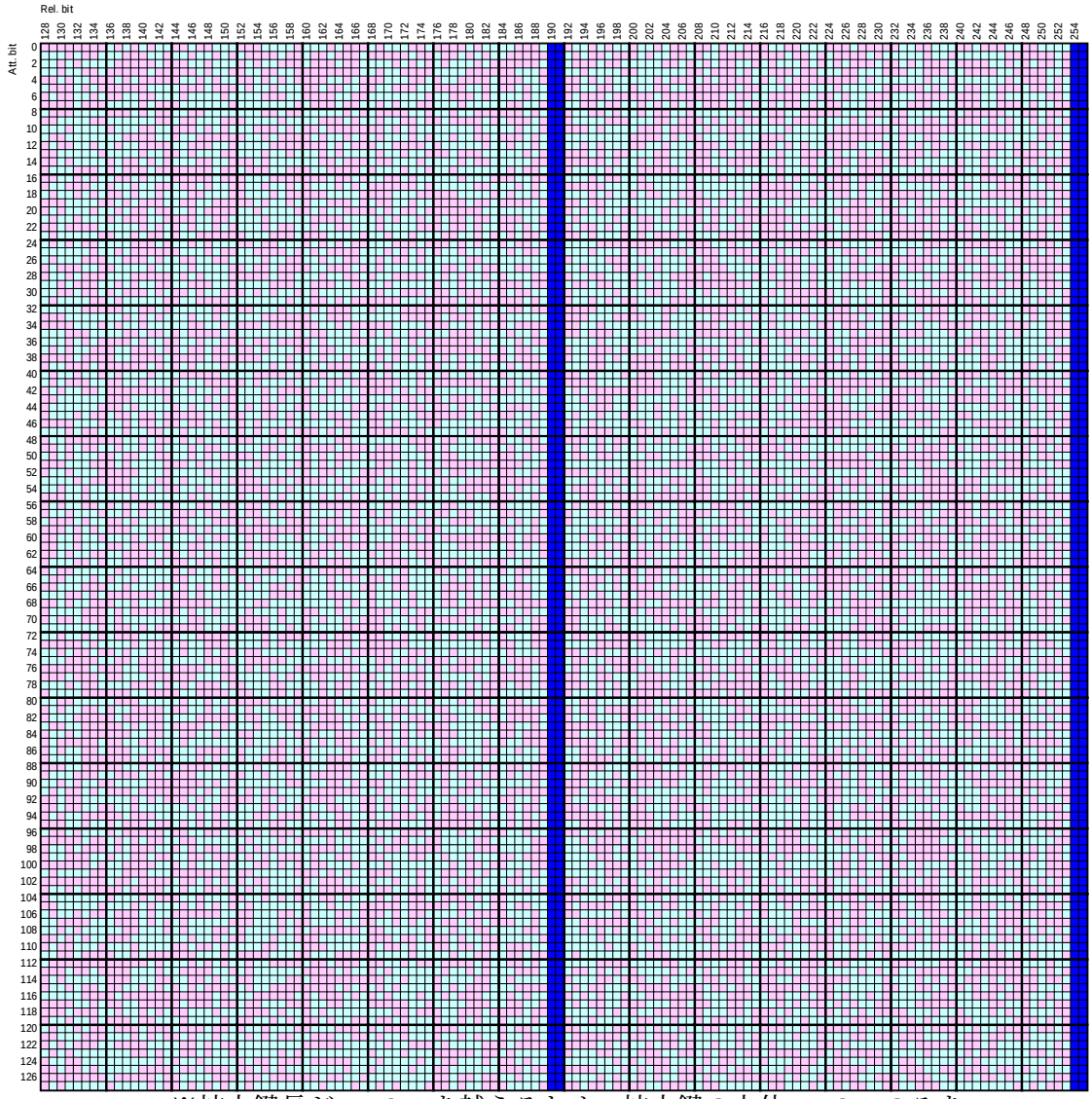


図 B.8.7 MARS 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(1/2)



※拡大鍵長が 256bit を越えるため、拡大鍵の上位 256bit のみを
グラフ表示している。

図 B.8.8 MARS 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(2/2)

B 結果グラフ

B.9 RC6

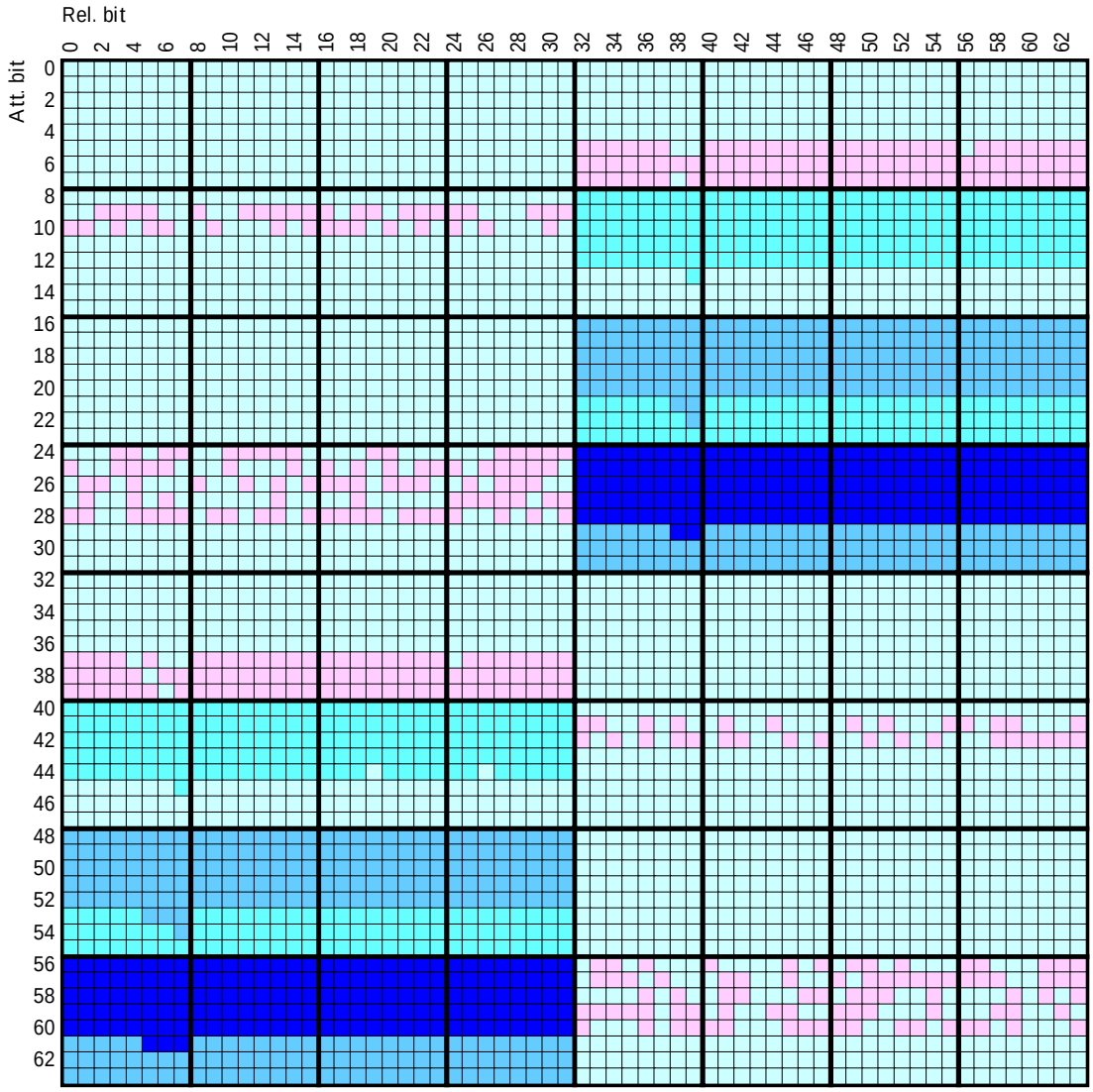


図 B.9.1 RC6 ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVA

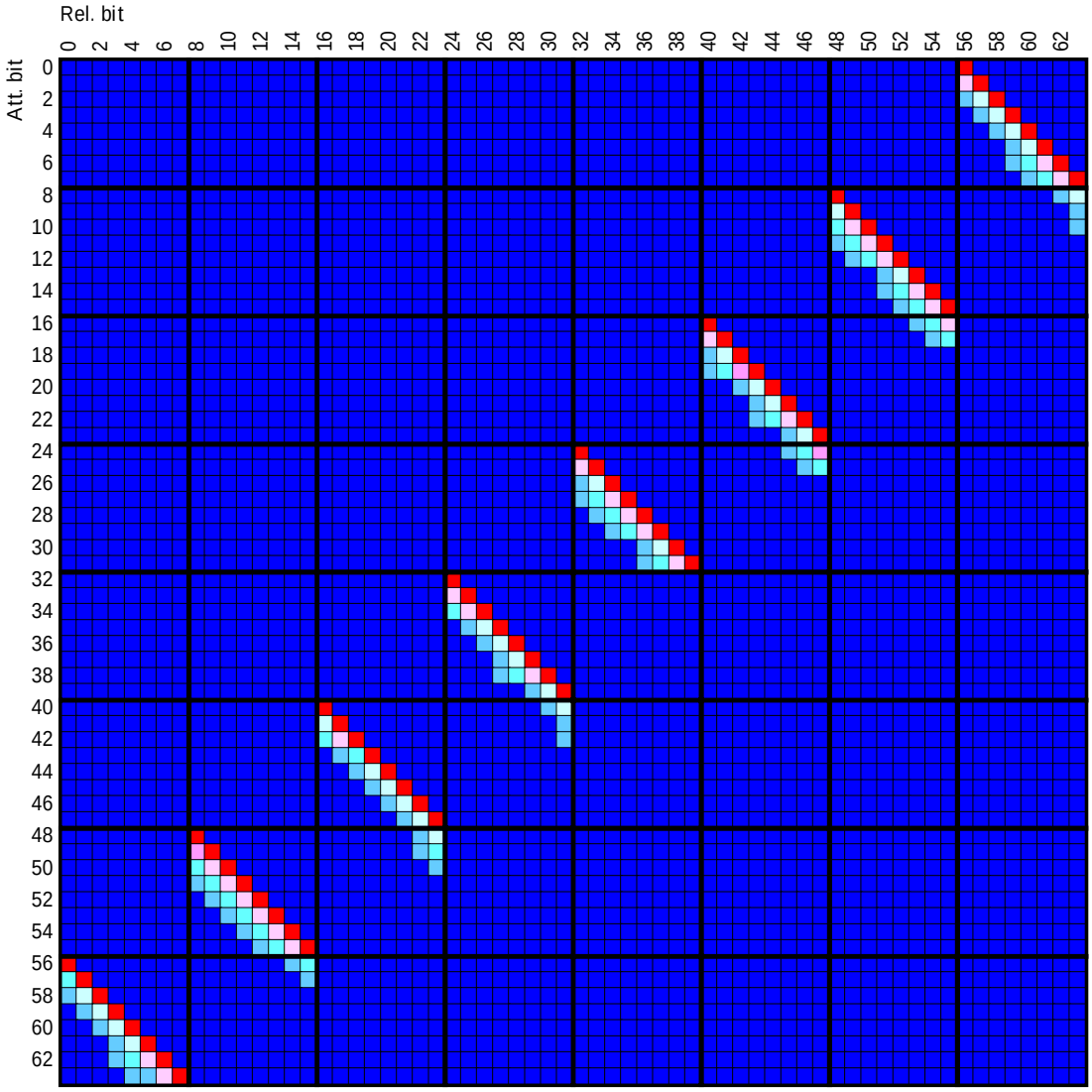


図 B.9.2 RC6 ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVA

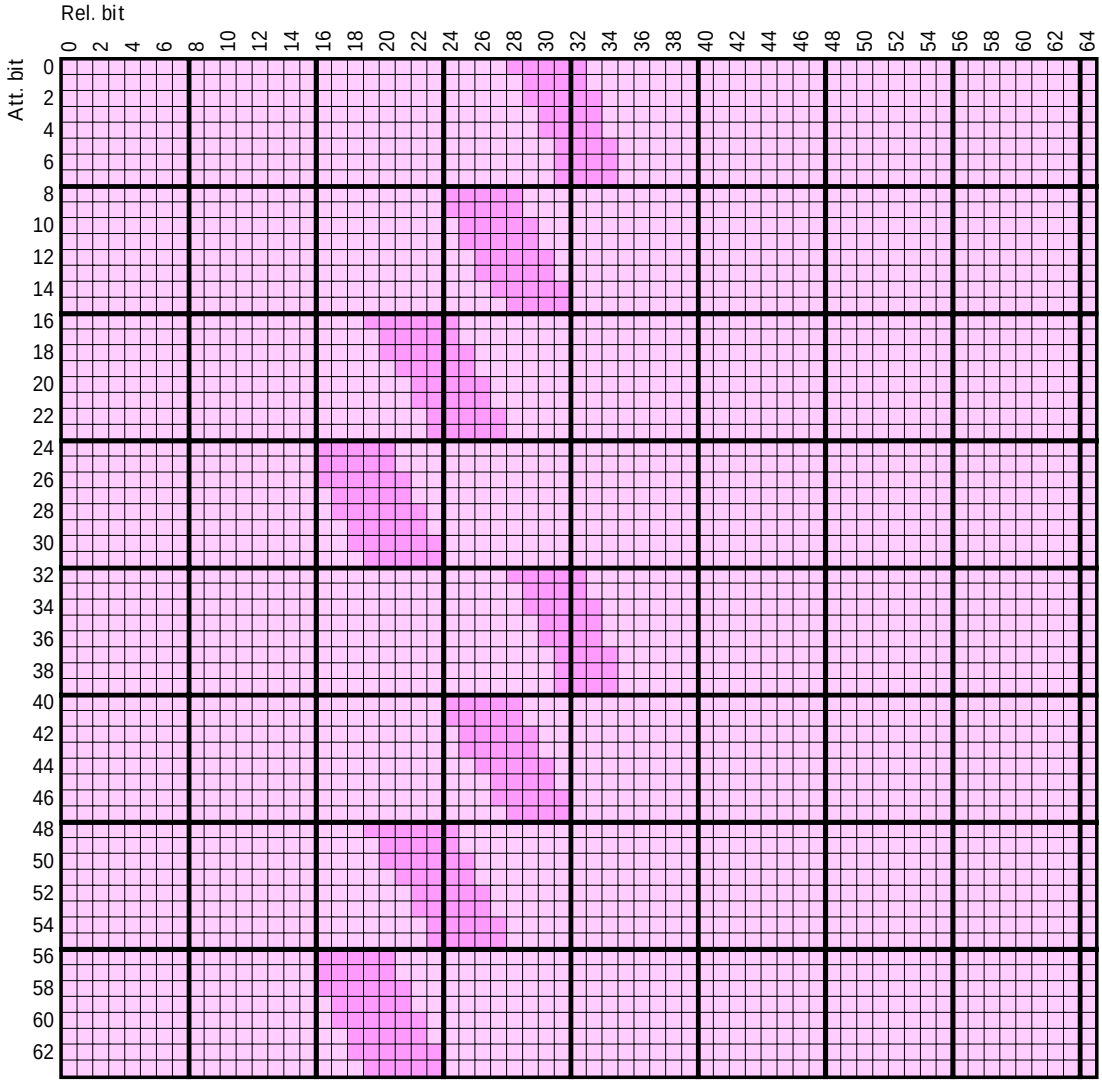


図 B.9.3 RC6 ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVD

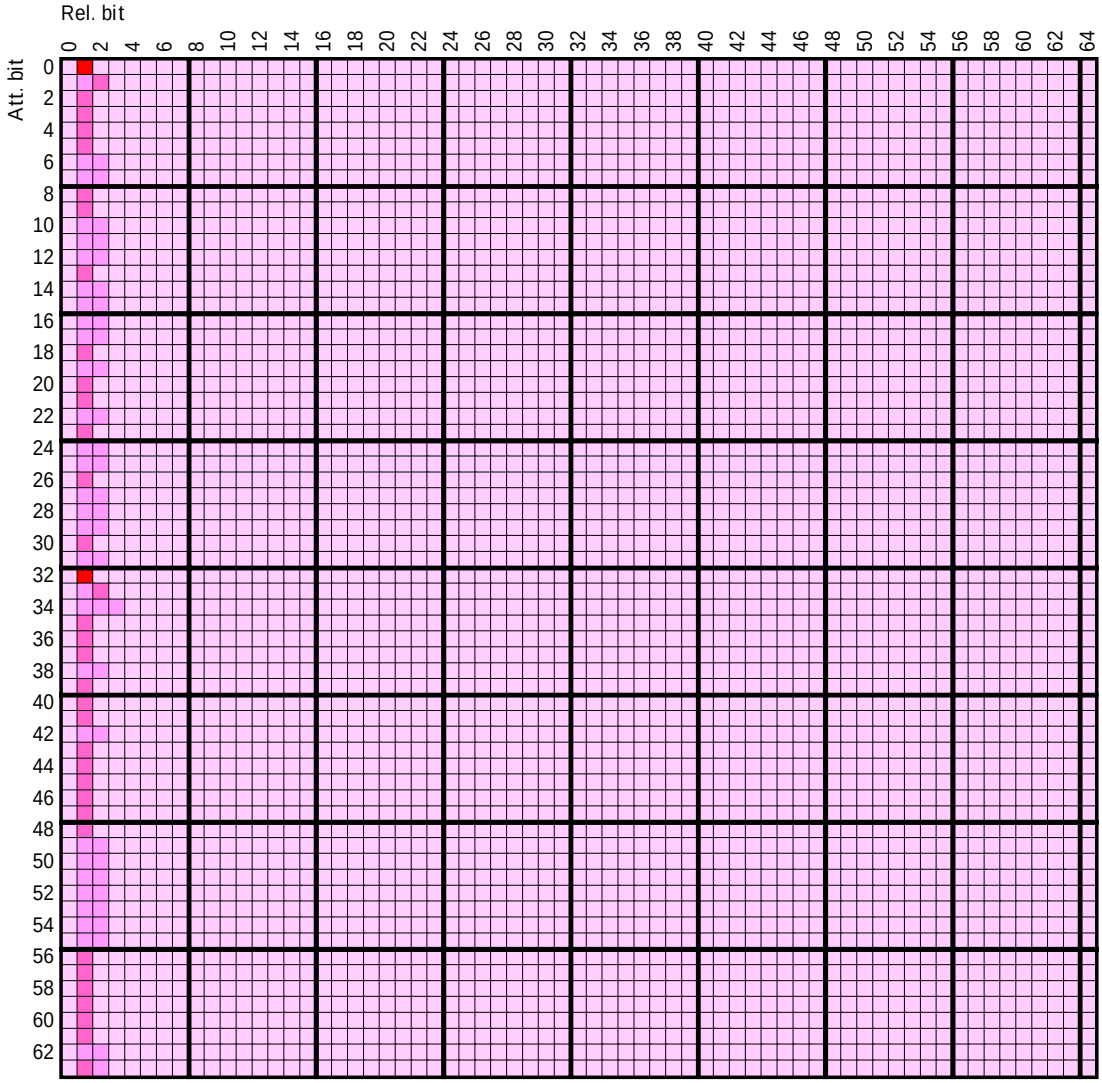


図 B.9.4 RC6 ﾗｳﾝﾄﾞ関数 拡大鍵と出力の相関(Hw=1) AVD

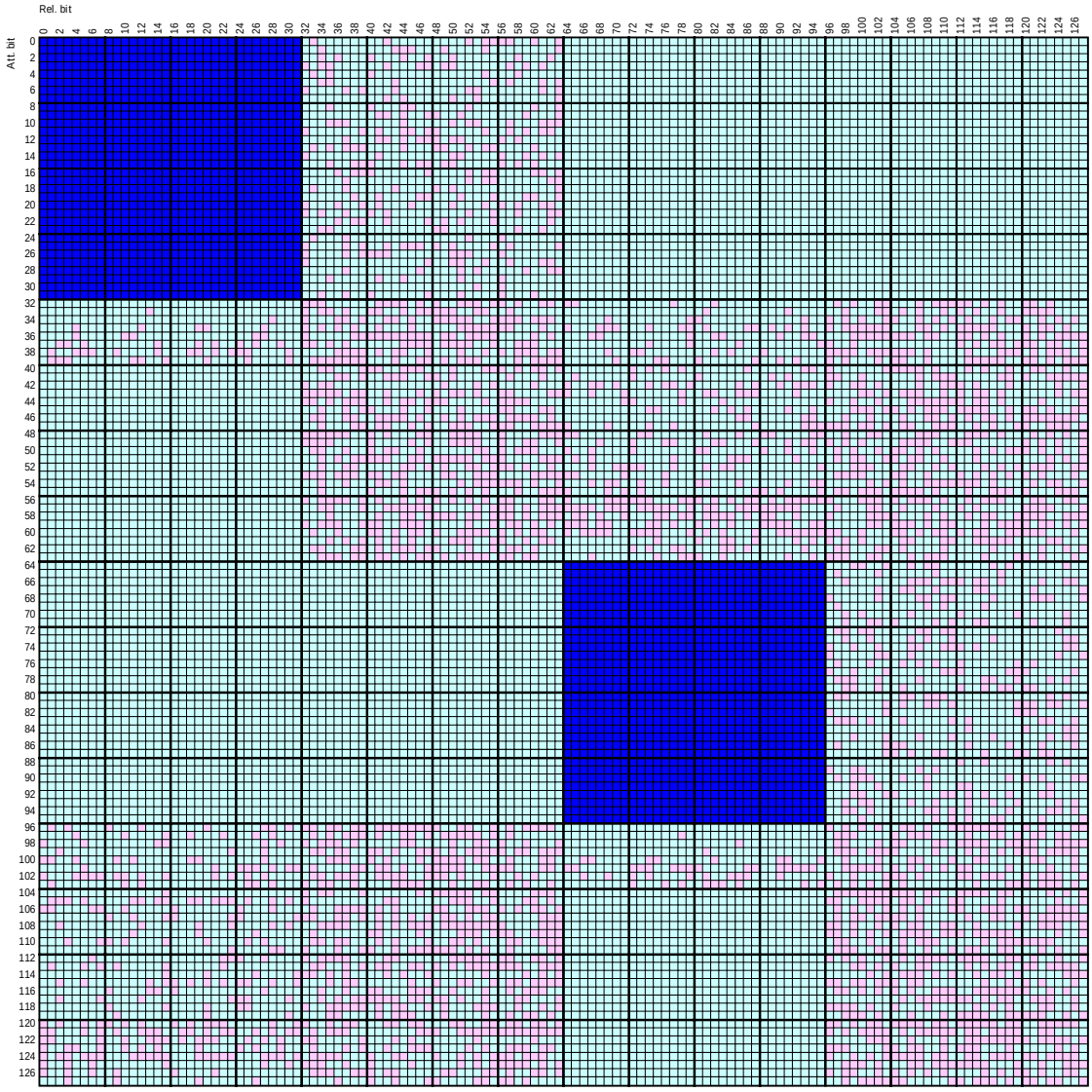


図 B.9.5 RC6 ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVA

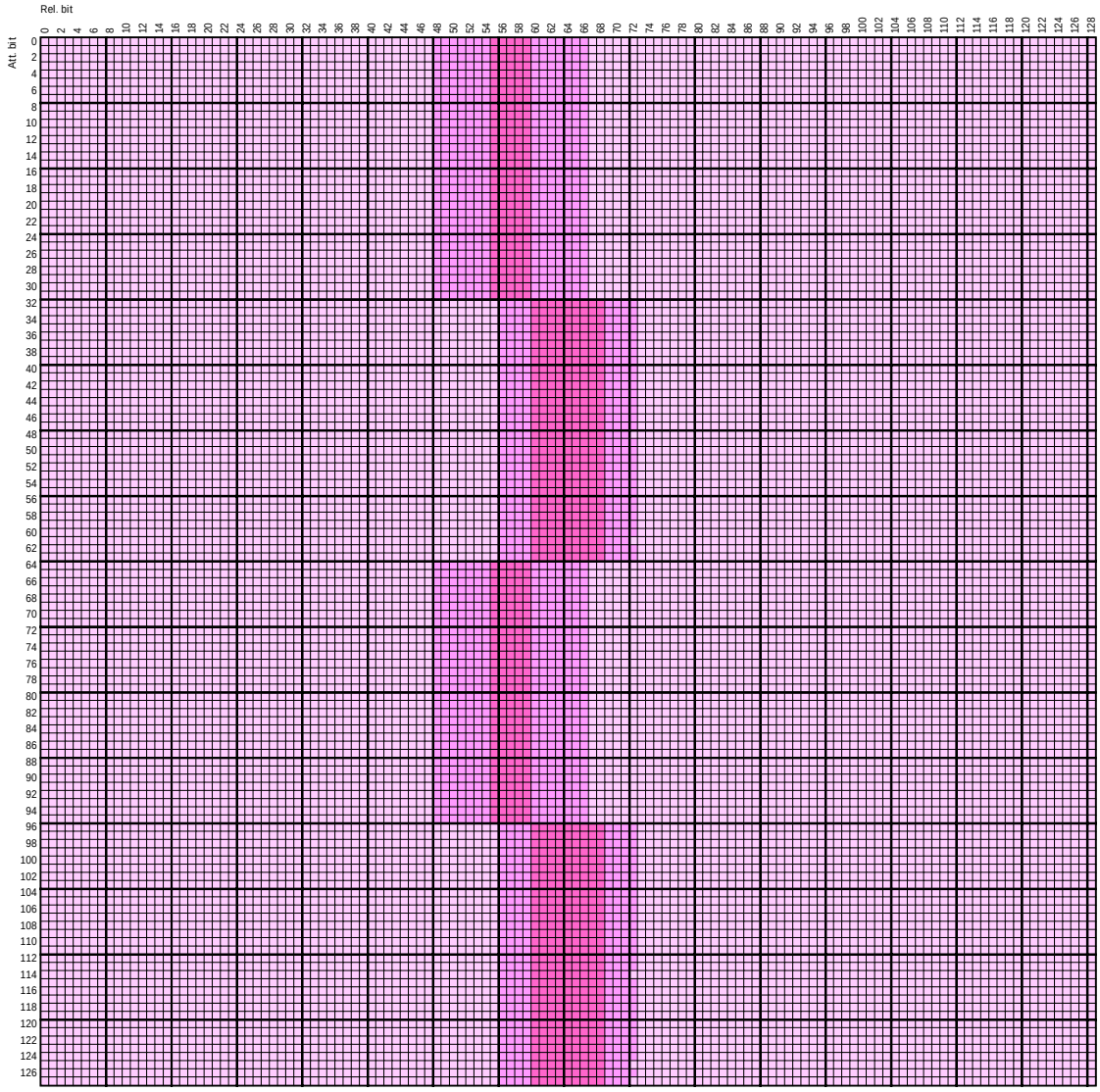


図 B.9.6 RC6 ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVD

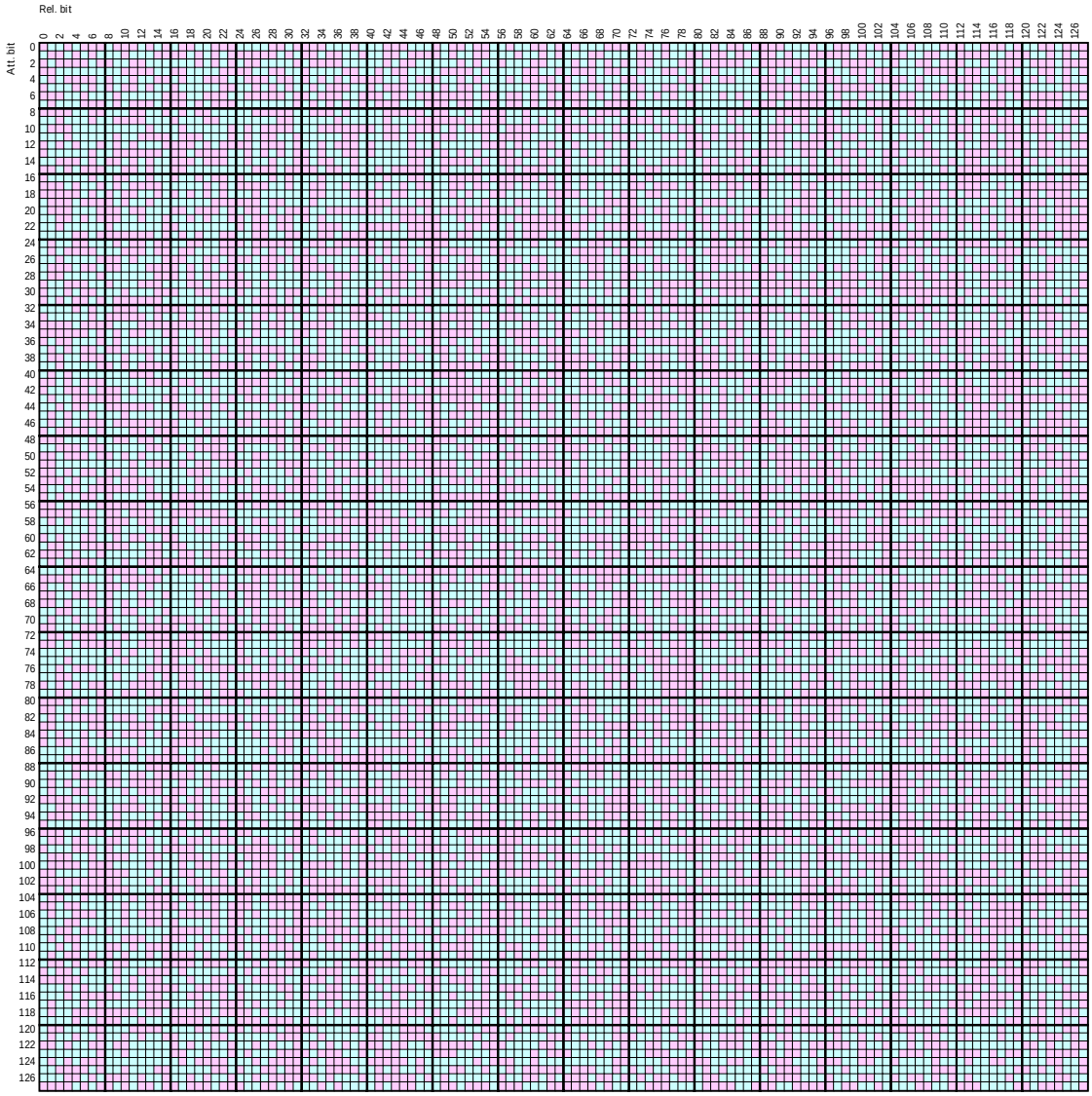
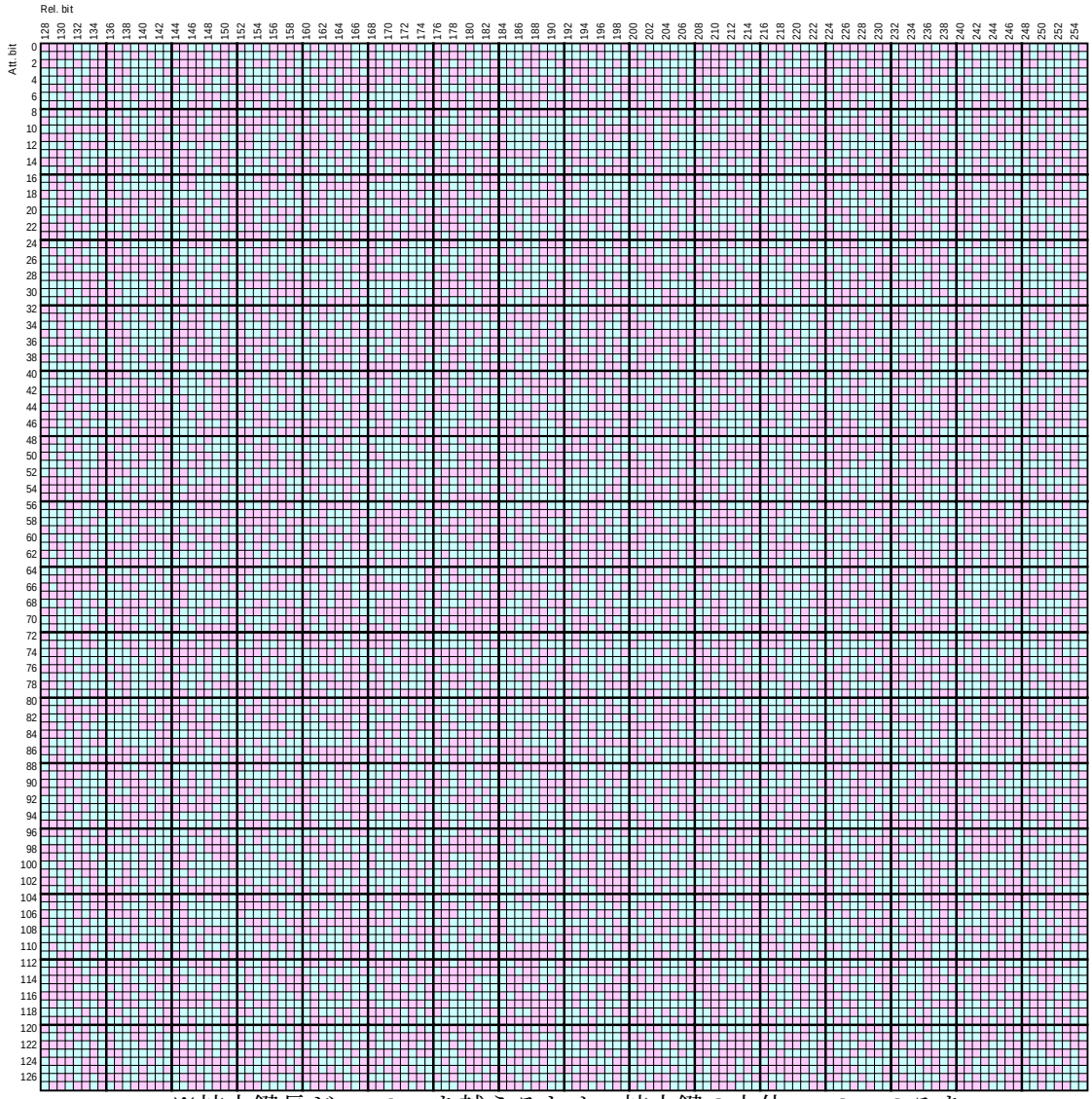


図 B.9.7 RC6 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(1/2)



※拡大鍵長が 256bit を越えるため、拡大鍵の上位 256bit のみを
グラフ表示している。

図 B.9.8 RC6 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(2/2)

B 結果グラフ

B.10 SC2000

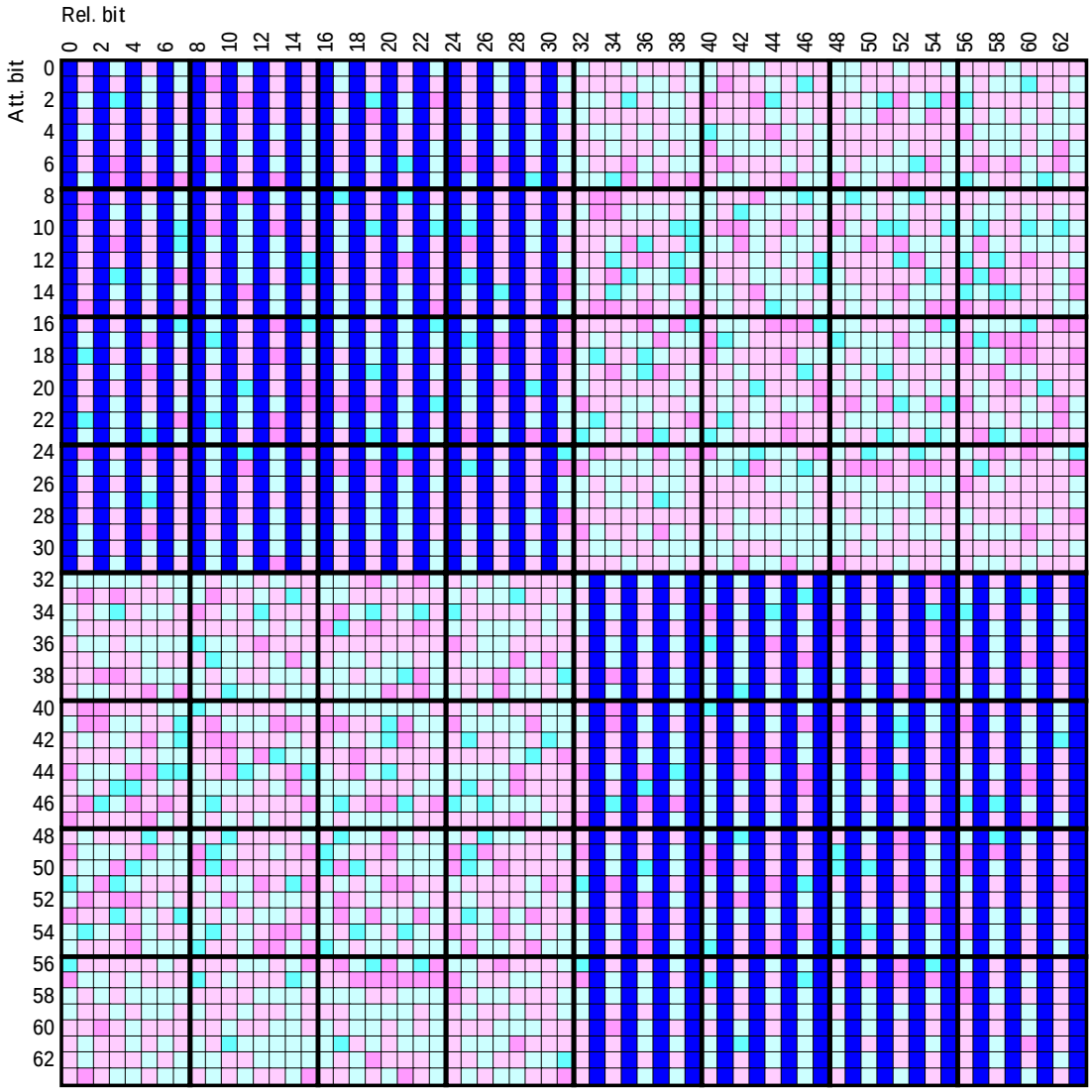


図 B.10.1 SC ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVA

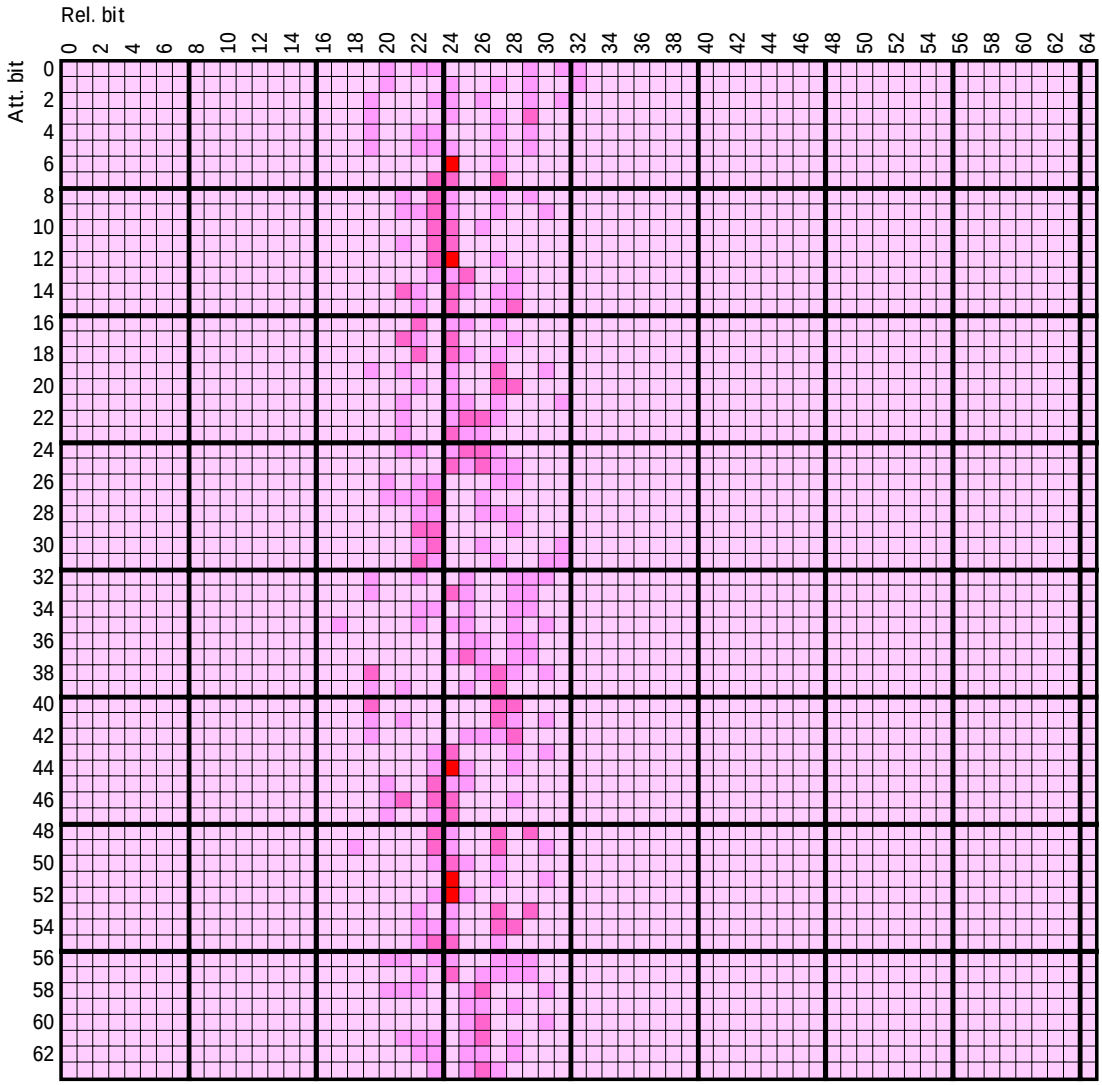


図 B.10.2 SC ﾗｳﾝﾄﾞ関数 入力と出力の相関(Hw=1) AVD

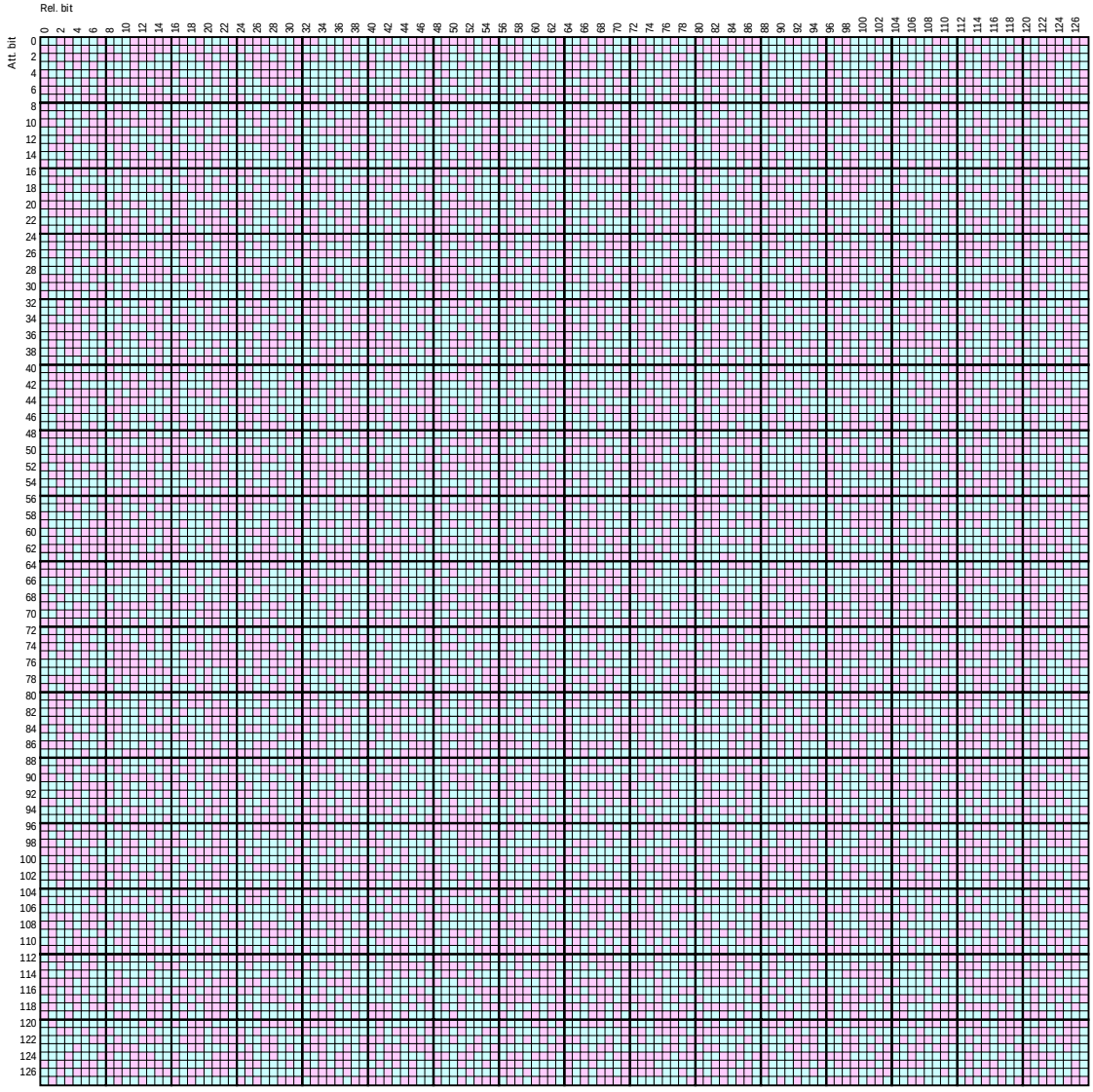


図 B.10.3 SC ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVA

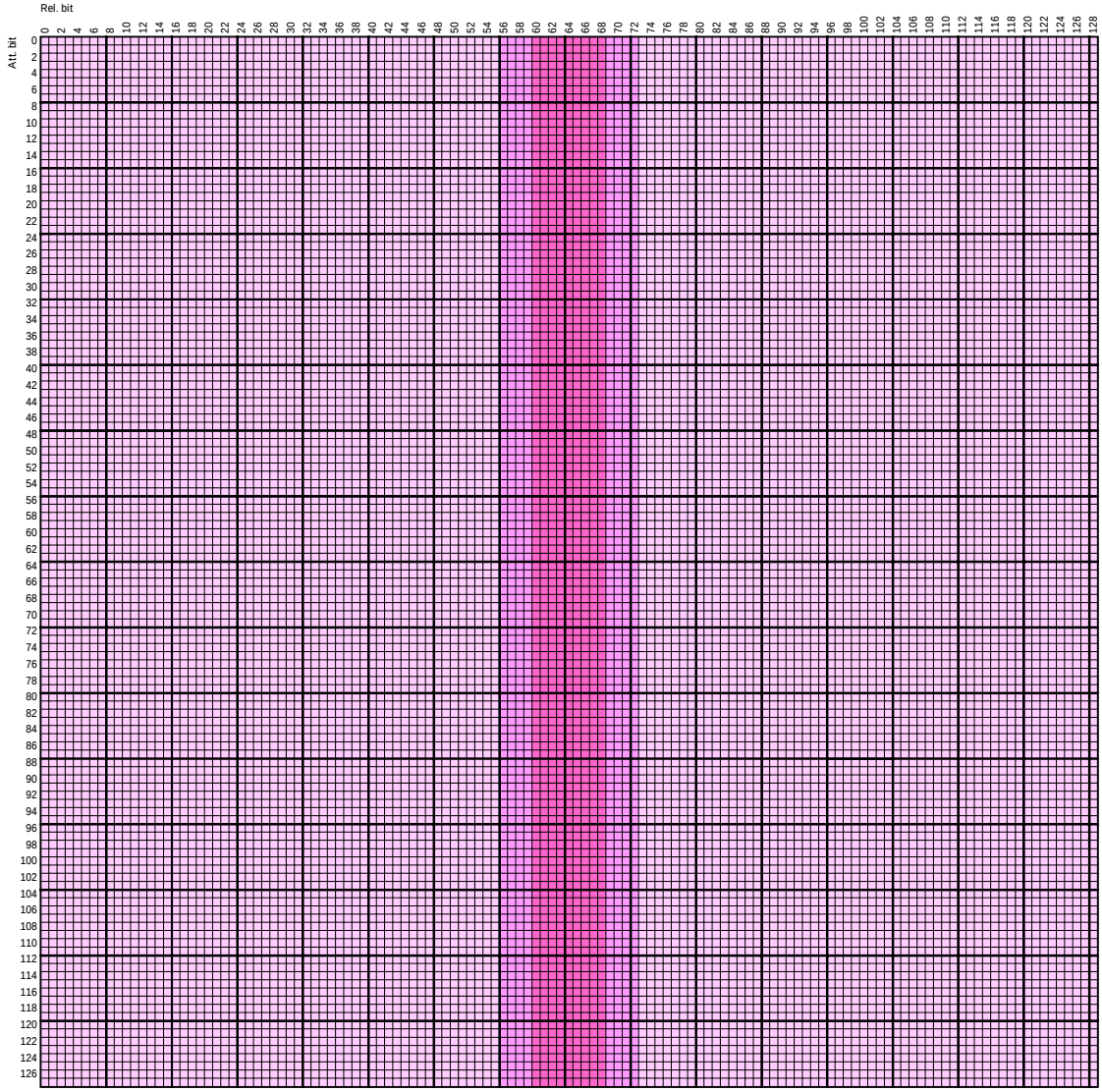


図 B.10.4 SC ﾃﾞｰﾀ攪拌部(128bit) 段数経過(Hw=1) R4 AVD

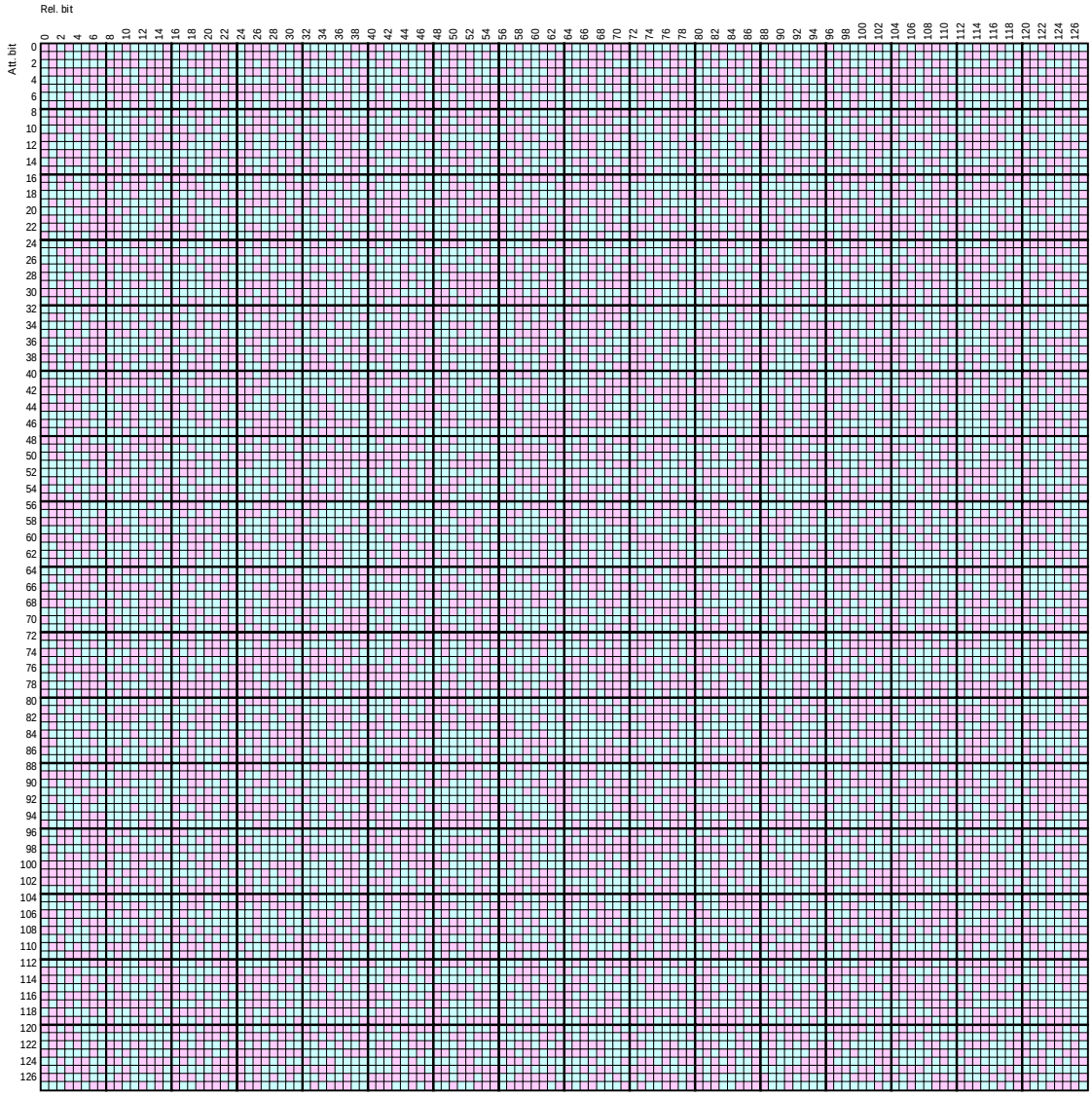
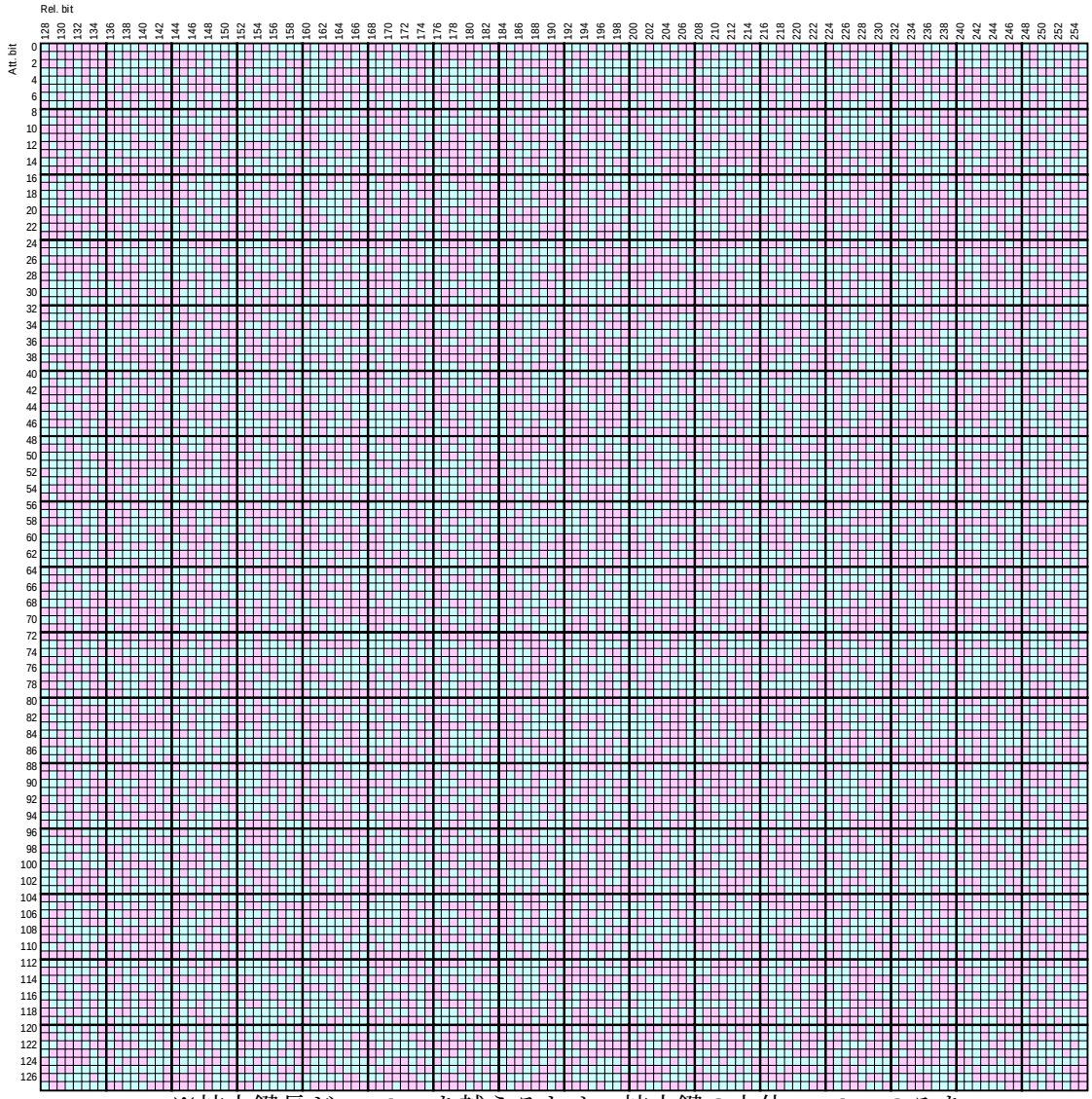


図 B.10.5 SC 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(1/2)



※拡大鍵長が 256bit を越えるため、拡大鍵の上位 256bit のみを
グラフ表示している。

図 B.10.6 SC 鍵ｽｹｼﾞｭｰﾗ(128bit) 秘密鍵と拡大鍵の相関(Hw=1) AVA(2/2)

C 評価対象

C.1 CIPHERUNICORN-E

(1) ラウンド関数

関数名	unsigned int F (int r, unsigned int x)
入力	r:ラウンド番号(=0) x:入力データ(32bit)
鍵	外部変数 EK.fk[r][0]:32bit 外部変数 EK.fk[r][1]:32bit 外部変数 EK.sk[r][0]:32bit 外部変数 EK.sk[r][1]:32bit
出力	関数戻り値(32bit)

(2) データ撹拌部

関数名	void CipherUnicornEncode (unsigned int *p, unsigned int *c)
入力	p:平文データ(32bit×2)
鍵	void CipherUnicornScheduler(unsigned int *k) k:秘密鍵データ(32bit×4)
出力	c:暗号文データ(32bit×2)

(3) 鍵スケジューラ

関数名	void CipherUnicornScheduler (unsigned int *k)
入力	なし
鍵	k:秘密鍵データ(32bit×4)
出力	外部変数 EK:拡大鍵(2624bit)

C.2 FEAL-NX

(1) ラウンド関数

関数名	void FEAL_F (unsigned char *a, unsigned char *b, unsigned char *e)
入力	b:入力データ(8 ビット×4)
鍵	外部変数 e[0]:8 ビット 外部変数 e[1]:8 ビット
出力	a:出力データ(8 ビット×4) 、事前に 0 クリア

(2) データ撹拌部

関数名	void FEAL_encrypt (unsigned char *p, unsigned int r, unsigned char *e, unsigned char *c)
入力	p:平文データ(8bit×8) r:ラウンド数(=32)
鍵	void FEAL_keygen(k, e, r) k:秘密鍵データ(8bit×16) e:拡大鍵データ(8bit×80)
出力	c:暗号文データ(8bit×8)

(3) 鍵スケジューラ

関数名	void FEAL_keygen (unsigned char *k, unsigned char *e, unsigned int r)
入力	r:ラウンド数(=32)
鍵	k:秘密鍵データ(8bit×16)
出力	e:拡大鍵データ(8bit×80)

C.3 Hierocrypt-L1

(1) ラウンド関数

関数名	void hcryptL1_encrypt (unsigned char *in, unsigned char *out, unsigned char *ks) ※最後に 2 回実行している hcryptL1_xs()を除く
入力	in:入力データ(8bit×8) ラウンド数 n=1 とする
鍵	ks:拡大鍵(8bit×16) ks[0][][]に鍵データをセットする
出力	out:出力データ(8bit×8)

(2) データ撹拌部

関数名	void hcryptL1_encrypt (unsigned char *in, unsigned char *out, unsigned char *ks)
入力	in:平文データ(8bit×8)
鍵	void hcryptL1_setkey(key, ks) key:秘密鍵データ(8bit×16) ks:拡大鍵データ(8bit×112)
出力	out:暗号文データ(8bit×8)

(3) 鍵スケジューラ

関数名	void hcryptL1_setkey (unsigned char *key, unsigned char *ks)
入力	なし
鍵	key:秘密鍵データ(8bit×16)
出力	ks:拡大鍵データ(8bit×112)

C.4 MISTY1

(1) ラウンド関数

関数名	void FO_txt (unsigned short a0, unsigned short a1, unsigned short a2, unsigned short a3, int r)
入力	r:ラウンド番号(=0) a0, a1:入力データ(各々16bit)
鍵	外部変数 EXTKEY[0][0](16bit) 外部変数 EXTKEY[2][5](9bit) 外部変数 EXTKEY[3][5](7bit) 外部変数 EXTKEY[0][2] (16bit) 外部変数 EXTKEY[2][1] (9bit) 外部変数 EXTKEY[3][1] (7bit) 外部変数 EXTKEY[0][7] (16bit) 外部変数 EXTKEY[2][3] (9bit) 外部変数 EXTKEY[3][3] (7bit) 外部変数 EXTKEY[0][4] (16bit)
出力	a2, a3:出力データ(各々16bit)、事前に 0 クリア

(2) データ撹拌部

関数名	void misty1 (unsigned char *text, unsigned char *key, int block, int mode)
入力	text:平文データ(8bit×8) block:処理ブロック数(1 固定) mode:暗号化/復号(0 固定)
鍵	FI_key(k) key:秘密鍵データ(8bit×16)
出力	text:暗号文データ(8bit×8)

(3) 鍵スケジューラ

関数名	FI_key (int k)
入力	k:鍵番号(=0-7)
鍵	key:秘密鍵データ(8bit×16)
出力	外部変数 EXTKEY[0][],[1][]:拡大鍵(256bit) ※EXTKEY[2][],[3][]は EXTKEY[1][]と同内容

C.5 Camellia

(1) ラウンド関数

関数名	void Camellia_Feistel (const unsigned char *x, const unsigned char *k, unsigned char *y)
入力	x:入力データ(8bit×8)
鍵	k:拡大鍵データ 8bit×8
出力	y:出力データ(8bit×8)

(2) データ撹拌部

関数名	void Camellia_Encrypt (const int n, const unsigned char *p, const unsigned char *e, unsigned char *c)
入力	n:秘密鍵長(128 or 192 or 256) p:平文データ(8bit×16)
鍵	void Camellia_Ekeygen(n, k, e) n:秘密鍵長(128 or 192 or 256) k:秘密鍵データ(8bit×16 or 24 or 32) e:秘密鍵データ(8bit×272)
出力	c:暗号文データ(8bit×16)

(3) 鍵スケジューラ

関数名	void Camellia_Ekeygen (const int n, const unsigned char *k, unsigned char *e)
入力	n:秘密鍵長(128 or 192 or 256)
鍵	k:秘密鍵データ(8bit×16 or 24 or 32)
出力	e:秘密鍵データ(8bit×272)

C.6 CIPHERUNICORN-A

(1) ラウンド関数

関数名	void F (unsigned long ida, unsigned long idb, unsigned long *k, unsigned long *oda, unsigned long *odb)
入力	ida, idb:(各々32bit)
鍵	k:(32bit×4)
出力	oda, odb:(各々32bit)

(2) データ撹拌部

関数名	void Encode (ulong *p, ulong *c)
入力	p:平文データ(32bit×4)
鍵	void Sche(unsigned long *mk) mk:秘密鍵データ(32bit×LINE) LINE=秘密鍵長/32
出力	c:暗号文データ(32bit×4)

(3) 鍵スケジューラ

関数名	void Sche (unsigned long *mk)
入力	なし
鍵	mk:秘密鍵データ(32bit×LINE) LINE=秘密鍵長/32
出力	unsigned long IK[8] unsigned long EK[16][4]

C.7 Hierocrypt-3

(1) ラウンド関数

関数名	void hcrypt_encrypt (unsigned char *in, unsigned char *out, unsigned char *ks, int key_len) ※最後に 4 回実行している hcrypt_xs()を除く
入力	in:入力データ(8bit×16) key_len:秘密鍵長(key_len=-128:ラウンド数 n=1 とする)
鍵	ks:拡大鍵データ(8bit×32) ks[0][][]に鍵データをセットする
出力	out:出力データ(8bit×16)

(2) データ撹拌部

関数名	void hcrypt_encrypt (unsigned char *in, unsigned char *out, unsigned char *ks, int key_len)
入力	in:平文データ(8bit×16) key_len:秘密鍵長(128 or 192 or 256)
鍵	void hcrypt_setkey(key, ks, key_len) key:秘密鍵データ(8bit×16 or 24 or 32) ks:拡大鍵データ(8bit×288) key_len:秘密鍵長(128 or 192 or 256)
出力	out:暗号文データ(8bit×16)

(3) 鍵スケジューラ

関数名	void hcrypt_setkey (unsigned char *key, unsigned char *ks, int key_len)
入力	key_len:秘密鍵長(128 or 192 or 256)
鍵	key:秘密鍵データ(8bit×16 or 24 or 32)
出力	ks:拡大鍵データ(8bit×288)

C.8 MARS

(1) ラウンド関数

関数名	void E_func (unsigned long Ida, unsigned long *ex1, unsigned long *ex2, unsigned long *ex3, unsigned long *pkey)
入力	Ida:入力データ(32bit)
鍵	pkey:拡大鍵(32bit×2)
出力	ex1, ex2, ex3:出力データ(32bit×3)

(2) データ撹拌部

関数名	void Encode (unsigned long *Idata, unsigned long *Odata, unsigned long *ek)
入力	Idata:平文データ(32bit×4)
鍵	void KeySchedule(length,skey,pkey) length:秘密鍵長(128 or 192 or 256) skey:秘密鍵データ(32bit× 4 or 6 or 8) pkey:拡大鍵データ(32bit×4)
出力	Odata:暗号文データ(32bit×4)

(3) 鍵スケジューラ

関数名	void KeySchedule (unsigned long length, unsigned long *skey, unsigned long *pkey)
入力	length:秘密鍵長(128 or 192 or 256)
鍵	skey:秘密鍵データ(32bit×4 or 6 or 8)
出力	pkey:拡大鍵データ(32bit×40)

C.9 RC6

(1) ラウンド関数

関数名	void Rc6EncryptBlock (unsigned long *S, unsigned char *plaintext,, unsigned char *ciphertext) ※pre-,post-whitening を除く
入力	plaintext:入力データ(8bit×16) [4]-[7],[12]-[15]にデータを入れる [0]-[3],[8]-[11]は 0 クリアする ROUNDS:1 で define する
鍵	S[4]:拡大鍵(32bit×4) S[2],S[3]のみ使用
出力	ciphertext:出力データ(8bit×16) [4]-[7],[12]-[15]に出力データが格納される

(2) データ撹拌部

関数名	void Rc6EncryptBlock (unsigned long *S, unsigned char *plaintext,, unsigned char *ciphertext)
入力	plaintext:平文データ(8bit×16)
鍵	void Rc6ComputeKeySchedule(key,KeyLengthInBytes,S) key:秘密鍵データ(8bit×16 or 24 or 32) KeyLengthInBytes:秘密鍵長(16 or 24 or 32) S:拡大鍵データ(32bit×44)
出力	ciphertext:暗号文データ(8bit×16)

(3) 鍵スケジューラ

関数名	void Rc6ComputeKeySchedule (unsigned char *key, int KeyLengthInBytes, unsigned long *S)
入力	KeyLengthInBytes:秘密鍵長(16 or 24 or 32)
鍵	key:秘密鍵データ(8bit×16 or 24 or 32)
出力	S:拡大鍵データ(32bit×44)

C.10 SC2000

(1) ラウンド関数

関数名	void F_func (unsigned long a, unsigned long b, unsigned long mask, unsigned long *c, unsigned long *d)
入力	a,b:入力データ(32bit×2) mask:マスク値(=0x55555555)
鍵	なし
出力	c,d:出力データ(32bit×2)

(2) データ撹拌部

関数名	void encrypt (unsigned long *out, unsigned long *in, unsigned long *ek, unsigned long keylength)
入力	in:平文データ(32bit×4) keylength:秘密鍵長(128 or 192 or 256)
鍵	void make_key(ekey, ukey, keylength) ekey:拡大鍵データ(ek:拡大鍵データ(32bit×56 or 64) 128bit 時 56 個, 192 or 256bit 時 64 個 ukey:秘密鍵データ(32bit×4 or 6 or 8) keylength:秘密鍵長(128 or 192 or 256)
出力	out:暗号文データ(32bit×4)

(3) 鍵スケジューラ

関数名	void make_key (unsigned long *ekey, unsigned long *ukey, unsigned long keylength)
入力	keylength:秘密鍵長(128 or 192 or 256)
鍵	ukey:秘密鍵データ(32bit×4 or 6 or 8)
出力	ek:拡大鍵データ(32bit×56 or 64) 128bit 時 56 個, 192 or 256bit 時 64 個