SASEBO の電力解析攻撃実験

Power Analysis Attacksts on SASEBO

2010 年 1 月 6 日

(独) 産業技術総合研究所
情報セキュリティ研究センター

目次

1 概要

標準評価ボード SASEBO-R および SASEBO-G を用い，ASIC および FPGA 上の暗号回路に対するサイドチャネル攻撃評価実験を行った．評価実験の対象となる SASEBO-R に搭載した暗号 LSI と SASEBO-G 上の Xilinx 社製 FPGA Virtex-2 は異なる半導体製造プロセスにより製造されているものの，いずれも 1.2V の 130nm CMOS プロセスが使用されている．

共通鍵ブロック暗号は 128 bit 鍵の AES を対象としている．SASEBO-R 上の暗号 LSI の回路は，S-box を 1 段の PPRM (Positive Porarity Reed-Muler) 論理で実装した AES を対象に，6 種類の攻撃手法を適用した．また SASEBO-G 上には，「標準暗号 LSI 仕様書 ～サイドチャネル攻撃対策版～ 第 1 版」の暗号 LSI と同じソースコードの各種対策版 AES 回路を実装して攻撃を行った．それらは，合成体による S-box を用いた AES4，それをベースにして DPA 対策を施した AES8 (MAO)，AES9 (MDPL)，AES11 (WDDL)である．なお，AES10 (Threshold Implementation)は電源系統の問題で安定動作しなかったため，今回は評価実験を見送った．また，公開鍵暗号は 1,024 bit の RSA 暗号を SASEBO-R 上の LSI 実装および SASEBO-G 上の FPGA 実装に対して，様々な入力データパターンを用いた SPA 攻撃を行った．以下それら攻撃手法と，実験結果について解説を行う．

2 AES への電力解析攻撃

2.1 攻撃手法

表 1 に AES の回路実装に適応することができる，代表的な電力解析攻撃手法を示す．今回の攻撃実験では，「標準暗号 LSI 仕様書 ～サイドチャネル攻撃対策版～ 第 1 版」で解説しているループアーキテクチャの AES 回路を対象としており，図 1 に示したように消費電力に 11 のピーク波形が見えるときに，最終 10 ラウンド目および，データ出力時のレジスタのスイッチングによって発生する電力波形の区間を対象に解析を行う．

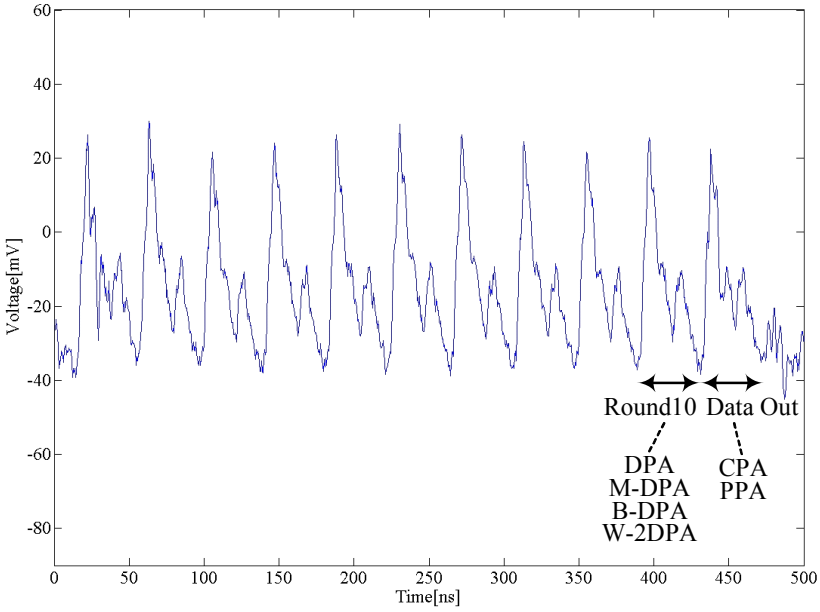

図 1 各攻撃法の対象となる SASEBO-R の AES 回路(PPRM1)の電力波形区間

表 1 AES 回路に対する攻撃法

攻撃手法	特徴	攻撃区間
DPA	推定する部分鍵に対応した中間値の特定の 1 ビットの値によって 2 組に分けた, 電力波形の平均の差を計算し, その平均波形とビット値の相関を調べる. 最も基本的かつ汎用的な攻撃.	10 ラウンド
M-DPA	推定する部分鍵に対応した中間値の複数ビットを用い, そのハミング重みが閾値以上であるか否かによって, 電力波形を 2 組に分類するする. その電力波形の平均の差を計算して, ハミング重みとの相関を調べる. 攻撃精度は回路の実装法に大きく依存する.	10 ラウンド
B-DPA	推定する部分鍵に対応した中間値の複数ビットに対する DPA の結果を結合する汎用的な攻撃.	10 ラウンド
CPA	推定する部分鍵に対応した中間値を格納するレジスタが遷移したときのハミング距離と消費電力の関係を調べる. 未対策の回路であれば, B-DPA の 1/10 以下の波形数で攻撃可能.	データ出力
PPA	CPA の拡張でハミング距離に重み付けを行うが, その効率的な係数の設定方法は提案されていない.	データ出力
M2-DPA	電力波形の中のある 2 つの区間の相関を解析する攻撃法. 攻撃精度は実装に依存する.	10 ラウンド
W2-DPA	DPA が平均波形の差を求めるのに対して, 2 乗平均の差を計算する汎用的な攻撃.	10 ラウンド

以下, 各攻撃手法について概説を行う. 式(1)はそれらで用いる記号の意味を示しており, $G_{condition}$ は条件を満たす電力波形の集合を, $N_{condition}$ はその集合に含まれる波形の個数を, そして $\overline{W}_{condition}$ は条件を満たす波形の平均を表す.

$$\begin{cases} G_{condition} = \{W_i, i \in 1...N \mid condition\} \\ N_{condition} = card(G_{condition}) \\ \overline{W}_{condition} = \sum_{G_{condition}} W_i / N_{condition} \end{cases} \quad (1)$$

- **Differential Power Analysis (DPA)**

Kocher らによって提案された DPA[1)]では秘密鍵の推定に次式の平均差分電力を評価する.

$$\Delta(b) = \overline{W}_{b=1} - \overline{W}_{b=0} \quad (2)$$

ここで, bは暗号アルゴリズムにおける中間変数のビット値で, $\Delta(b)$ は, b=1 および b=0 のときの平均電力波形の差を意味し, DPA トレースと呼ばれる. DPA では, 既知の平文あるいは暗号文と部分鍵の予測値から中間変数のビット値 b を計算する. 以下ではこのbを“選択ビット”と呼ぶ. また, $\Delta(b)$ は複数の鍵候補の中から, 正しい鍵を選択するための“選択関数”と呼ばれる. AES 実装に対最も一般的な攻撃では, 最終ラウンドの 1byte の部分鍵 $\boldsymbol{k}$ を予測し, それに対応する既知の暗号文の 1byte データ $\boldsymbol{c}$ から,

$$\boldsymbol{b} = \{b_7, \cdots, b_1, b_0\} = S^{-1}(\boldsymbol{c} \oplus \boldsymbol{k}) \quad (3)$$

を計算する. ここで S^{-1} は AES の関数 InvSubBytes で用いる 8bit の S-box である. 8bit の部分鍵 $\boldsymbol{k}$

の 256 通り全てのパターンに対して $\Delta(b)$ を計算し，その絶対値が最大となる $\boldsymbol{k}$ を正解鍵とする．この DPA の例では，選択ビットとして $\boldsymbol{b} = \{b_7, \cdots, b_1, b_0\}$ の 8 つのビット値から 1 つを選んで $\Delta(b)$ を計算するが，どのビットも同一の部分鍵の導出に用いることが可能である．

論理回路に対する DPA は，選択ビットとして設定した回路上のノードの値によって，消費電力に差が発生する場合に攻撃が成立する．例えば文献 [2]では，NAND や NOR といった非線形ゲートの入力を選択ビットとした場合に，その非線形ゲートを含めた後段の論理回路の遷移確率に偏りが生じることが示されている．また文献 [2] [3] [4]では，DPA は論理回路でランダムマスク法や，相補論理を実現する対策回路に対しても有効に働く可能性があることが示されている．特に文献 5)では，ランダムマスク法を実現した ASIC 回路に対して DPA が成功した例が示されている．式(3)による選択関数では，出力される暗号文から，その直前の演算の部分鍵を推定するため，最終ラウンド処理で発生する消費電力波形を用いる．また，暗号化の対象となる平文を選択的に設定可能であれば，1 ラウンド目の SubBytes 出力またはその線形変換を用いた選択関数が設定できることが文献 6)で示されている．

- **Messerges' multi-bit DPA**

式(1)の拡張として，複数の選択ビットを用いるマルチビット DPA と呼ばれる攻撃手法(以下，M-DPA と略記する)がいくつか提案されている [7] [8]．文献 7)で Messerges らは式(4)に示したように，d ビットの選択ビットのハミング重み H_W が $d/2$ 以上であるか否かで電力波形のグループ分けを行う手法を示している．

$$\begin{cases} G_0 = \{W_i, i \in 1...N \mid H_W(\boldsymbol{b}) < d/2\} \\ G_1 = \{W_i, i \in 1...N \mid H_W(\boldsymbol{b}) \geq d/2\} \\ \Delta(Hw(\boldsymbol{b})) = \overline{W}_{G_1} - \overline{W}_{G_0} \end{cases} \tag{4}$$

M-DPA の攻撃精度が DPA よりも向上するケースは，論理回路の消費電力の大小が，選択関数として設定した複数のビット値によって決定まる場合である．DPA と異なり，差が発生するだけでは攻撃精度の向上につながらないことに注意が必要である．例えば．選択関数として式(.3)を用いる場合，$\boldsymbol{b} = \{b_7, \cdots, b_1, b_0\}$ のどのビットにおいても，その値 0，1 によって消費電力の大小が同じ傾向を示す必要がある．つまり，b_0 が 0 よりも 1 のときの消費電力が大きいならば，他のビットも 1 のときに消費電力が大きくなること，言い換えれば，DPA トレース $\Delta(b)$ の極性が，選択関数のビット位置に依存せず常に一定であることが攻撃精度の向上に重要である．このような現象は，SubBytes 関数を AND-XOR の 2 段論理で構成するような場合が主であるため，論理回路に対する M-DPA はその攻撃対象が DPA よりも限定されると考えられる．

- **Bevan's multi-bit DPA**

Bevan らは，式(5)のように複数の選択ビットで計算された DPA トレースの絶対値の和を用いる攻撃法を提案している [8]．以下ではこの式を用いた攻撃手法を B-DPA と略記する．

$$\sum_{b_i \in \boldsymbol{b}} |\Delta(b_i)| \tag{5}$$

B-DPA ではまず，設定可能な複数の選択ビットを用いて DPA を行い，その結果を式(5)で結合する．B-DPA が DPA よりも攻撃精度が向上するケースは，選択関数として設定した複数のビット値によって，論理回路の消費電力に差が生じる場合である．M-DPA のように，ビット値によって消費電力の大小関係が決定する必要はないが，消費電力に差が生じる選択ビットが少ないと DPA よりも攻撃精度が低下する．

- **Correlation Power Analysis**

Correlation Power Analysis(以下 CPA と略記する) は, Brier らによって提案された強力な攻撃法である [9]. CPA では, 部分鍵 $\boldsymbol{k}$ の予測よって計算可能なレジスタのハミング距離 H_D と, 対応する電力波形の相関を式(6)によって計算する.

$$\begin{cases} G_j = \{W_i, i \in 1...N \mid H_D(\boldsymbol{b}) = j\} \\ \sigma_{W,H_D} = \sum_{j=0}^{d} j \cdot N_j \cdot \overline{W}_j - \overline{W} \cdot \overline{H_D(\boldsymbol{b})} \\ \rho(\boldsymbol{b}) = \dfrac{\sigma_{W,H_D}}{\sigma_W \sigma_{H_D}} \end{cases} \tag{6}$$

ここで, d は予測した鍵によってその値が計算できるレジスタ長で, 電力波形をレジスタ値のハミング距離 0~d の d+1 個のグループに分類する. CPA では $\rho(\boldsymbol{b})$ が最大となる $\boldsymbol{k}$ を正解鍵とする. レジスタの変化前・変化後の値をそれぞれ $\boldsymbol{x}$, $\boldsymbol{y}$ とし, $H_W(\boldsymbol{x})$ を $\boldsymbol{x}$ のハミング重みとすれば, $H_D(\boldsymbol{b}) = H_W(\boldsymbol{x} \oplus \boldsymbol{y})$ となる. なお, $\boldsymbol{x}$, $\boldsymbol{y}$ は既知の暗号文出力(または平文出力) と予測した部分鍵 $\boldsymbol{k}$ から計算できる値である.

CPA が成功するためには, ハミング距離を算出するレジスタに接続される論理回路の消費電力が, そのレジスタの遷移するビット数と相関を持つ必要があり, この条件は一般の論理回路で成立する. ただし, 解析の計算量の問題から, ハミング距離の算出に用いる部分鍵は 8~16bit 程度とする. AES の CPA における選択関数として最も一般的なのは, 次式の 8 ビット関数である.

$$H_D(\boldsymbol{b}) = H_W(S^{-1}(\boldsymbol{c}_i \oplus \boldsymbol{k}_i) \oplus \boldsymbol{c}_j) \tag{7}$$

ここで, c_i と c_j は暗号文出力(または平文出力)のある byte で, 関数 ShiftRows(または InvShiftRows) によって j 番目の位置が i 番目に移動する場合の式となる. この選択関数が有効となるには, 9 ラウンド目の中間値と 10 ラウンド目の結果(つまり暗号文出力または平文) が同じレジスタに格納される必要がある. 式(7)では, 式(3)の DPA で用いる電力波形から 1 サイクル遅れたものを用いる. これは, 式(7)の遷移は, 暗号文(または平文) がレジスタに格納されたときに発生するためである.

- **Partitioning Power Analysis**

Partitioning Power Analysis(以下 PPA と略記する) は, Le らによって提案された CPA を拡張した攻撃法で [10], 式(8)に示されるように, 攻撃対象に応じて攻撃者がハミング距離毎に重み付け a_j を設定する. 解析対象に応じて変更することで, ハミング距離と電力波形の関係をより柔軟に設定できる特徴を持つ. 効率のよい重みの設定方法は文献 10)では今後の課題としている. 攻撃原理は CPA と同じであるが, 式(6)と異なり, 式(8)では正規化を行っていない.

$$\begin{cases} G_j = \{W_i, i \in 1...N \mid H_D(\boldsymbol{b}) = j\} \\ \Sigma_H(\boldsymbol{b}) = \sum_{j=0}^{d} a_j \cdot \overline{W}_{G_j} \end{cases} \tag{8}$$

- **Messerges' Second-Order DPA**

Messerges は DPA を拡張し, ある 2 サイクル間の消費電力に着目した式(9)の選択関数を用いる 2 次の DPA(以下 M2-DPA と略記する) を提案している. ここで, $\overline{W}_{t,condition}$ は条件を満たす t サイクル目の電力波形の平均である.

$$\begin{cases} \overline{S}_0 = \left| \overline{W}_{t,b=0} - \overline{W}_{t',b=0} \right| \\ \overline{S}_1 = \left| \overline{W}_{t,b=1} - \overline{W}_{t',b=1} \right| \\ \Delta_{2\mathrm{nd}}(\boldsymbol{b}) = \overline{S}_1 - \overline{S}_0 \end{cases} \tag{9}$$

M2-DPA は, ランダムマスクによる対策を施した実装をターゲットとした攻撃手法である. ソフトウェア実装において, t サイクル目に平文 $\boldsymbol{P}$ と乱数 $\boldsymbol{R}$ が XOR され, t'サイクル目に t サイクル目の結果に対して鍵 $\boldsymbol{K}$ が XOR される場合, t サイクル目と t'サイクル目の消費電力の差に着目することで, 乱数 $\boldsymbol{R}$ の効果を打ち消すことができるとされる. 論理回路においても, 乱数のマスクを実行するサイクルと鍵加算のサイクルが分離できれば適応可能である. しかし, AES 回路への攻撃は対策手法に依存するため一般化することはできない.

- **Waddle's Zero-Offset Second-Order DPA**

Waddle らは文献 [12]で, DPA を拡張した 2 次の DPA を複数提案している. その中で最も基本的な攻撃手法である Zero-Offset 2DPA(以下 W2-DPA と略記する) は, 式(10)で定義される. DPA では選択ビットに対する平均波形の差を計算するのに対し, W2-DPA では 2 乗平均の差を計算している. 乱数などを用いて平均波形を選択ビットに依存せず一定にするような対策をとっても, 選択ビットに依存して電力波形の分散が異なる場合は, W2-DPA で攻撃できる可能性がある.

$$\begin{cases} \overline{W}^{(2)}_{condition} = \Sigma_{G_{condition}} (W_i)^2 / N_{condition} \\ \Delta_{2\mathrm{nd}}(\boldsymbol{b}) = \overline{W}^{(2)}_{b=1} - \overline{W}^{(2)}_{b=0} \end{cases} \tag{10}$$

2.2 実験結果

表 3 に, AES の電力解析攻撃実験時の測定条件を示す. 電力波形は暗号 LSI および FPGA のコア電源側に挿入したそれぞれ 3.3 Ωおよび 0.1 Ω抵抗の両端の電位差を測定している. AES 回路の FPGA への実装には Xilinx ISE 9.2i を用いている. AES の実装法あるいは攻撃法に応じて, 平文入力はランダムに与えながら 1 万サンプルまたは 10 万サンプルの電力波形を取得し, 最終ラウンドの 16 byte のラウンド鍵を S-box 毎に解析した. DPA では各 S-box に対応する 8bit それぞれに対して 8 つの平均差分電力波形を求めた後, その波形を加算している. また PPA では 8bit 単位で決まるハミング距離 0~8 に対して, 式(8)の重み付け $a_0 \sim a_8$ を–8, –6, –4, –2, 0, 2, 4, 6, 8 として相関値を求めた.

表 3 測定条件

項目		条件
デジタルオシロスコープ		Agilent MSO8104A
サンプリング周波数		2GSample/sec
プローブ		Agilent 1130A
プローブヘッド		Agilent E2695A SMA
安定化電源		3.3 V
動作クロック周波数		24 MHz
電圧測定ポイント	暗号 LSI	コア電源側に挿入した 3.3 Ω抵抗の両端
	FPGA (xc2vp30)	コア電源側に挿入した 0.1 Ω抵抗の両端
秘密鍵		2B 7E 15 16 28 AE D2 A6 AB F15 88 09 CF 4F 3C
攻撃対象の最終ラウンド鍵		D0 14 F9 A8 C9 EE 25 89 E1 3F 0C C8 B6 63 0C A6

- **SASEBO-R 上の暗号 LSI への攻撃**

暗号 LSI は, 各攻撃法の性能比較を主目的に, 最も消費電力が大きく攻撃が容易であった AND-XOR ロジックである 1 段の PPRM 論理による S-box を用いた AES2(PPRM1)を対象に, DPA, CPA, W2-DPA, M-DPA, M2-DPA, PPA の 6 つの攻撃を行った.

図 2-1/-2 は 1 万波形による DPA 結果で, 16 個の S-box(S0 が MSB 側, S15 が LSB 側) それぞれに対応する 8bit の部分鍵候補の平均差分出力 (相関値) を示している. 全ての S-box において明確な相関値のピークが現われ, 鍵の推定が正しく行われている. また, 図 3-1/-2 は横軸の波形数の増加に伴う, 正しい鍵の推定順位(平均差分電力の大きさの順位)の変動を縦軸に log スケールで示している. S-box による違いはあるものの, 極めて早い段階(少ない波形数)でほとんどの部分鍵が正しく推定される様子が分かる.

図 4-1/-2 と図 4-1/-2 は, 同じ条件での CPA の結果である. DPA と同様に全ての部分鍵が早い段階で正しく推定されているが, 全体的に DPA よりもやや少ない波形数で攻撃が成功している. また, 両者の S0 や S10 の鍵の推定精度のグラフの比較から, 情報のリーク量は S-box によって一意に決まるのではないことがわかる. 攻撃法によって決まる電力モデルに, その実装が合っているかどうかが攻撃の精度向上に重要である. 暗号アルゴリズムの詳細な実装法が公開されることは通常なく, また同じ Verilog-HDL コードから合成された 16 個の S-box でも, この実験のように推定精度にばらつきが生じ, さらに鍵やデータのパターンによっても差が生じるため, 安全性評価には, 様々な電力モデルに基づく攻撃法を試す必要があることがわかる.

図 6~9 は S0 に対する W2-DPA, M-DPA, M2-DPA, PPA の解析結果である. ベースとなる DPA と CPA が高い精度で成功しているため, これらの攻撃法も同様の結果となっている. 今回の 1 段の PPRM 論理を用いた S-box 実装に対しては, 全ての部分鍵を 1,000~4,000 程度の波形で正しく推定することができた. また, 暗号 LSI 上のその他の S-box 実装を用いた AES 回路(全て DPA 対策なし)に対しても, 波形数の差こそあれ鍵の導出を行うことに成功している.

- **SASEBO-G 上の FPGA 実装への攻撃**

図 10 以降は, SASEBO-G 上の FPGA に実装した AES 回路に対する攻撃実験結果である. SASEBO-G 上の xc2vp7 が本来は暗号回路を実装用の FPGA であるが, AES 回路に対策を施すと規模が増大して載らないものが出てきた. そこで通常は制御 FPGA として使用している右側の xc2vp30 に, 合成体上の S-box を用いた各種 AES 回路を実装して実験を行った. なお, 最大の回路規模となった DPA 対策版 Threshold Implementation はこの FPGA 上に実装することはできたものの, コア電圧の変動が大きく安定して動作しなかったため, 今回は評価対象から外すこととした.

図 10~15 は DPA 対策を施していない AES 回路に対して, DPA, W2-DPA, CPA をそれぞれ, 10 万波形, 10 万波形, 1 万波形で解析を行った結果である. 暗号 LSI の場合と比較して攻撃の精度が低いのは, 電力波形の S/N 比の低下が主な理由であると思われる. このように, 波形の質が悪い場合に, CPA は大きな効果を発揮し, DPA, W2-DPA と比べて 1 桁以上高い精度を示している.

図 16~23 は Masked-AND Operation (MAO)対策を施した AES 回路に対する, DPA, W2-DPA, CPA の結果で, 波形数は無対策版と同様にそれぞれ 10 万波形, 10 万波形, 1 万波形である. 図 16~17 の DPA では, 全ての S-box において鍵の推定に失敗している. しかしながら, 加算する前の 8 つの平均差分波形を個別に解析した結果, 複数の S-box において入力の bit-1 と bit-6 が DPA に対して弱いことが分かった. そこでこの 2 bit だけを用いて DPA を行った結果を図 18~19 に示す. 6 つの S-box S2, S3, S4, S9, S10, S13 で鍵の推定が正しく行われていることが分かる. 暗号モジュールを攻撃する第三者は, 正しい鍵を基にこのように選択関数を構成することは困難であるが(自分が保有するモジュールに自ら鍵を設定できる場合は, それを基に解析した結果を使って, 他者が保有するモジュールを攻撃することは可能), 安全性の評価試験においては, このように正しい鍵の知識を用いてモジュールの脆弱性を検証することも重要である. また, 正解鍵が 1 位でなくとも上位に位置している場合は, その実装が何らかの脆弱性を有し, 波形数の増加に従って鍵推定の精度が向上する可能性がある.

Masked-AND は 1 ビットの乱数が複数の信号に関与するため，それらの相関から W2-DPA も原理的には成功する可能性があるが，図 20~21 に示すように，今回の実験では正解鍵は得られなかった．信号の遅延差が大きいことやサンプル数が不十分であるといった原因が考えられる．また図 22~23 の CPA は，データのマスクによってハミング距離を正しく計算することができないため，まったく攻撃できていない．選択関数のモデルが実装とまったく合っていないため，波形数を増やしても結果は変わらないと考えられる．また，同じ Verilog-HDL コードを SASEBO-G に実装し，異なる測定環境で行った 10 万波形による CPA 実験でも攻撃に失敗している．

図 24~29 は WDDL 版の AES 回路に対する攻撃結果である．図 24~25 は休止相(Precharge)に対する DPA，図 26~27 は稼働相(Evaluation)に対する DPA で，それぞれ 10 万波形で解析を行っている．そして図 28~29 は，1 万波形による稼働相での CPA の結果である．DPA は休止相，稼働相共にいくつかの S-box で攻撃に成功している．WDDL はどのような入力に対しても対となる信号線の一方にスイッチングを発生させることで，データに依存した消費電力の差をなくす対策法である．しかし，信号線対に関与する AND や OR といった基本ゲートのスイッチング速度に差があり，また配線を含めた寄生容量や抵抗にもばらつきがあるため，実際の回路ではこのような情報のリークが生じる．特に S6 と S15 では，休止相および稼働相の双方で極めて大きなリークが生じていることがわかり，回路上で信号線対のバランスが大きく乱れていると考えられる．また，Masked-AND の時と同様に，リークが大きいビットだけ選択して加算することによって，さらに精度の高い鍵推定が可能となると思われる．

CPA は基本演算のビット幅(この実験では S-box の 8 bit)に応じて，レジスタや信号線のスイッチングによるハミング距離を用いる攻撃であるが，WDDL の稼働相の実験においてはハミング重みを使用した．これは，休止相で信号対がプリチャージされるため，前の演算結果と今回の演算結果の差によってレジスタのスイッチングが起こるのではなく，レジスタは毎回同じ値に設定された状態から演算結果に変化し，つまり演算結果のハミング重みがハミング距離となるからである．WDDL ではペアになる AND/OR ゲートの出力遅延差などから，有意な電力差が現れる可能性があるが，遅延の大小関係はビット毎にまちまちであるため，8bit 単位のハミング距離(=ハミング重み)と消費電力の相関は低く，逆にビット毎に打ち消し合う可能性がある．図 28~29 の結果においては正解鍵の導出に失敗しているが，S10 や S15 では波形数の増加に伴って，正解鍵の順位が向上しているようにも見える．また，今回の実験の CPA は 1 万波形しか用いていないが，同じ Verilog-HDL コードを SASEBO-G に実装し，異なる測定環境で行った 10 万波形による実験では DPA よりも精度は劣るものの CPA でも攻撃に成功している．

図 30~35 は，MDPL 版の AES 回路に対する DPA および CPA の攻撃結果を示している．WDLL と同様に，DPA は 10 万波形を用いて休止相(図 30~31)と稼働相(図 32~33)に対して，CPA は 1 万波形で稼働相(図 34~35)に対する攻撃を行った．MDPL は消費電力が大きく，本実験では電力波形の S/N 比は非常に悪いため，いずれの攻撃も失敗しており，また正解鍵に対する解析波形を個別に調べても有意な情報を見分けることはできなかった．しかしながら，同じ Verilog-HDL コードを SASEBO-G に実装し，異なる測定環境で行った 10 万波形による DPA および CPA 実験では，DPA においていくつかの bit の選択関数で正しい鍵の導出が行われているものがあった．一方，CPA は 10 万波形でも攻撃に失敗していた．波形数を 100 万に増やせば CPA でも鍵推定に成功する可能性はあるが，安全性評価の方針としては，一つの攻撃法に対して脆弱性を持つことが示されればそれ以上の解析は不要である．

- **AES 回路に対する対策法と攻撃法のまとめ**

上記の実験結果から，未対策の AES 回路に対しては，データのスイッチングに着目したハミング距離と消費電力の相関を用いる CPA の攻撃の精度が，他の攻撃法に比べて非常に高いことが分かる．しかし，対策を施した回路に対しては，そのモデルがうまくマッチしなるため，精度が極端に低下している．一方，最も基本的な解析手法である DPA は，モデルがシンプルなため各種対策法に適用でき，高い効果を発揮している．しかし，これは攻撃対象の電力モデルがわからない場合で

あり，評価試験においては，対策を含めた実装方式の情報を入手することも可能であると考えられる．したがって，その情報を利用して実際の回路の特徴をとらえた電力モデルを構成することができれば，より精度の高い攻撃(＝評価)も可能となる．

FPGA に実装した対策手法は，いずれも電力解析を困難とする効果があり，今回の実験においてはその強さは

MDPL > MAO > WDDL

となっていた．しかし，いずれの対策法も，遅延時間の制御や寄生容量･抵抗のバランスを保つことが前提となっており，FPGA 実装ではそこまで制御することは極めて困難である．したがって今回の実験は，各対策法が必ずしもこの順序で強いことを示しているわけではなく，また十分な波形数が得られれば必ず DPA で破ることができるというわけでもない．さらに対策法のアルゴリズムによる効果だけでなく，波形の S/N 比も解析結果を大きく左右するため，実装形態や計測環境を含めた安全性の評価も重要である．

安全性評価が攻撃と大きく異なる 2 点を再確認すると，

1. 実装方式の情報が得られる
2. 正解鍵があらかじめ分かっている

となる．これらの情報を用いることで，MAO に対する DPA で bit-1 と bit-6 を用いたように，正解鍵から逆に，消費電力モデルを構築することも可能である．このように攻撃者よりも有利な立場での解析においても脆弱性が見つからなければ，その実装は極めて安全性が高いと言える．逆にそのような解析で対策手法に脆弱性が見つかったからと言って，必ずしも危険な実装，無効な対策法というわけではなく，無対策の場合に対して攻撃のコストを増大させることができるのであれば，有効な手法であることになる．例えば，100 万波形集めれば必ず正解の鍵を導出できることが一般に知られてしまっている実装は非常に危険である．その一方，実装情報を利用し，既知の鍵に対して 1 万波形集めた評価実験で特定の bit に部分鍵の情報が漏れていることがわかったとしても，その性質を用いなければ100万波形でも正解にたどりつけないのであれば安全な実装であると言ってもよいであろう．したがって，安全性評価においては，評価者が知り得る情報にアクセスできない場合の，攻撃のコストを考慮することも重要である．

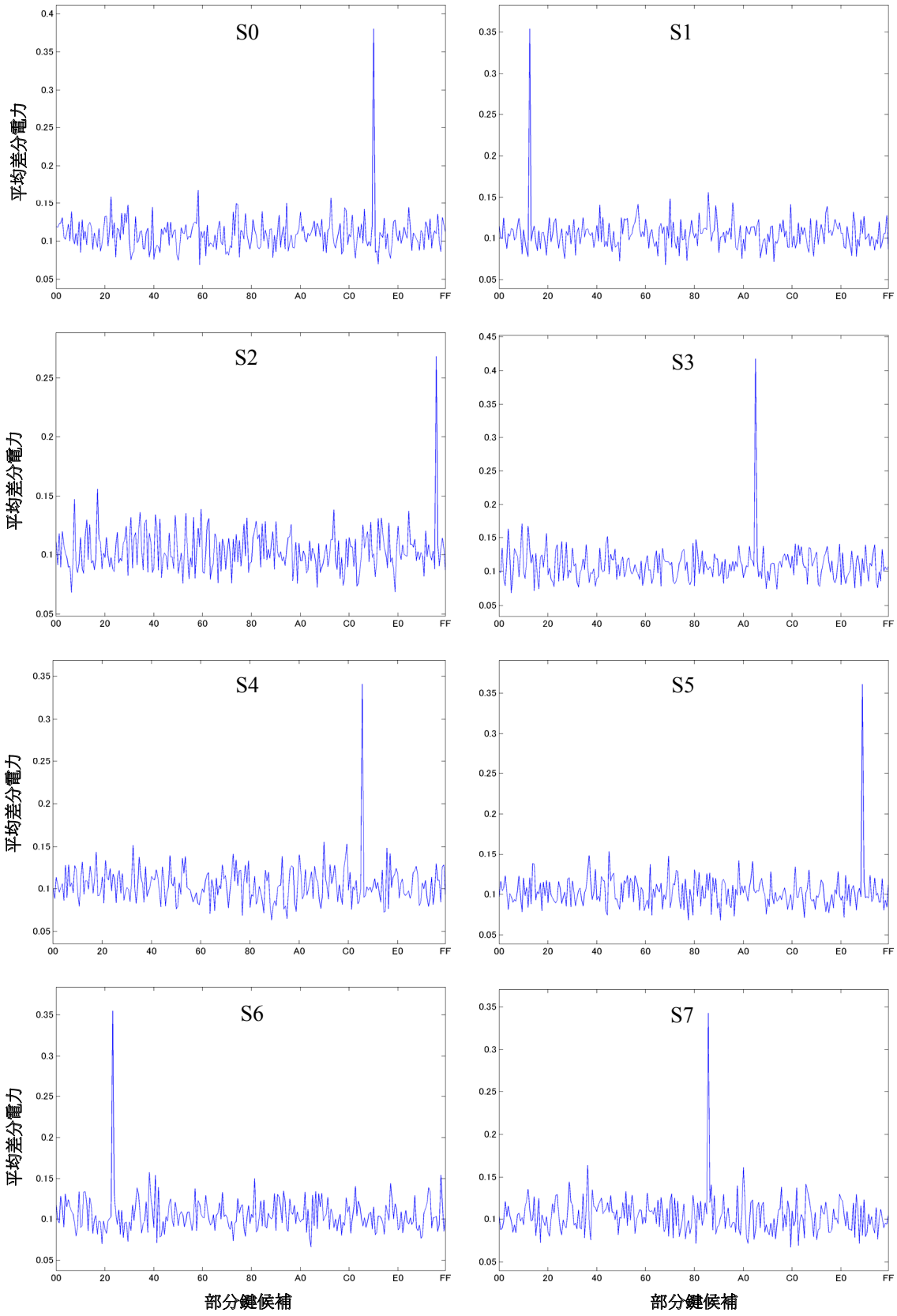

図 2-1　SASEBO-R 上の AES 回路(PPRM1)に対する DPA の平均差分電力

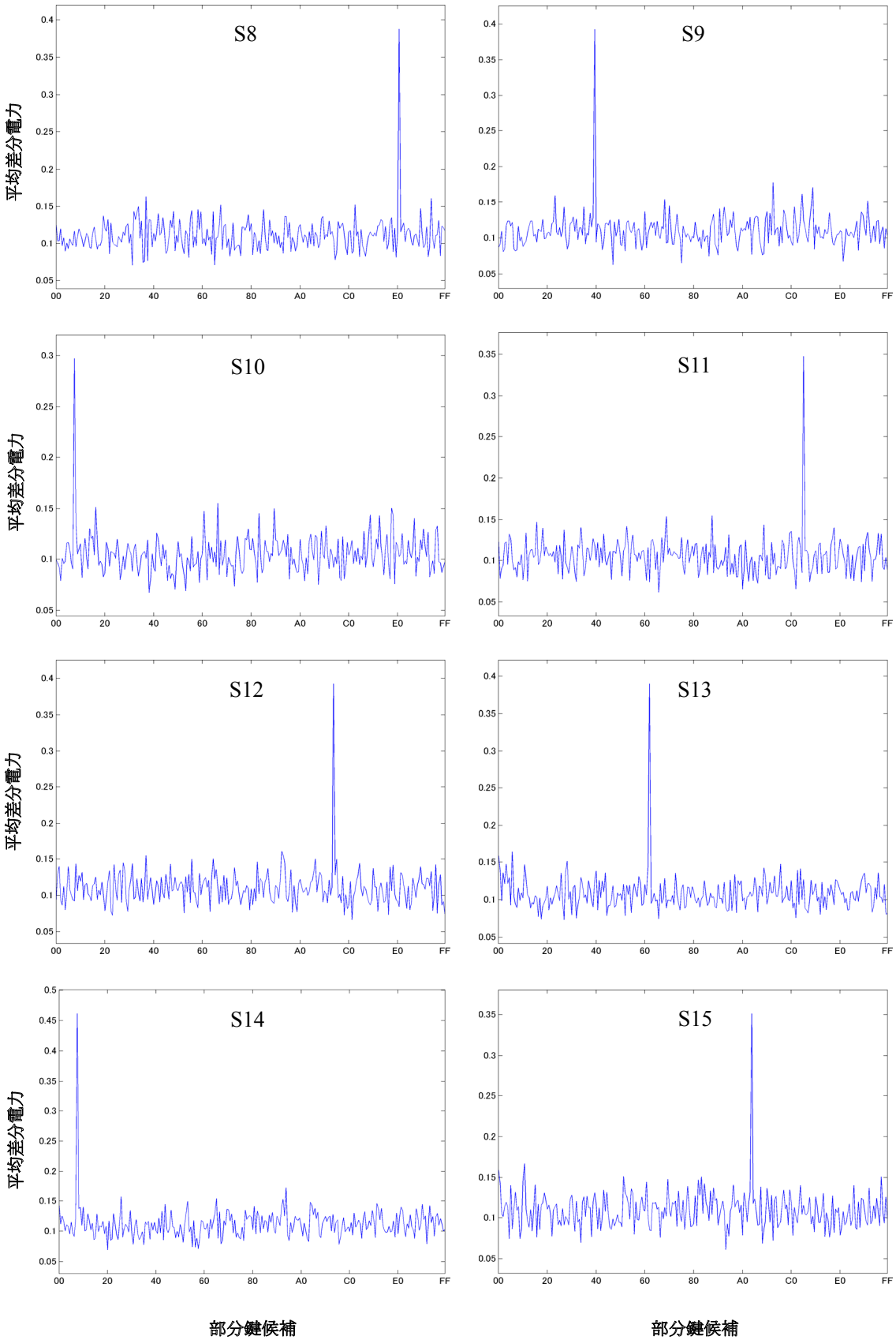

図 2-2　SASEBO-R 上の AES 回路(PPRM1)に対する DPA の平均差分電力

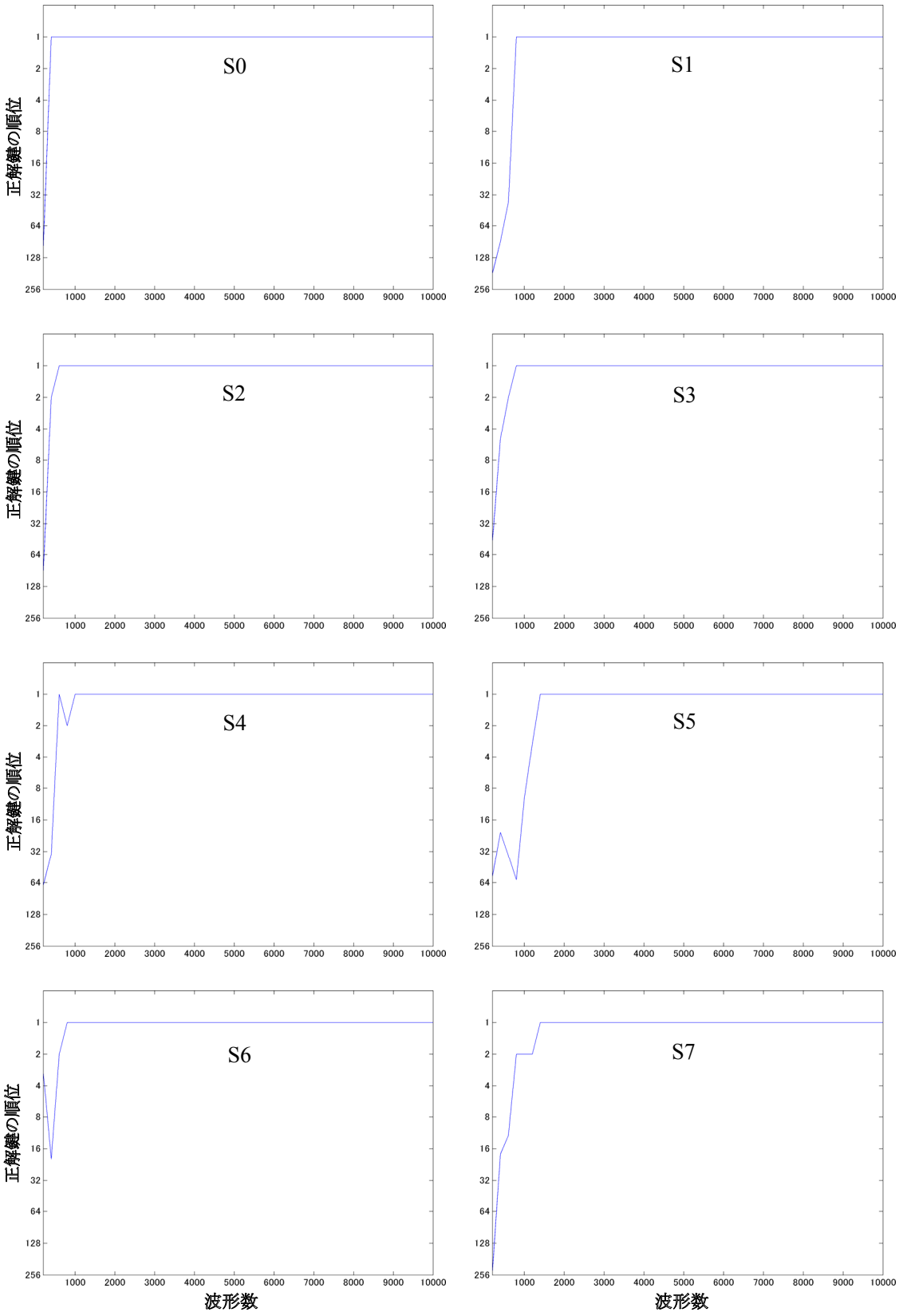

図 3-1　SASEBO-R 上の AES 回路(PPRM1)に対する DPA の精度と波形数の関係

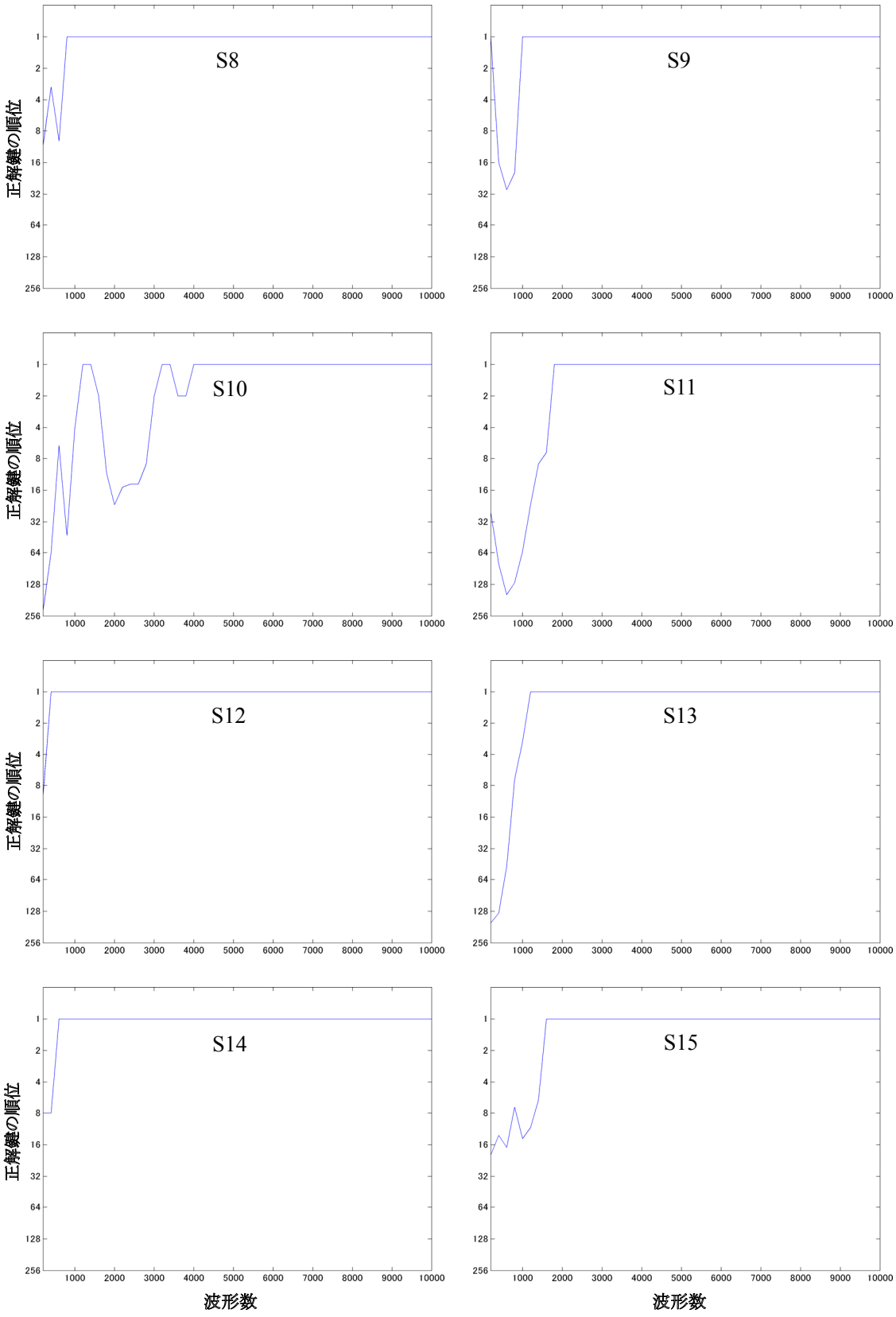

図 3-2　SASEBO-R 上の AES 回路(PPRM1)に対する DPA の精度と波形数の関係

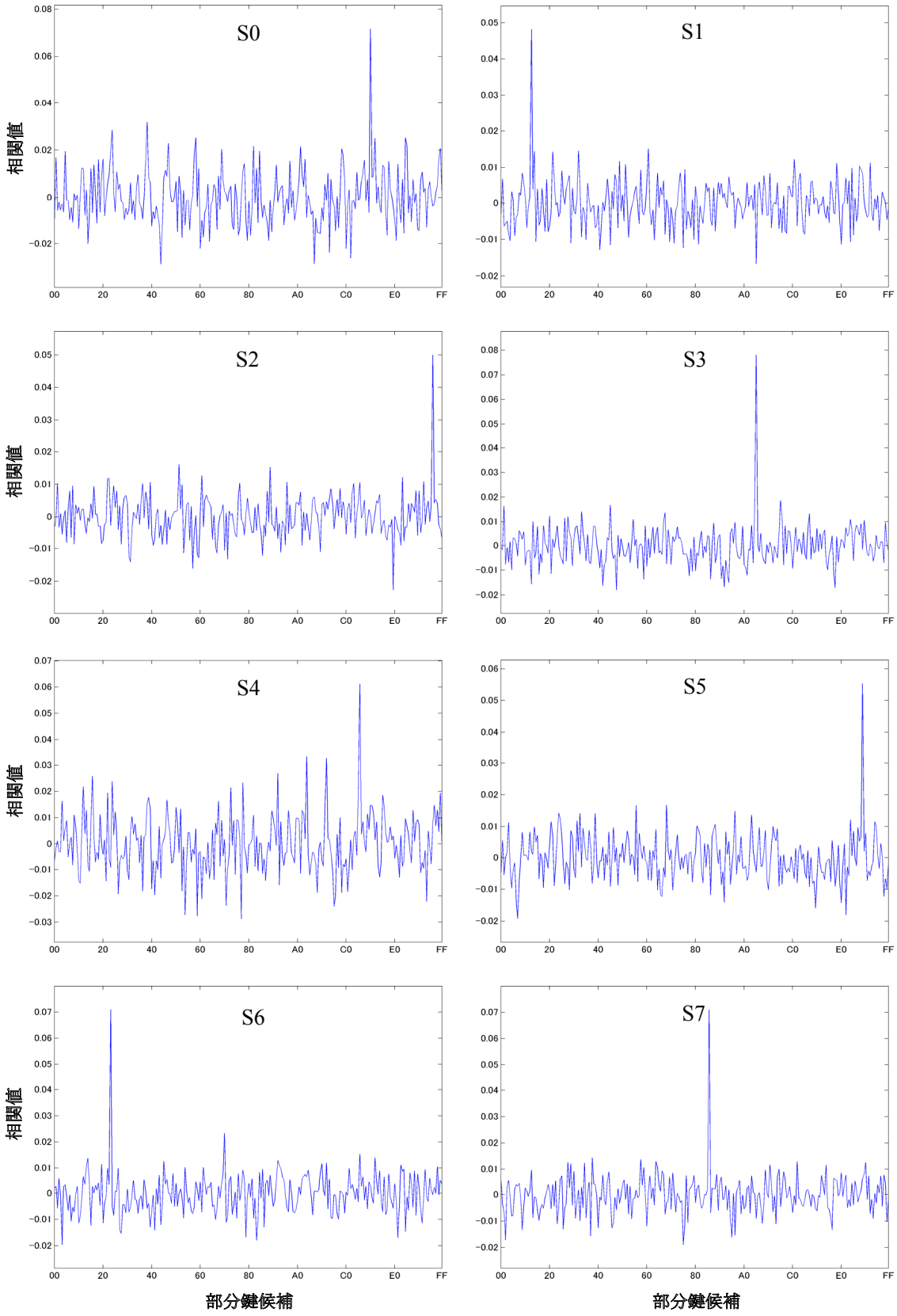

図 4-1　SASEBO-R 上の AES 回路(PPRM1)に対する CPA の相関値

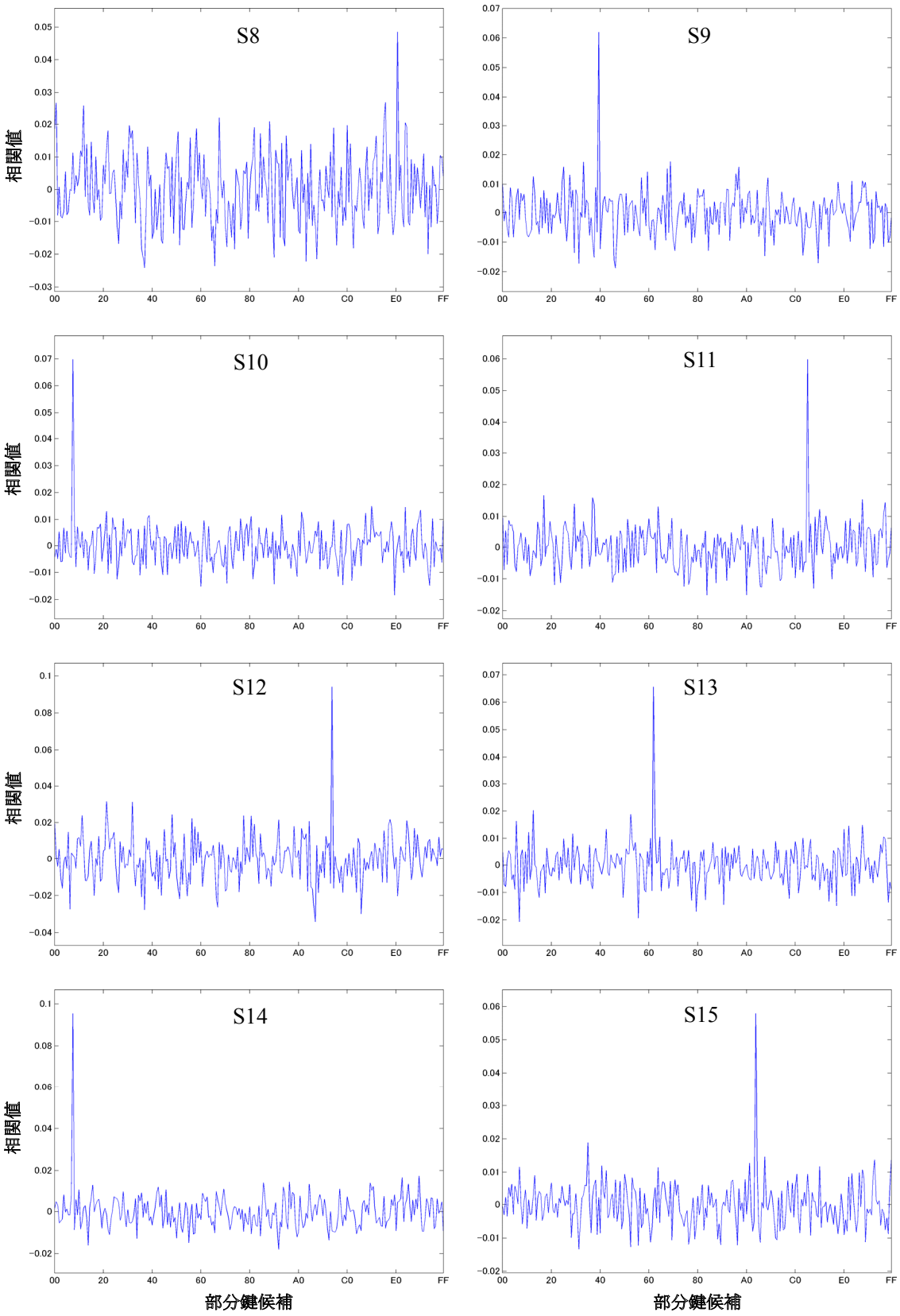

図 4-2　SASEBO-R 上の AES 回路(PPRM1)に対する CPA の相関値

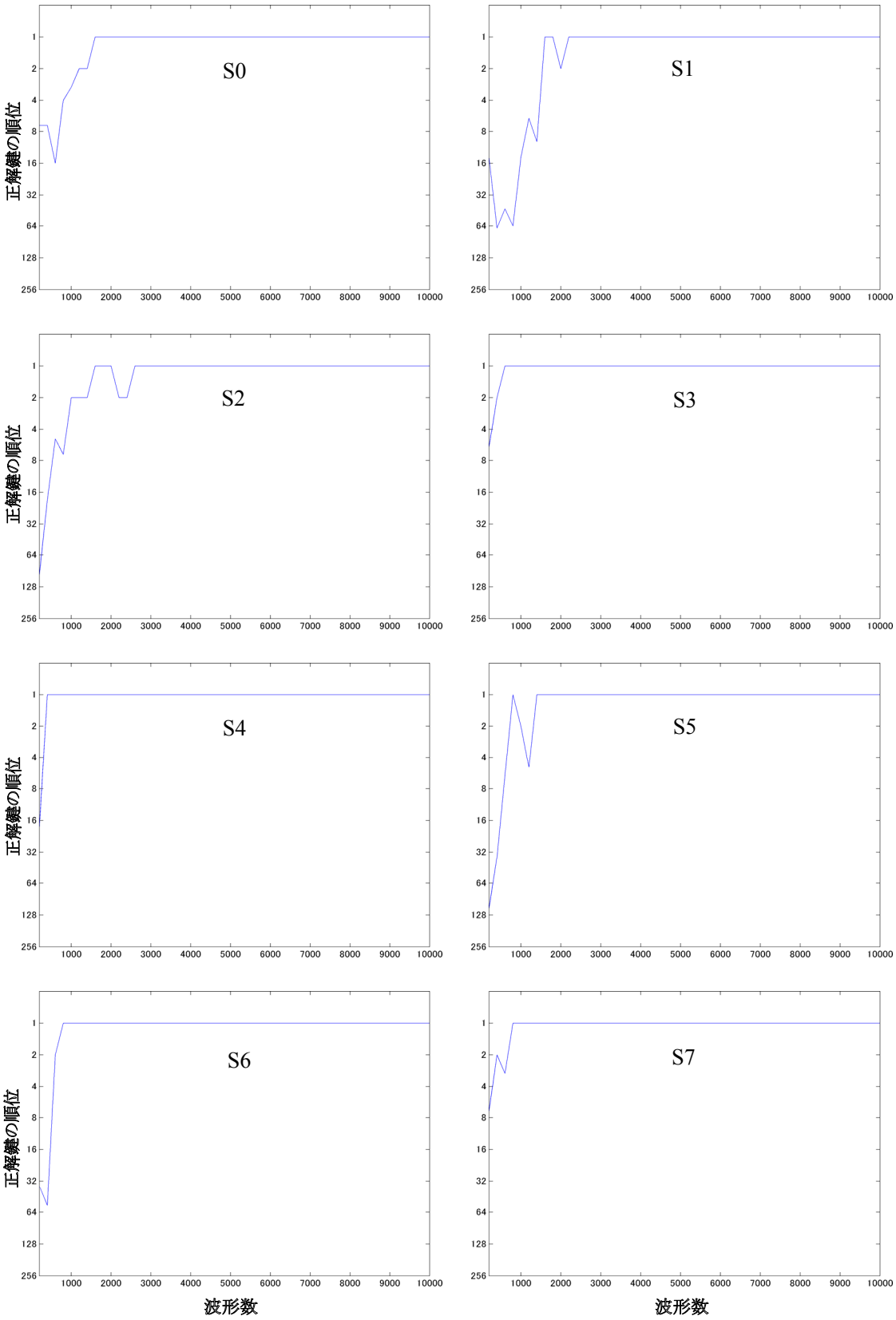

図 5-1　SASEBO-R 上の AES 回路(PPRM1)に対する CPA の精度と波形数の関係

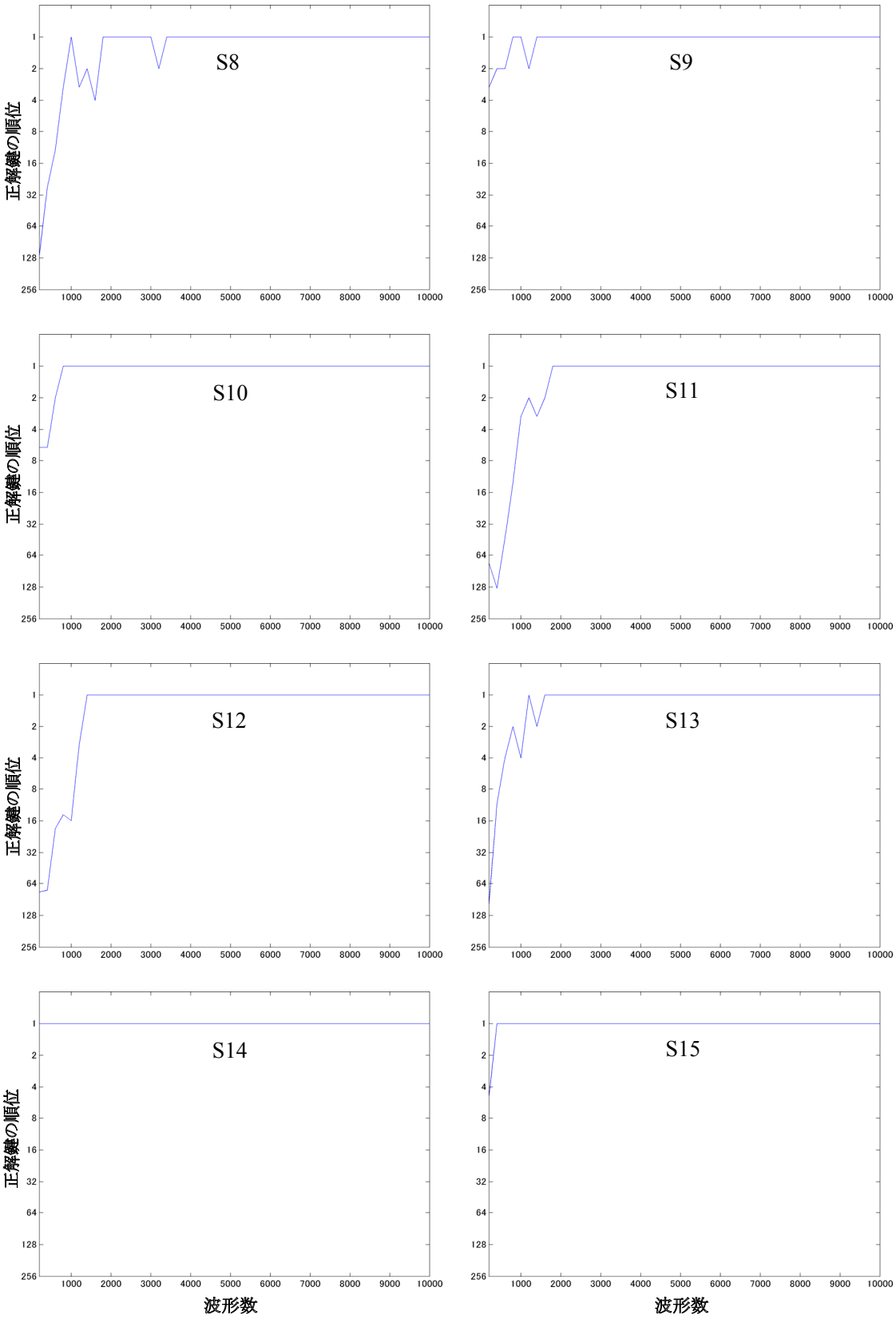

図 5-2　SASEBO-R 上の AES 回路(PPRM1)に対する CPA の精度と波形数の関係

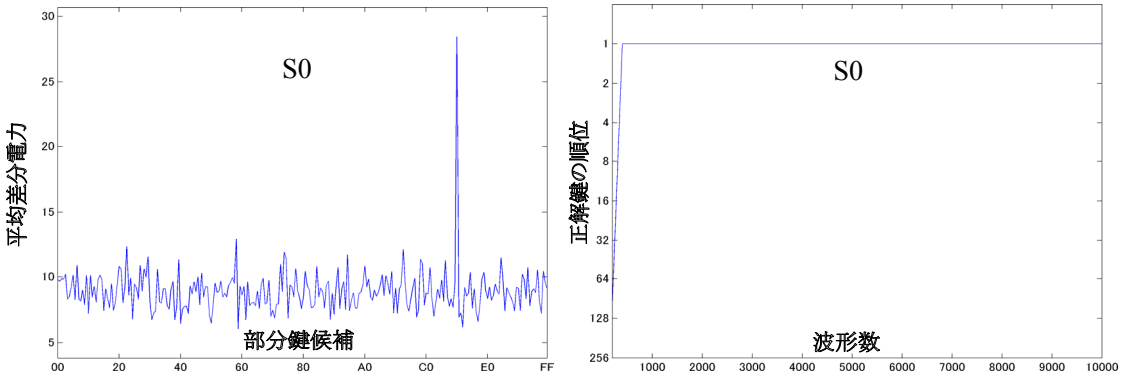

図 6　SASEBO-R 上の AES 回路(PPRM1)に対する W2-DPA の結果

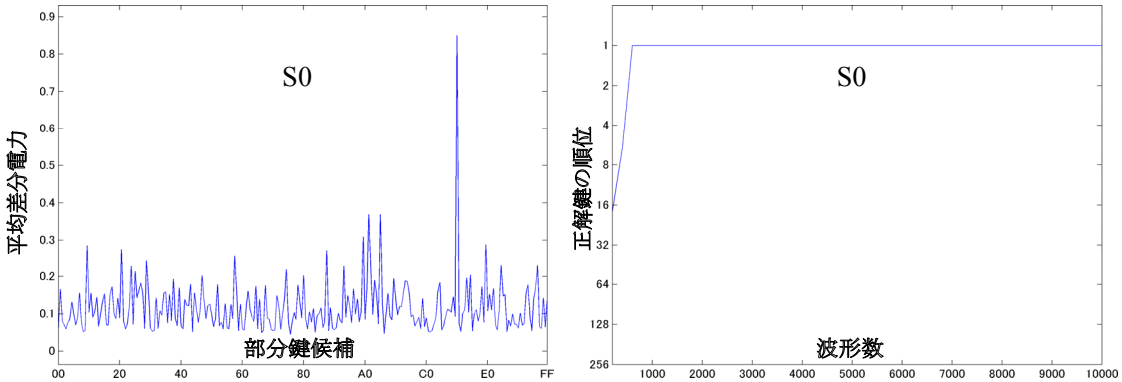

図 7　SASEBO-R 上の AES 回路(PPRM1)に対する M-DPA の結果

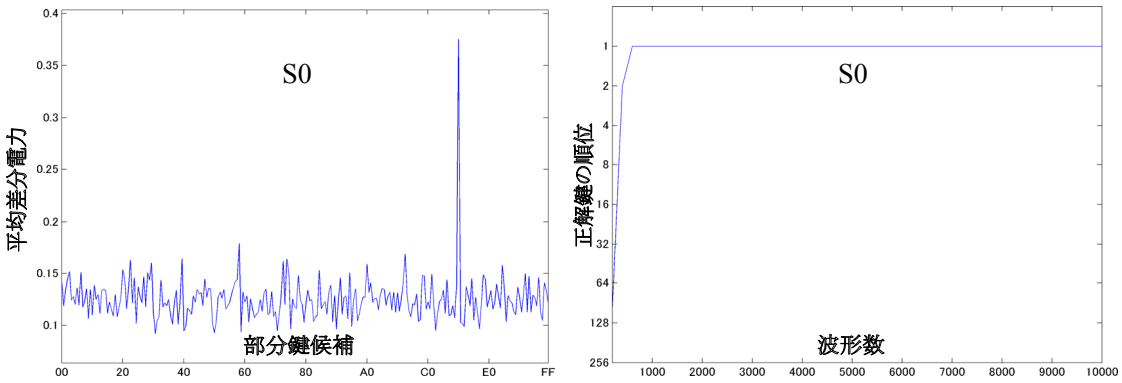

図 8　SASEBO-R 上の AES 回路(PPRM1)に対する M2-DPA の結果

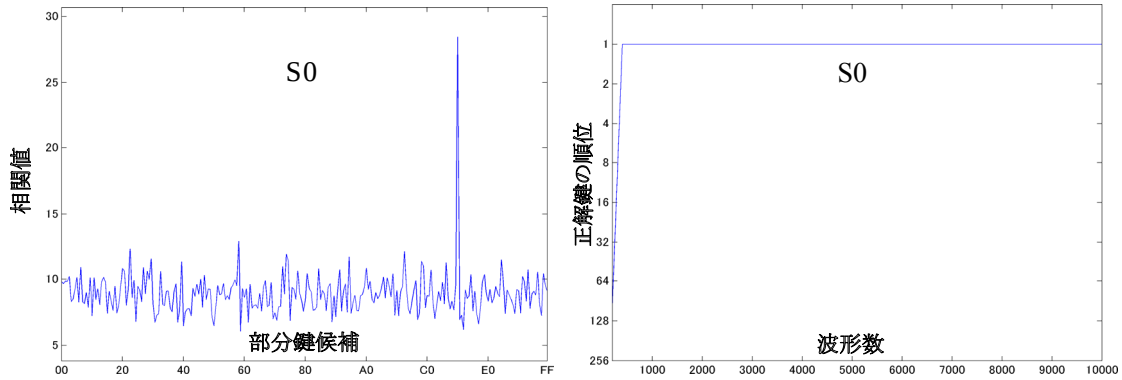

図 9　SASEBO-R 上の AES 回路(PPRM1)に対する PPA の結果

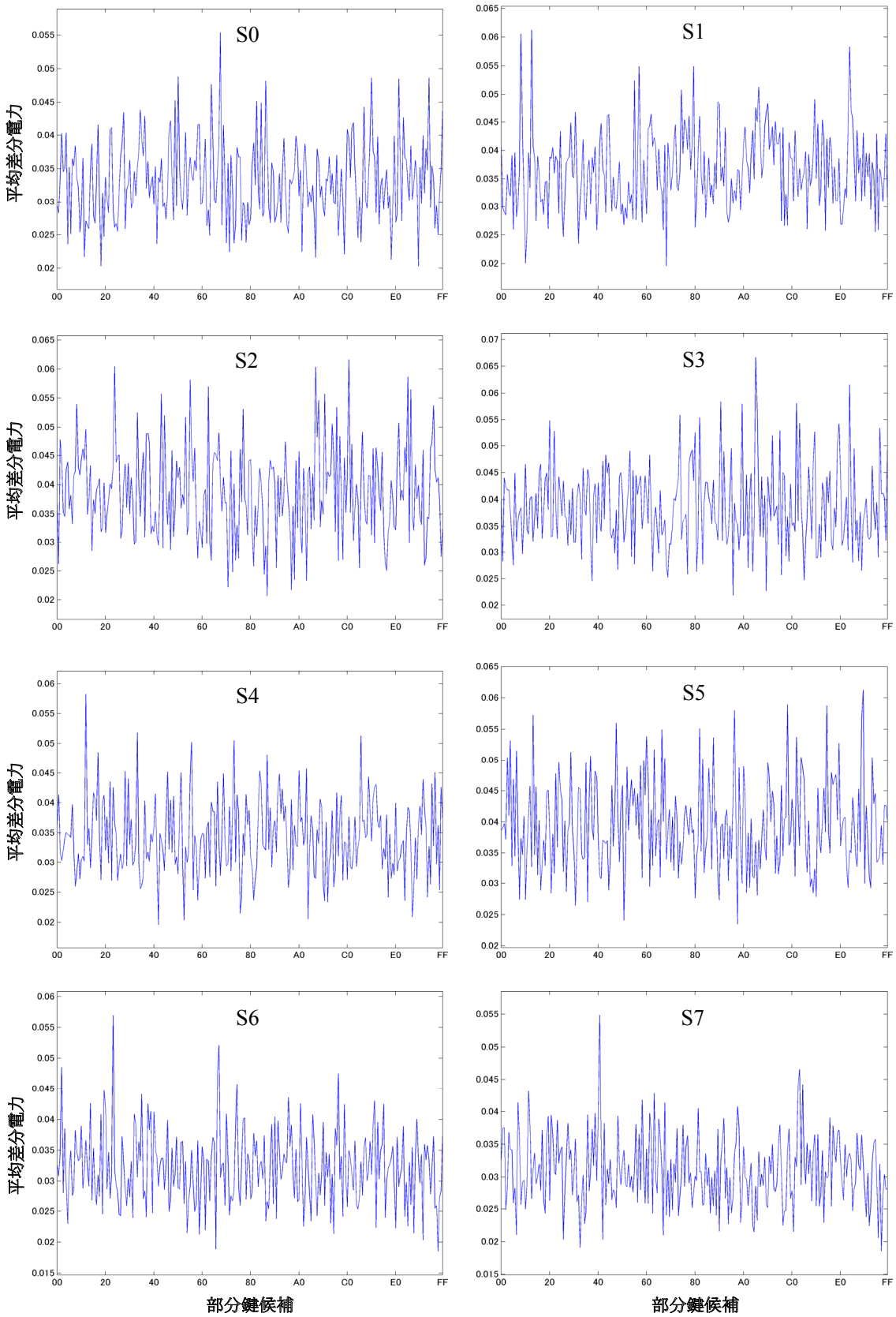

図 10-1　SASEBO-G 上の AES 回路(Comp)に対する DPA の平均差分電力

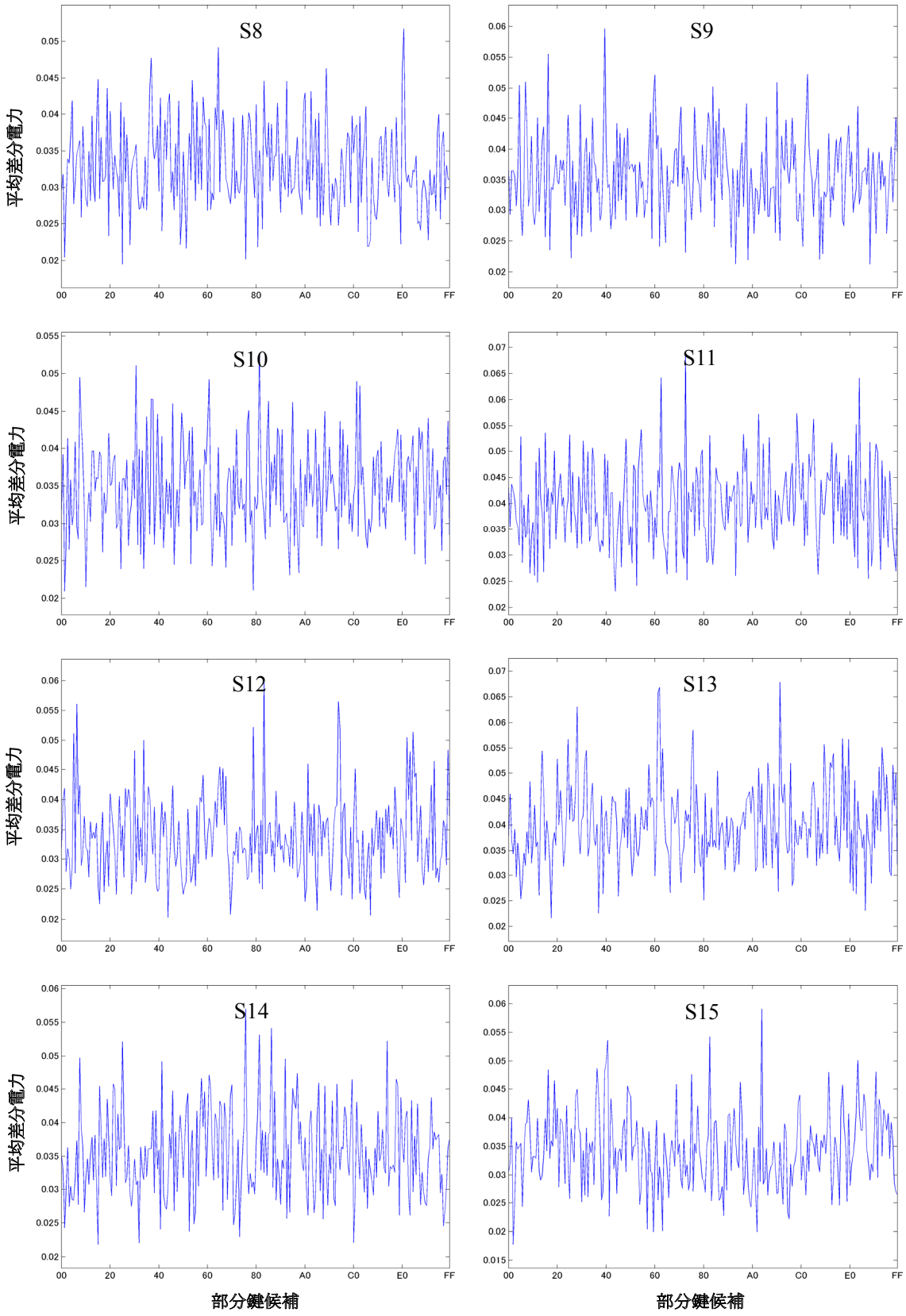

図 10-2　SASEBO-G 上の AES 回路(Comp)に対する DPA の平均差分電力

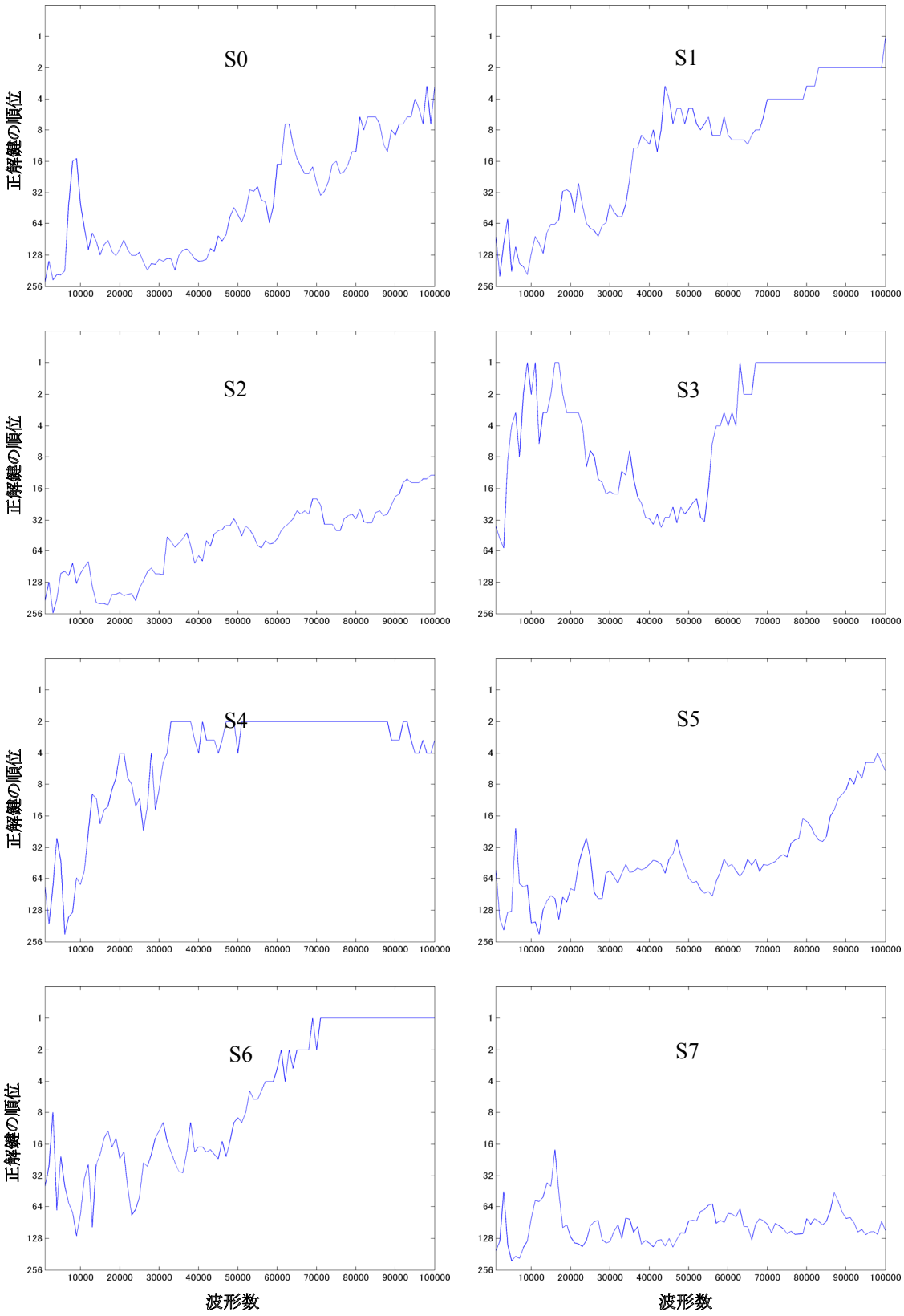

図 11-1　SASEBO-G 上の AES 回路(Comp)に対する DPA の精度と波形数の関係

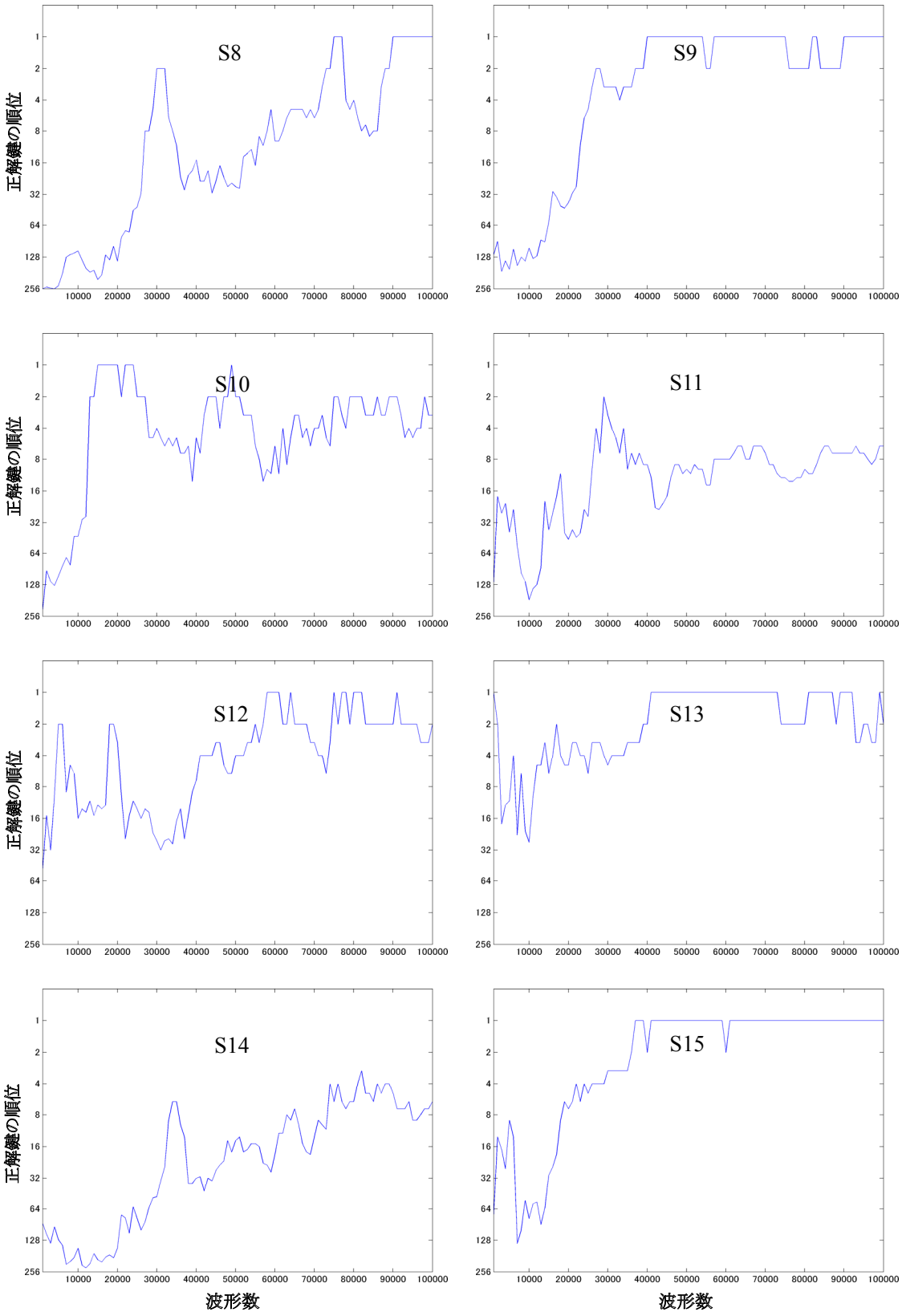

図 11-2　SASEBO-G 上の AES 回路(Comp)に対する DPA の精度と波形数の関係

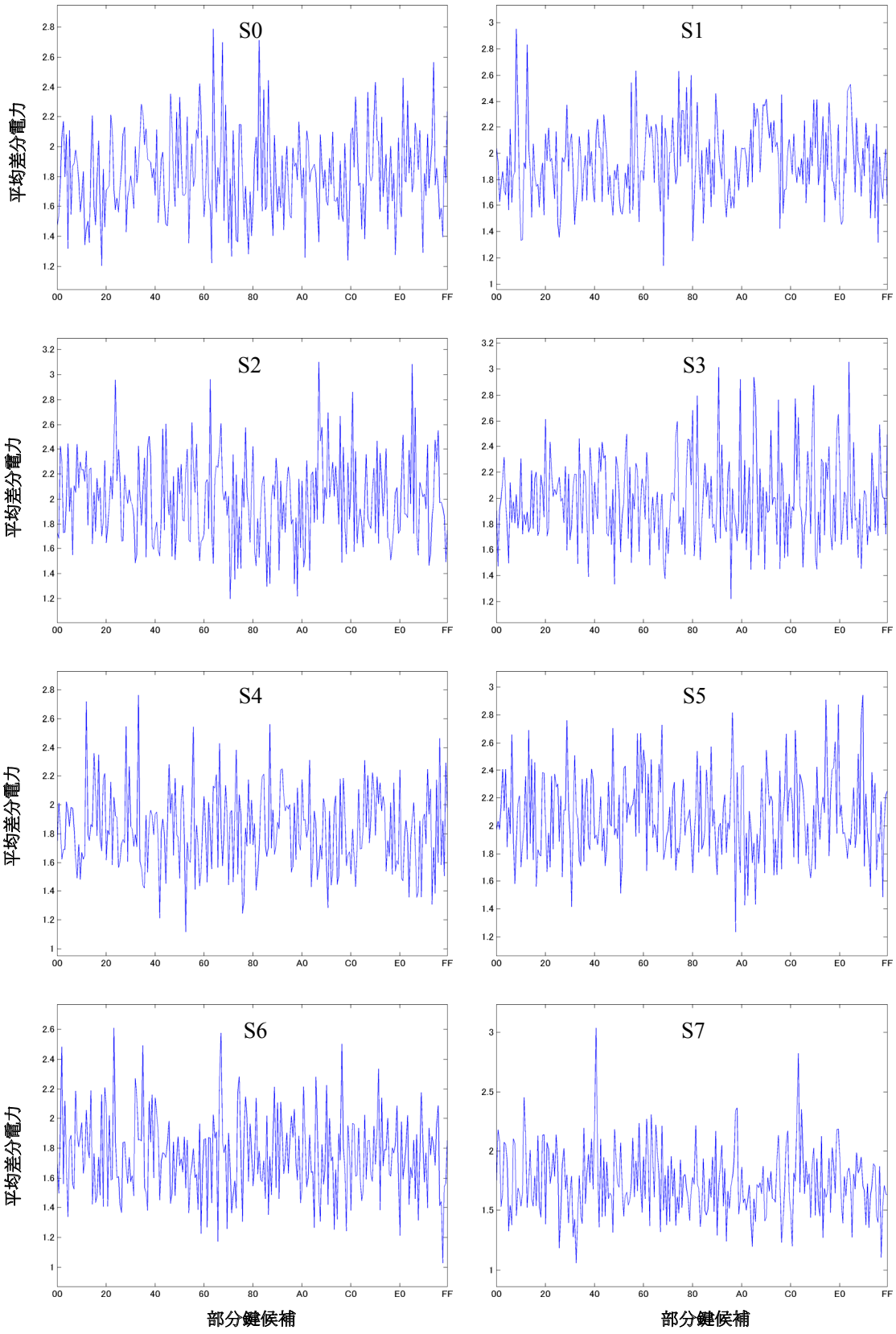

図 12-1　SASEBO-G 上の AES 回路(Comp)に対する W2-DPA の相関値

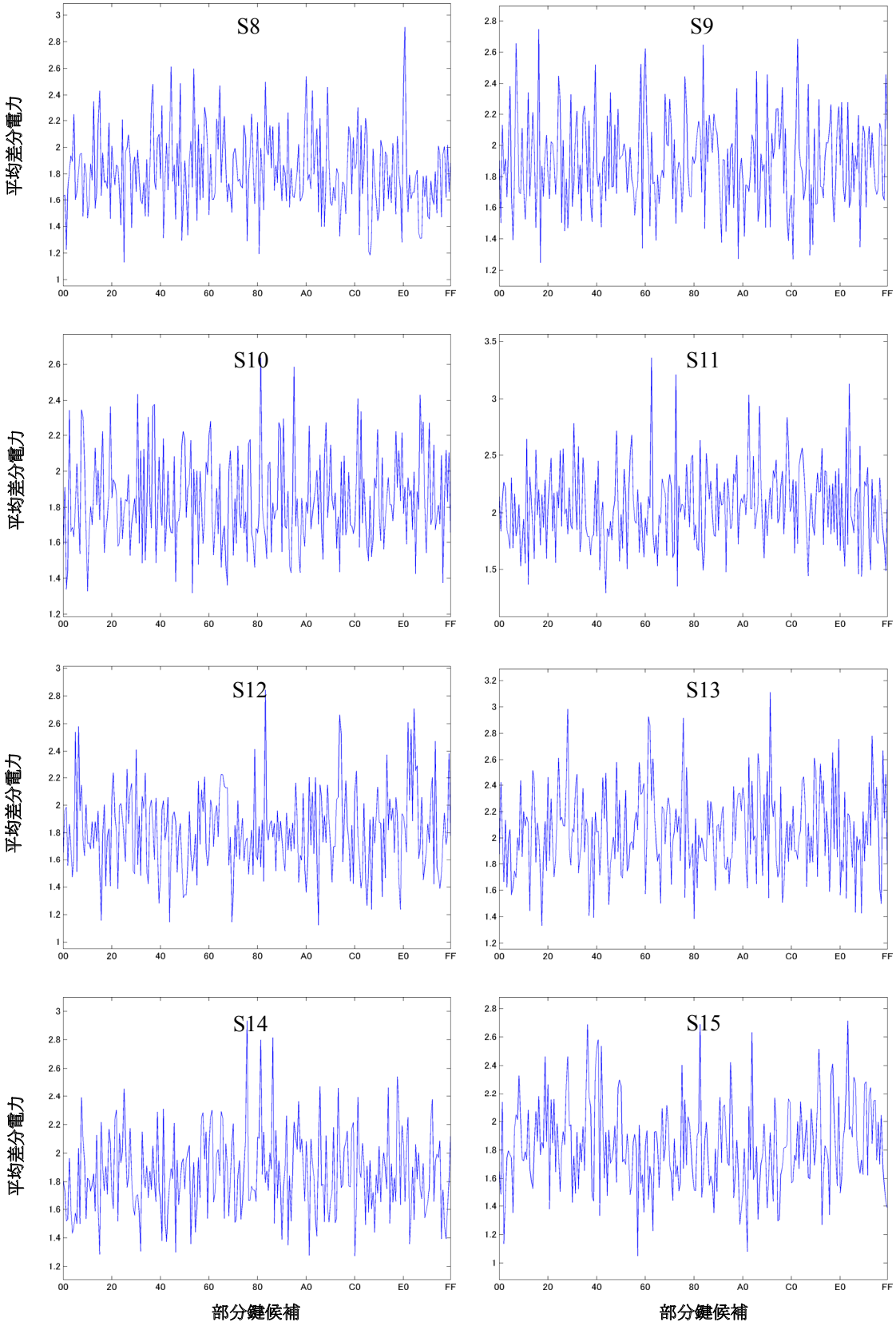

図 12-2　SASEBO-G 上の AES 回路(Comp)に対する W2-DPA の相関値

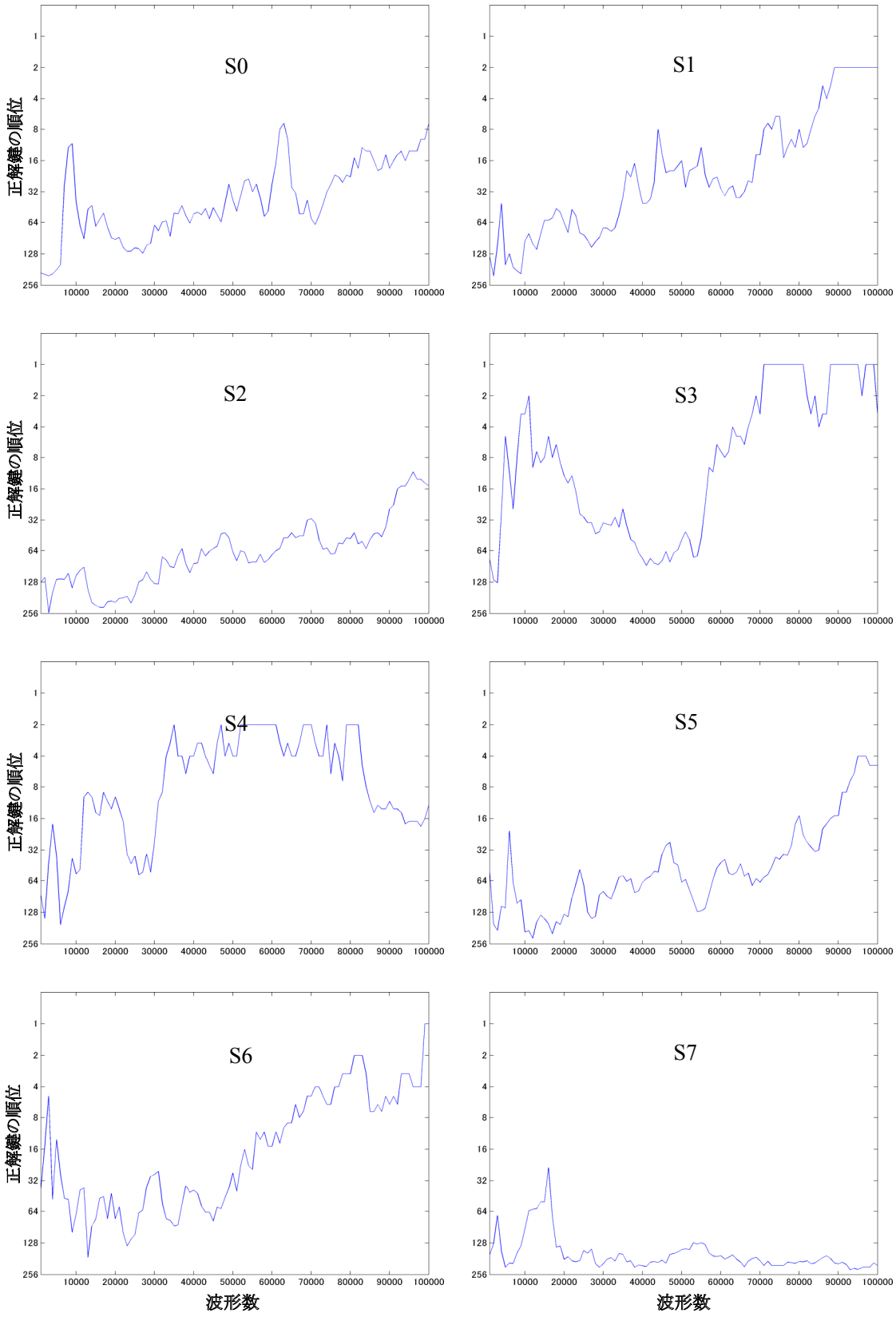

図 13-1　SASEBO-G 上の AES 回路(Comp)に対する W2-DPA の精度と波形数の関係

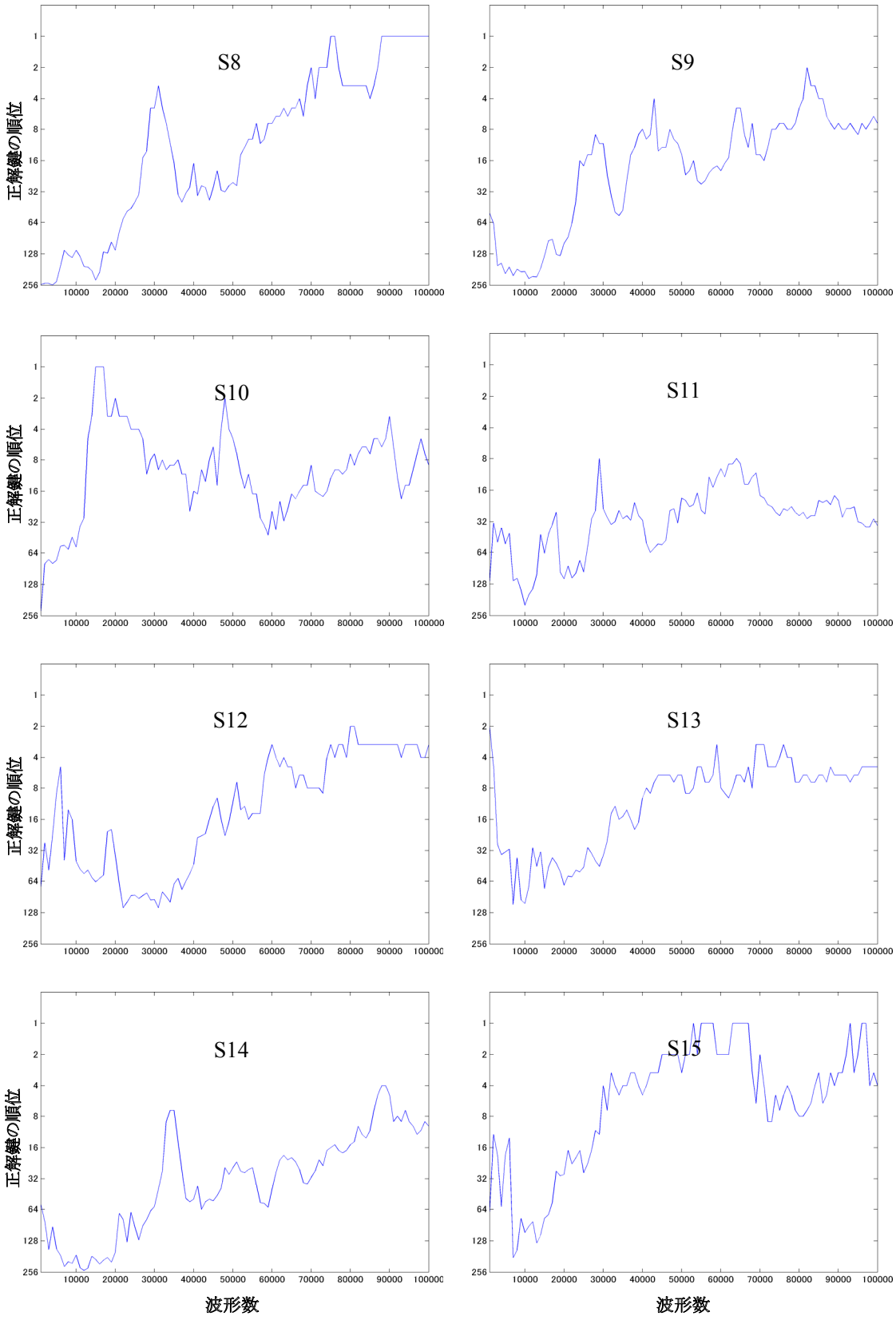

図 13-2　SASEBO-G 上の AES 回路(Comp)に対する W2-DPA の精度と波形数の関係

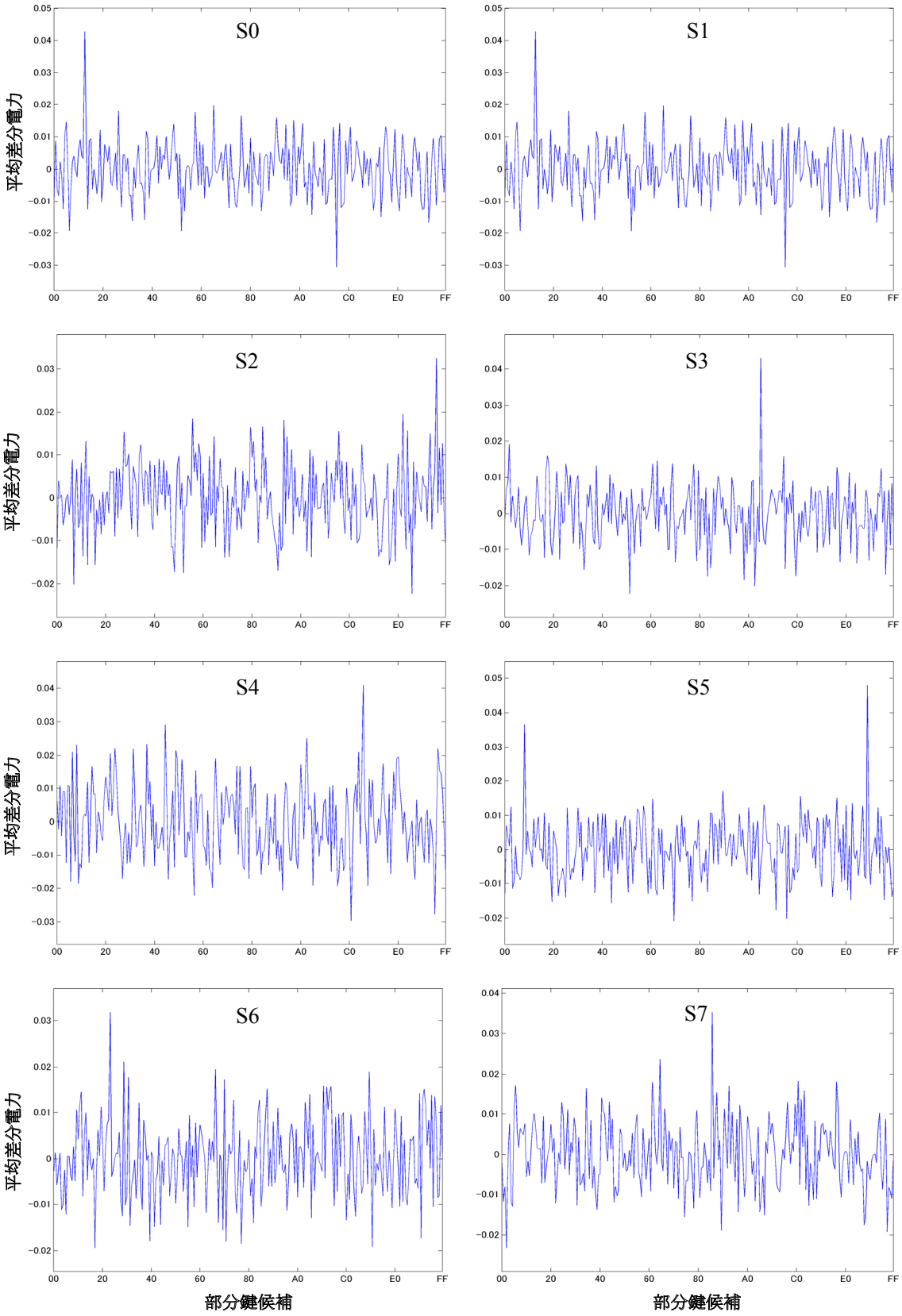

図 14-1　SASEBO-G 上の AES 回路(Comp)に対する CPA の相関値

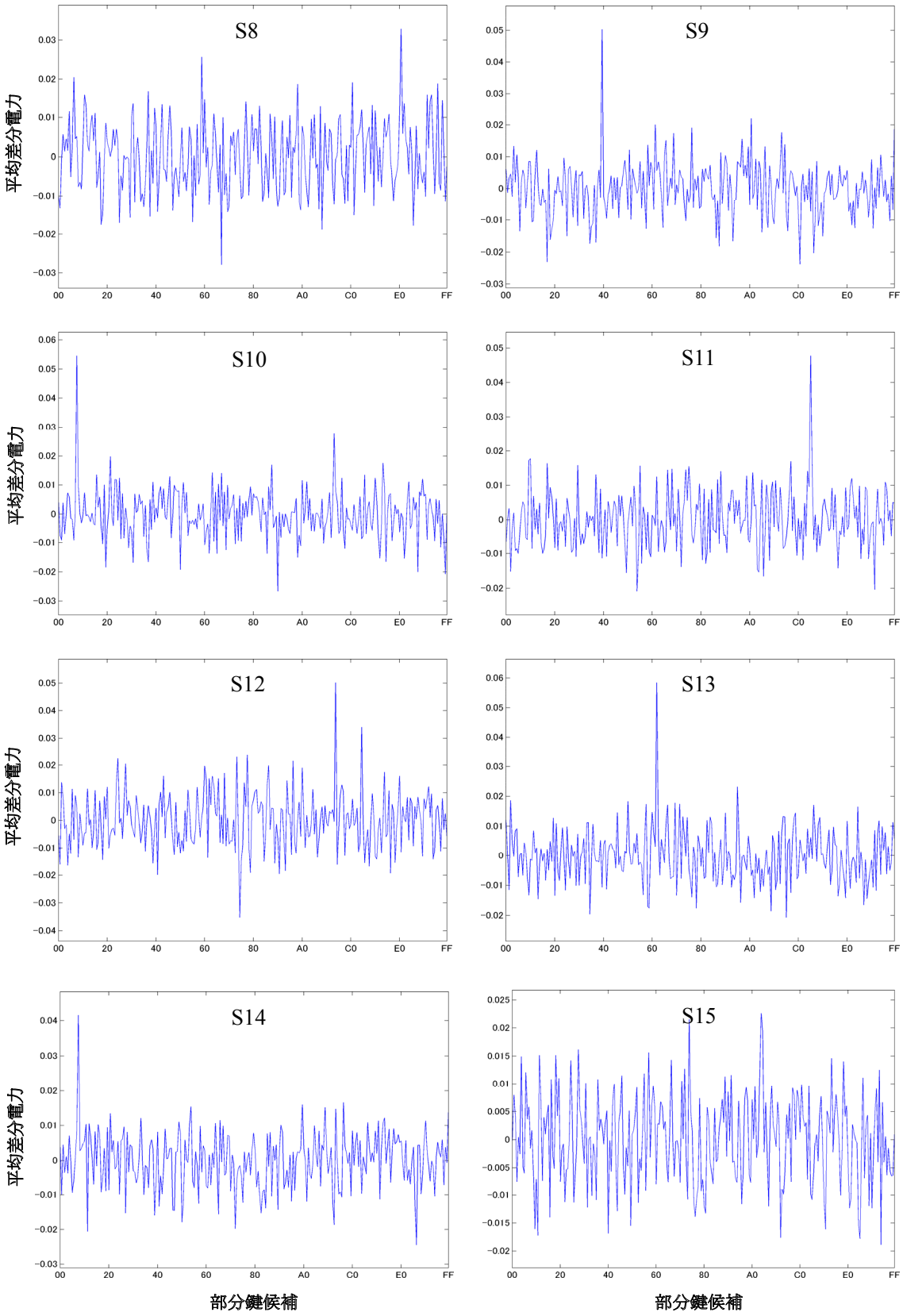

図 14-2　SASEBO-G 上の AES 回路(Comp)に対する CPA の相関値

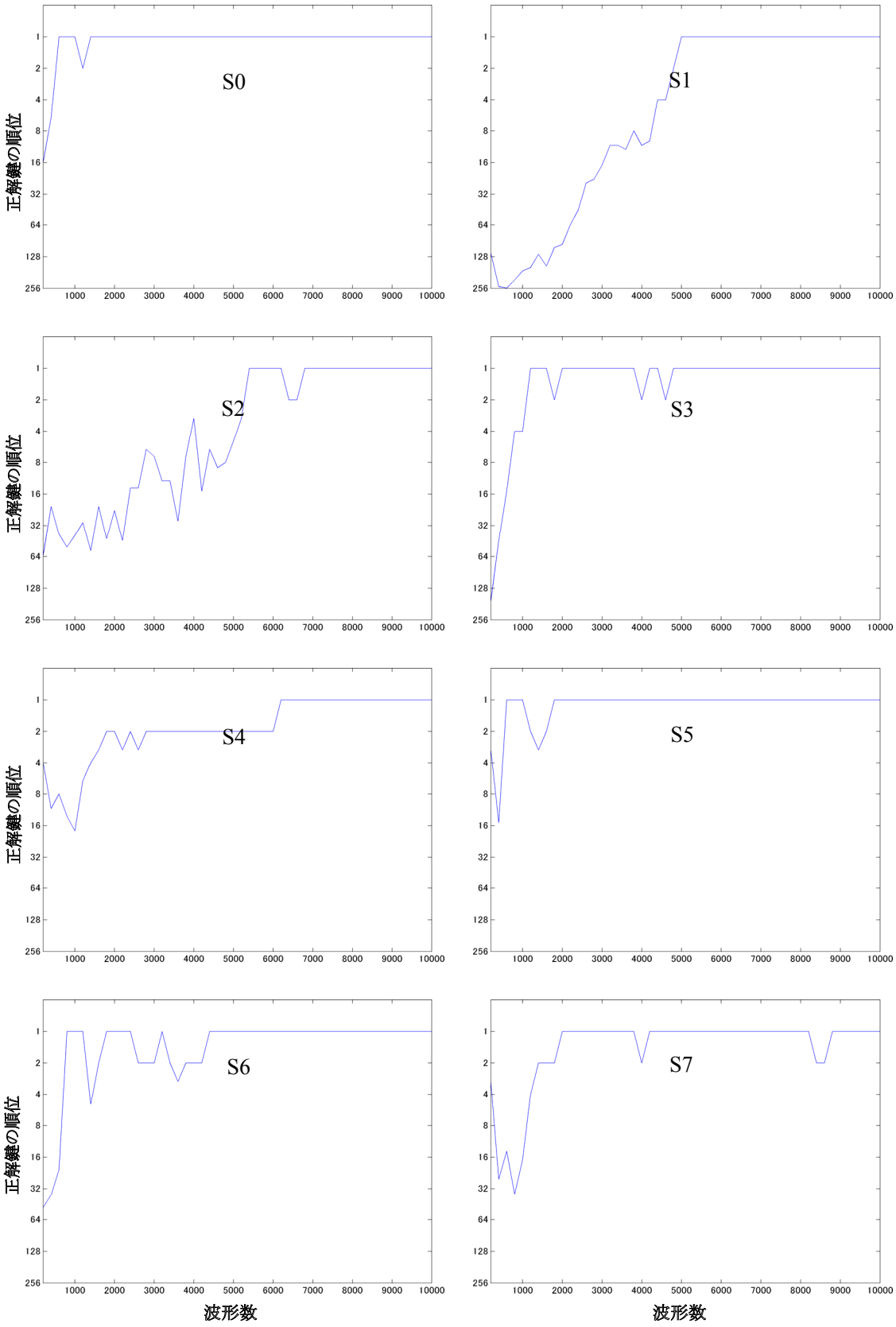

図 15-1　SASEBO-G 上の AES 回路(Comp)に対する CPA の精度と波形数の関係

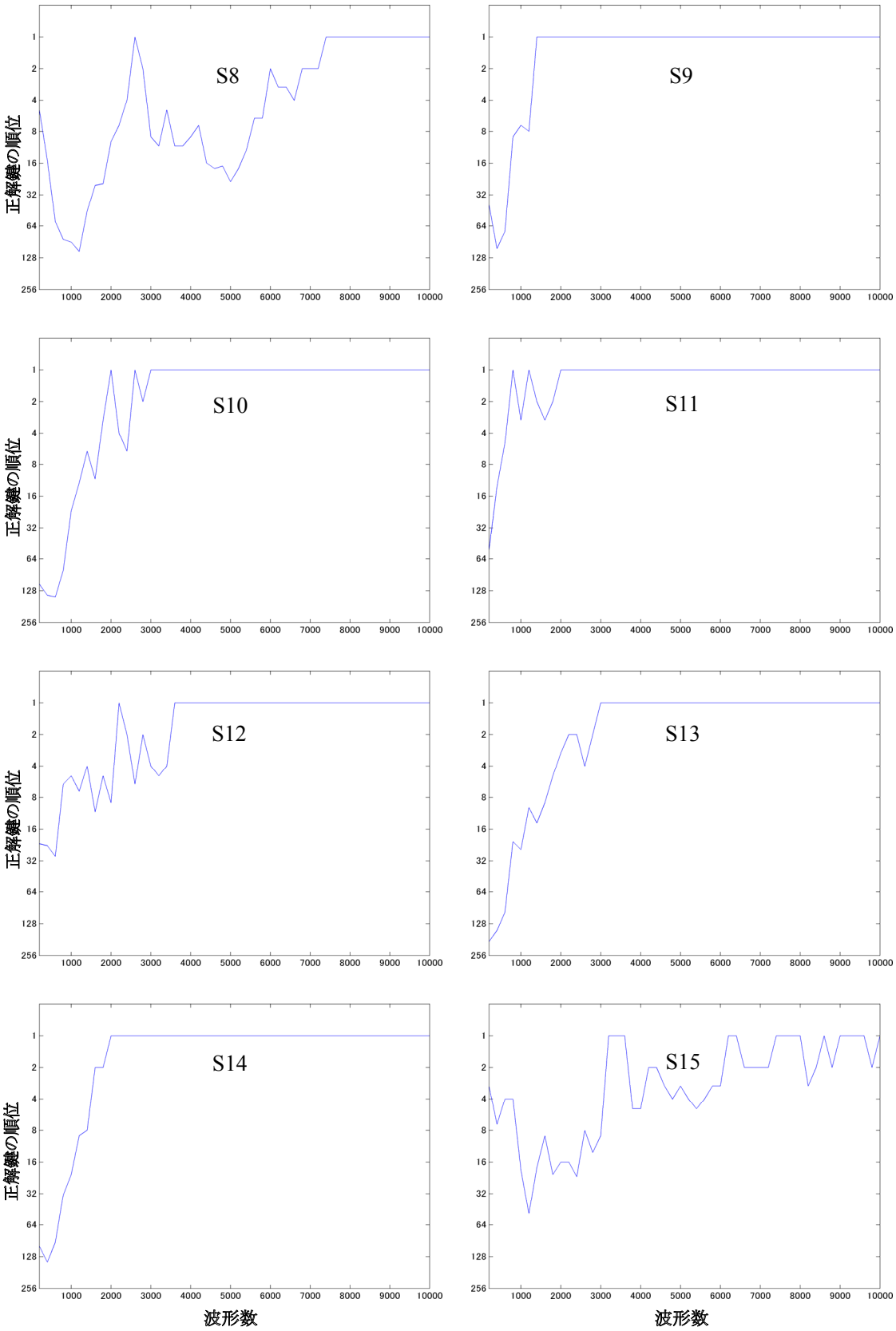

図 15-2　SASEBO-G 上の AES 回路(Comp)に対する CPA の精度と波形数の関係

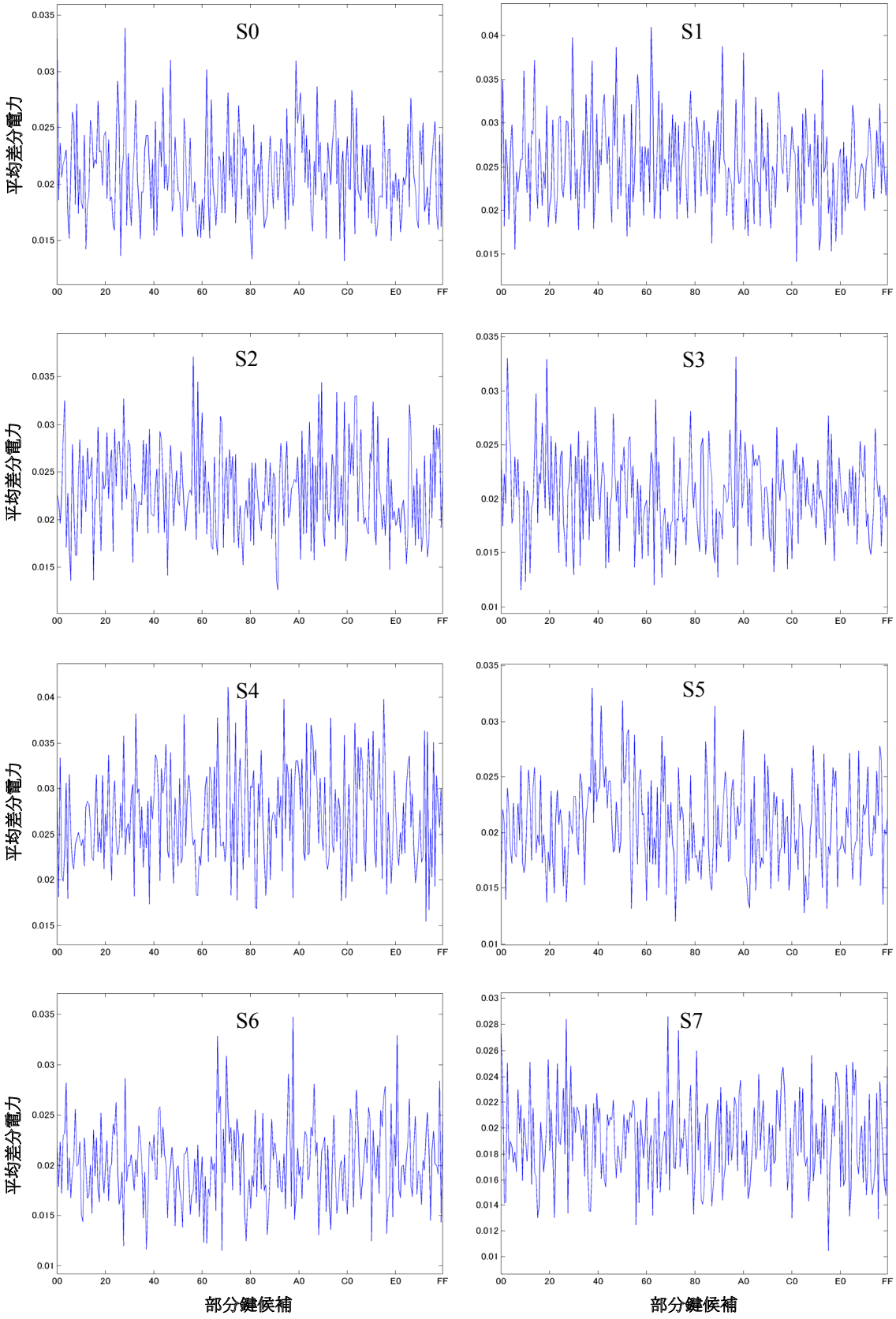

図 16-1　SASEBO-G 上の AES 回路(MAO)に対する DPA の平均差分電力

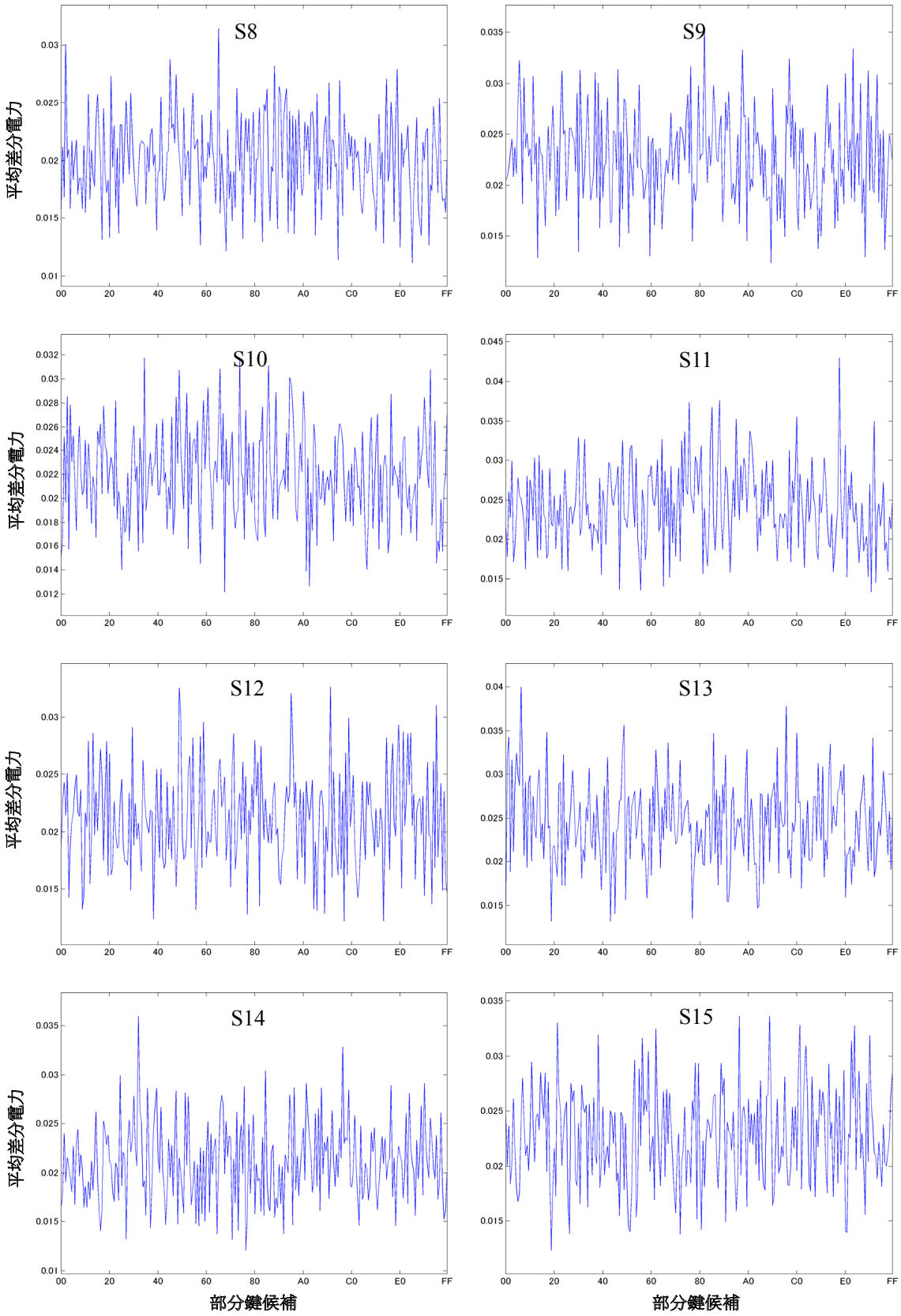

図 16-2　SASEBO-G 上の AES 回路(MAO)に対する DPA の平均差分電力

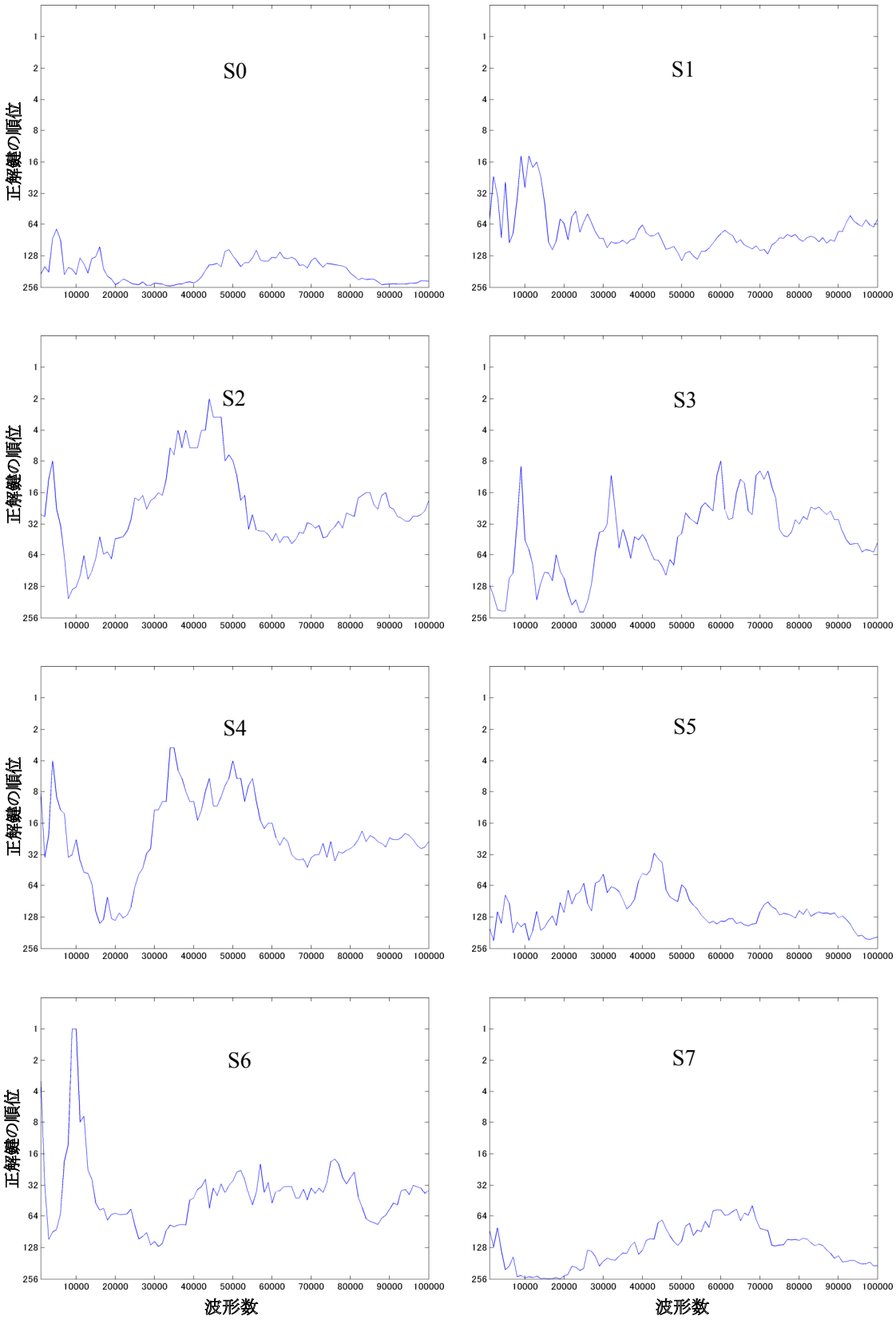

図 17-1　SASEBO-G 上の AES 回路(MAO)に対する DPA の精度と波形数の関係

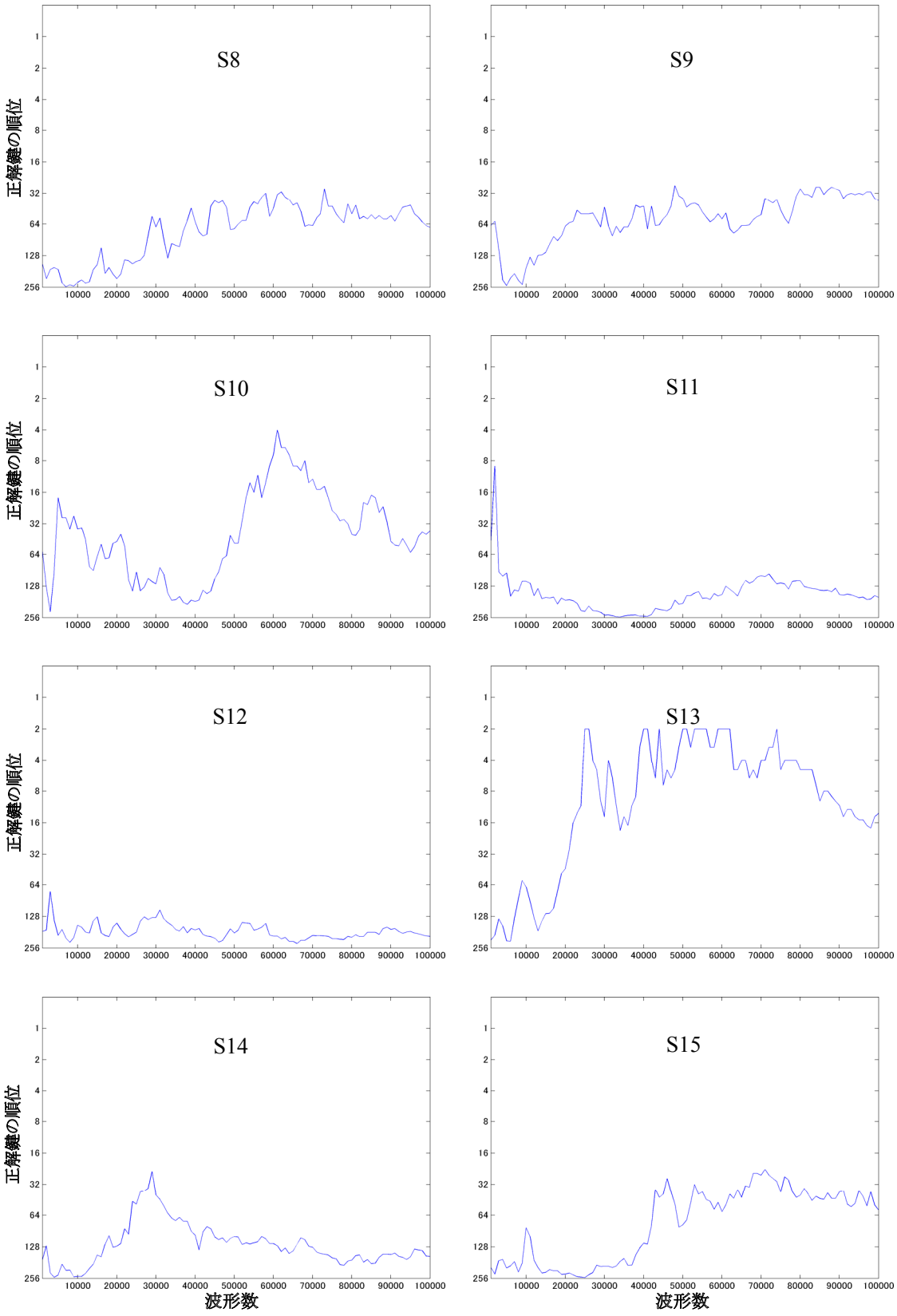

図 17-2　SASEBO-G 上の AES 回路(MAO)に対する DPA の精度と波形数の関係

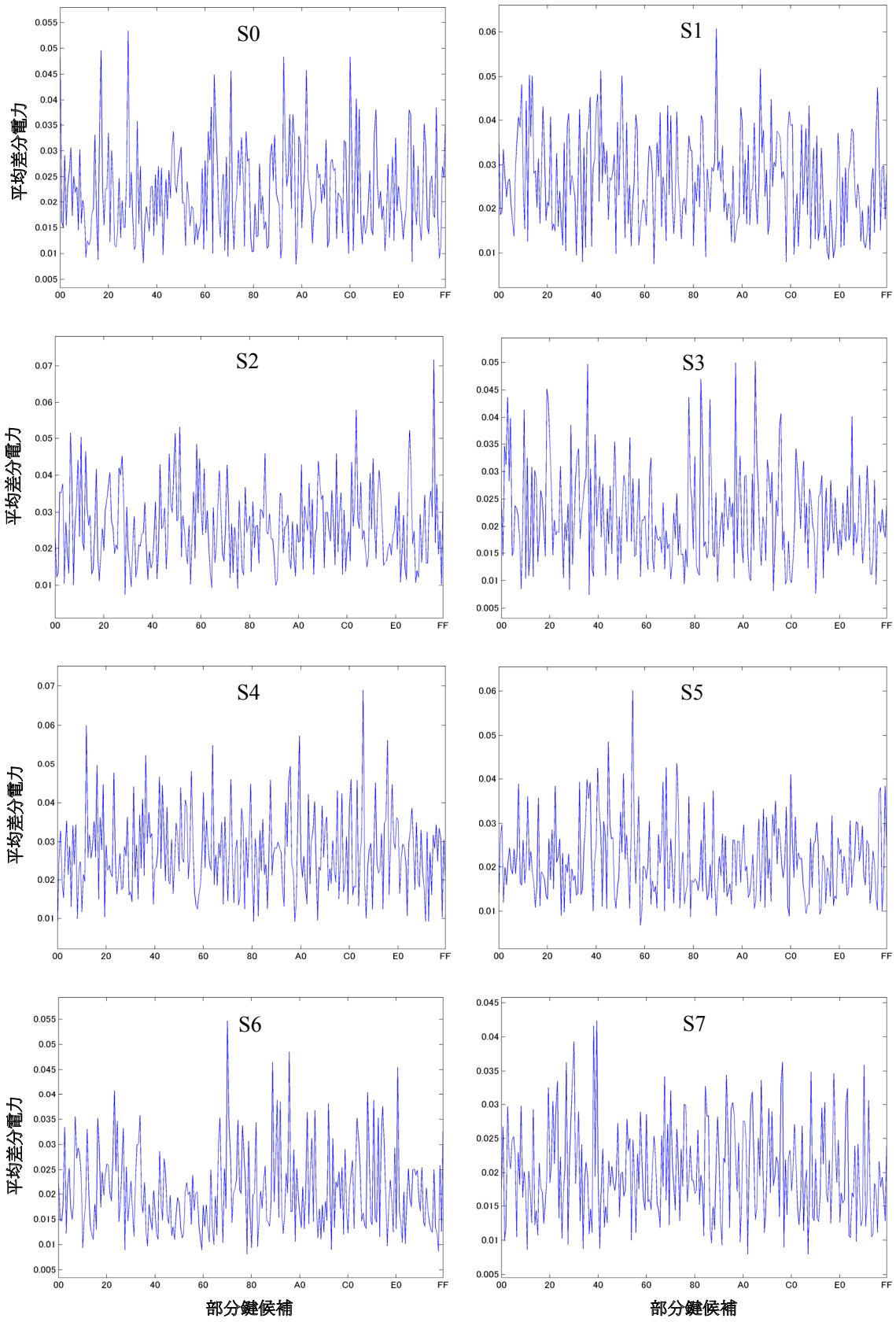

図 18-1　SASEBO-G 上の AES 回路(MAO)に対する DPA の平均差分電力(bit1&bit6)

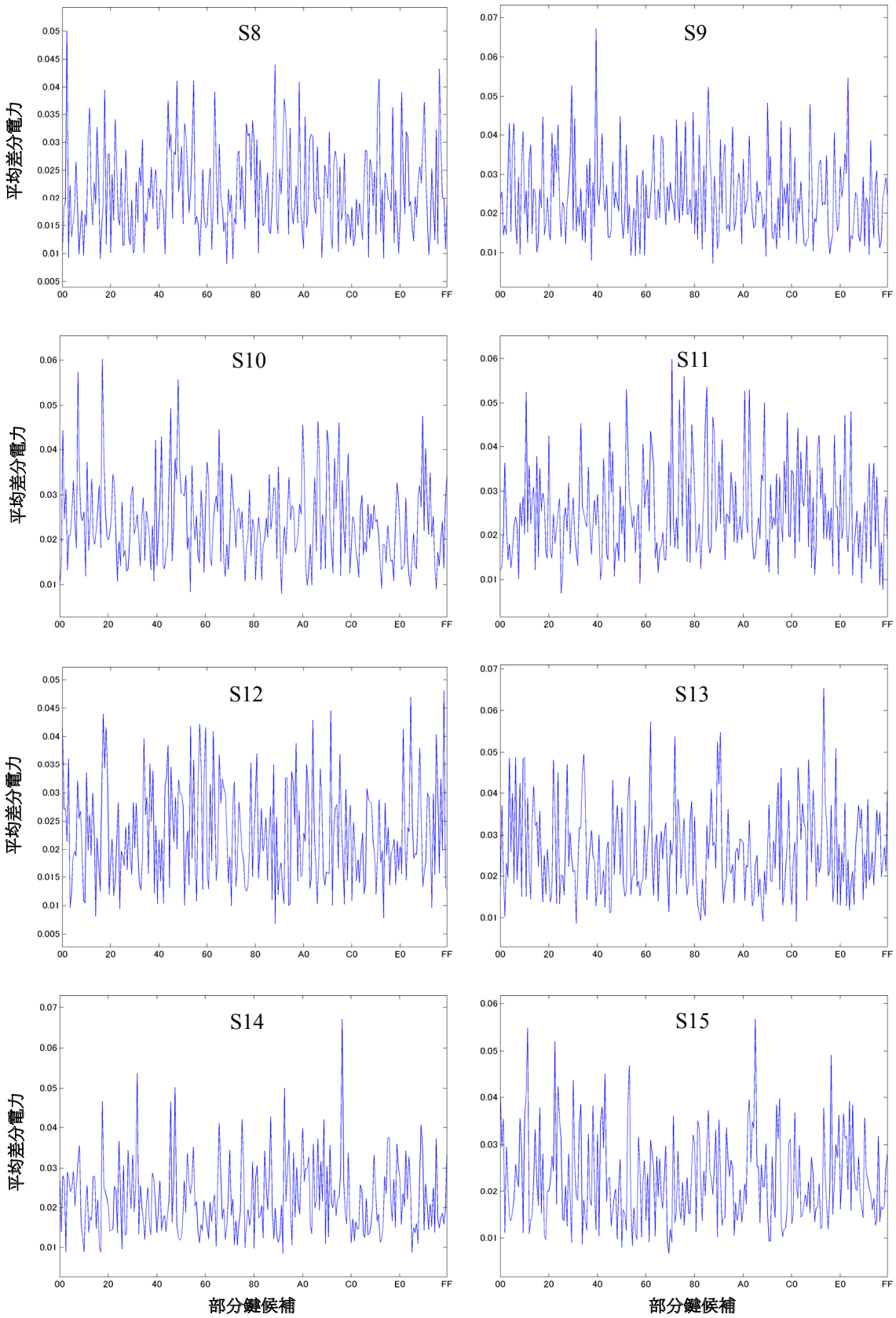

図 18-2　SASEBO-G 上の AES 回路(MAO)に対する DPA の平均差分電力(bit1&bit6)

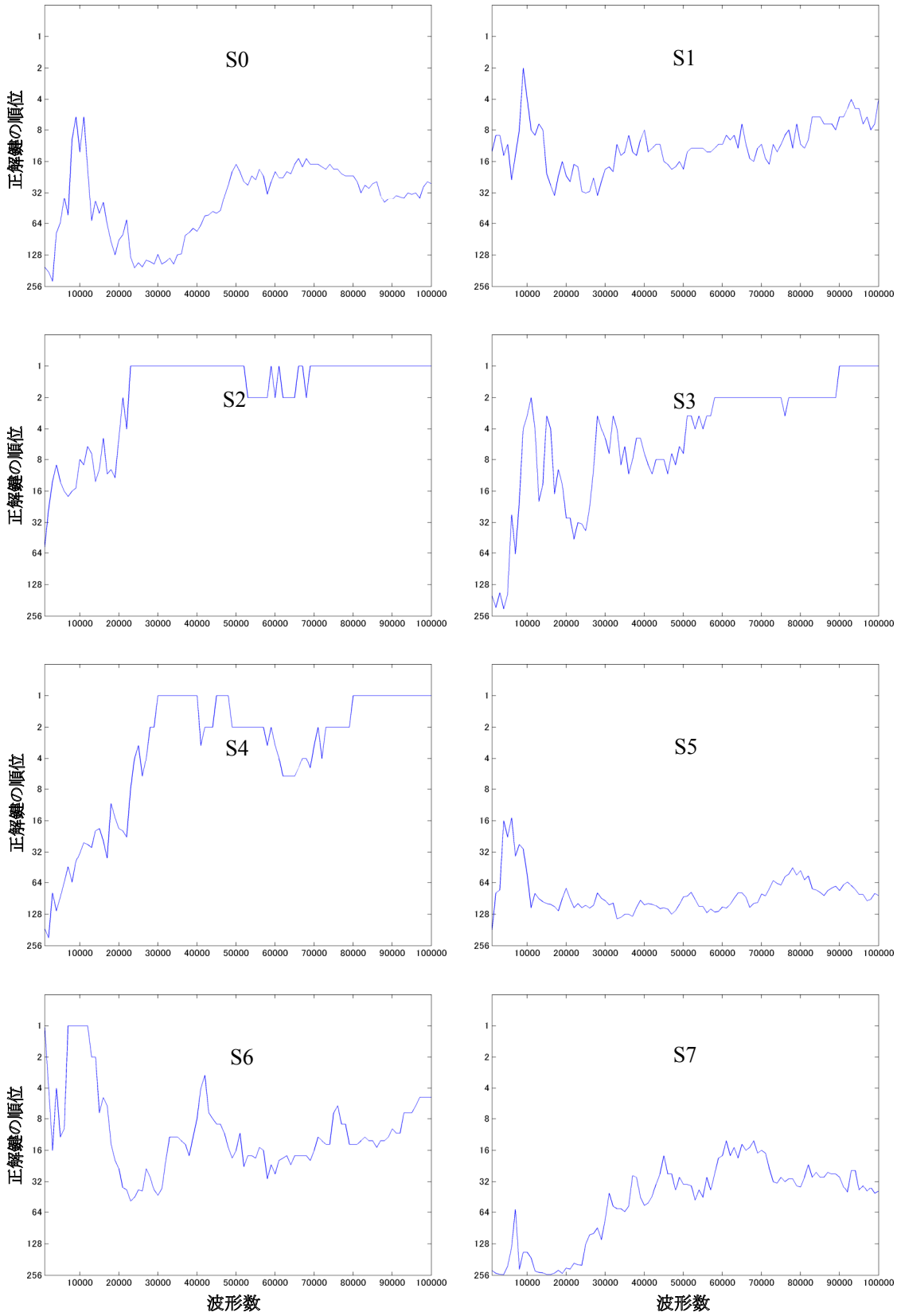

図 19-1　SASEBO-G 上の AES 回路(MAO)に対する DPA の精度と波形数の関係(bit1&bit6)

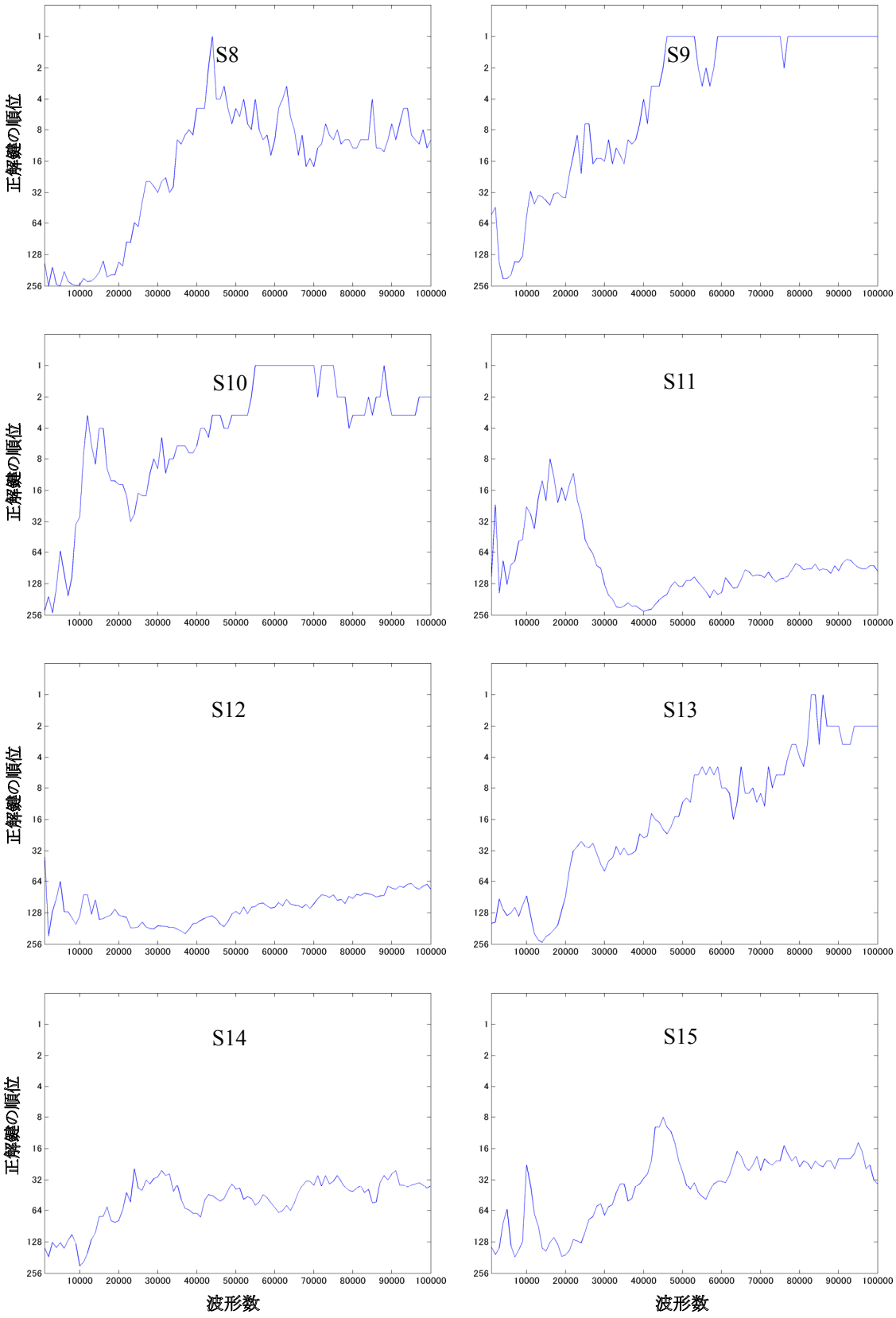

図 19-2　SASEBO-G 上の AES 回路(MAO)に対する DPA の精度と波形数の関係(bit1&bit6)

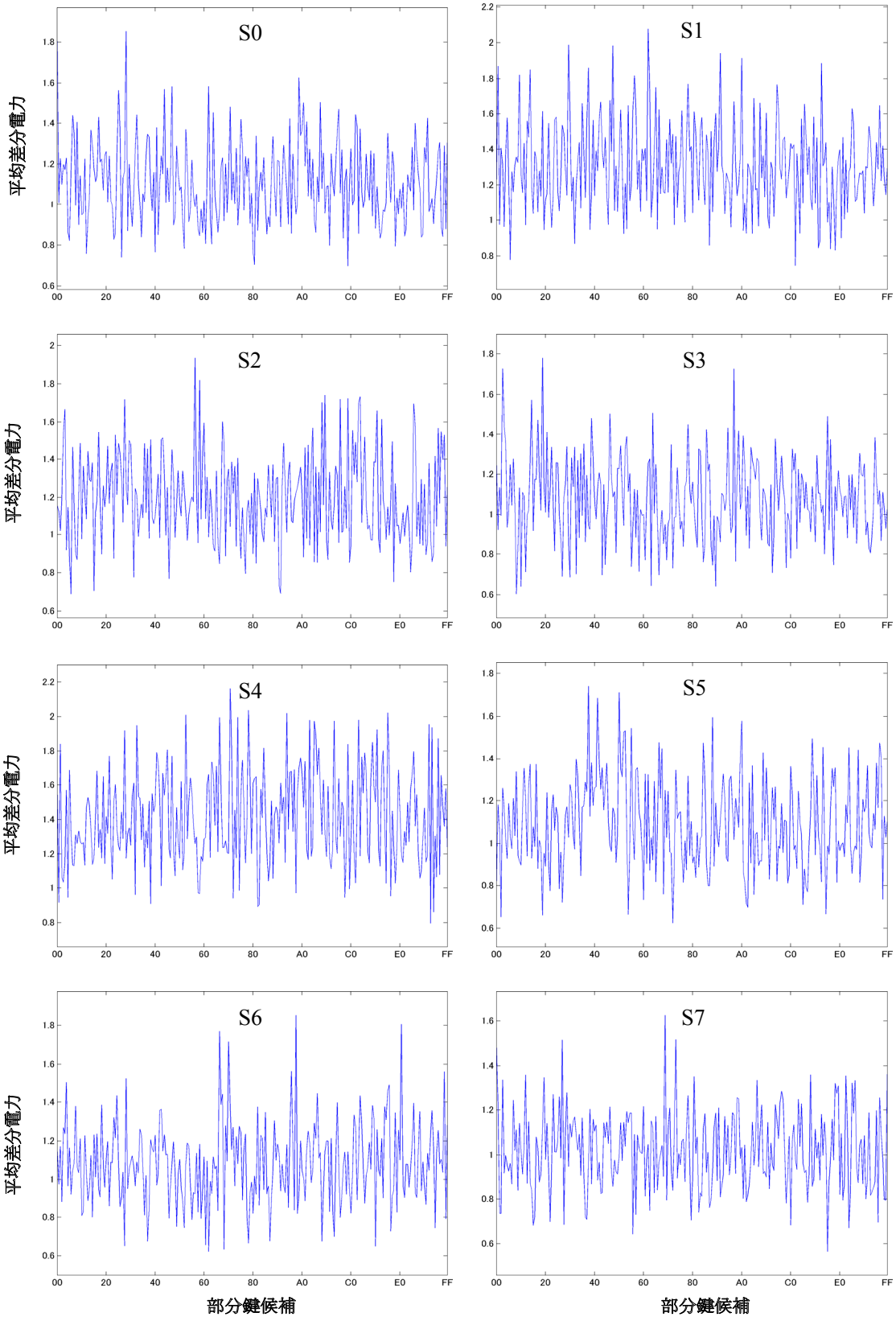

図 20-1　SASEBO-G 上の AES 回路(MAO)に対する W2-DPA の平均差分電力

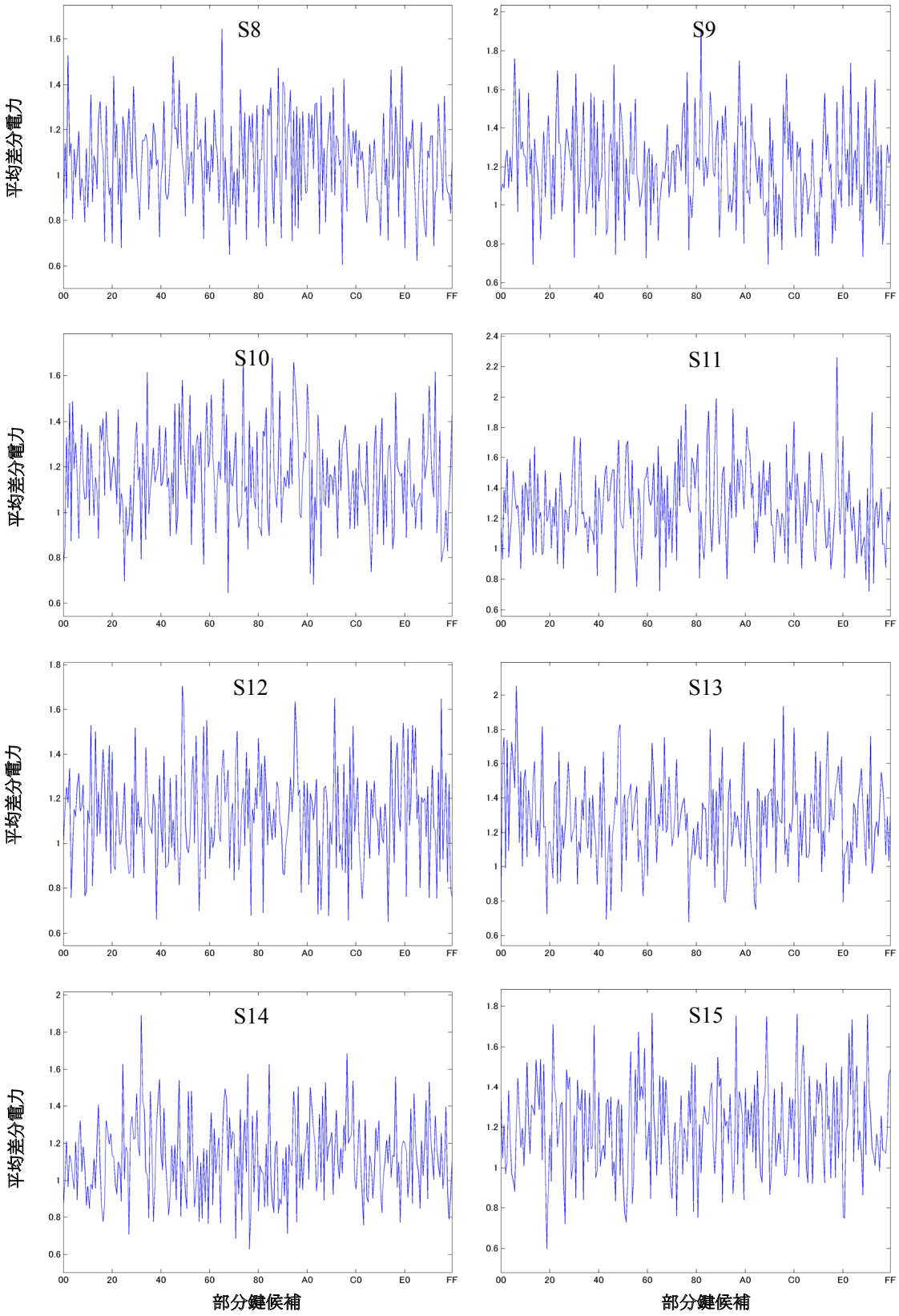

図 20-2　SASEBO-G 上の AES 回路(MAO)に対する W2-DPA の平均差分電力

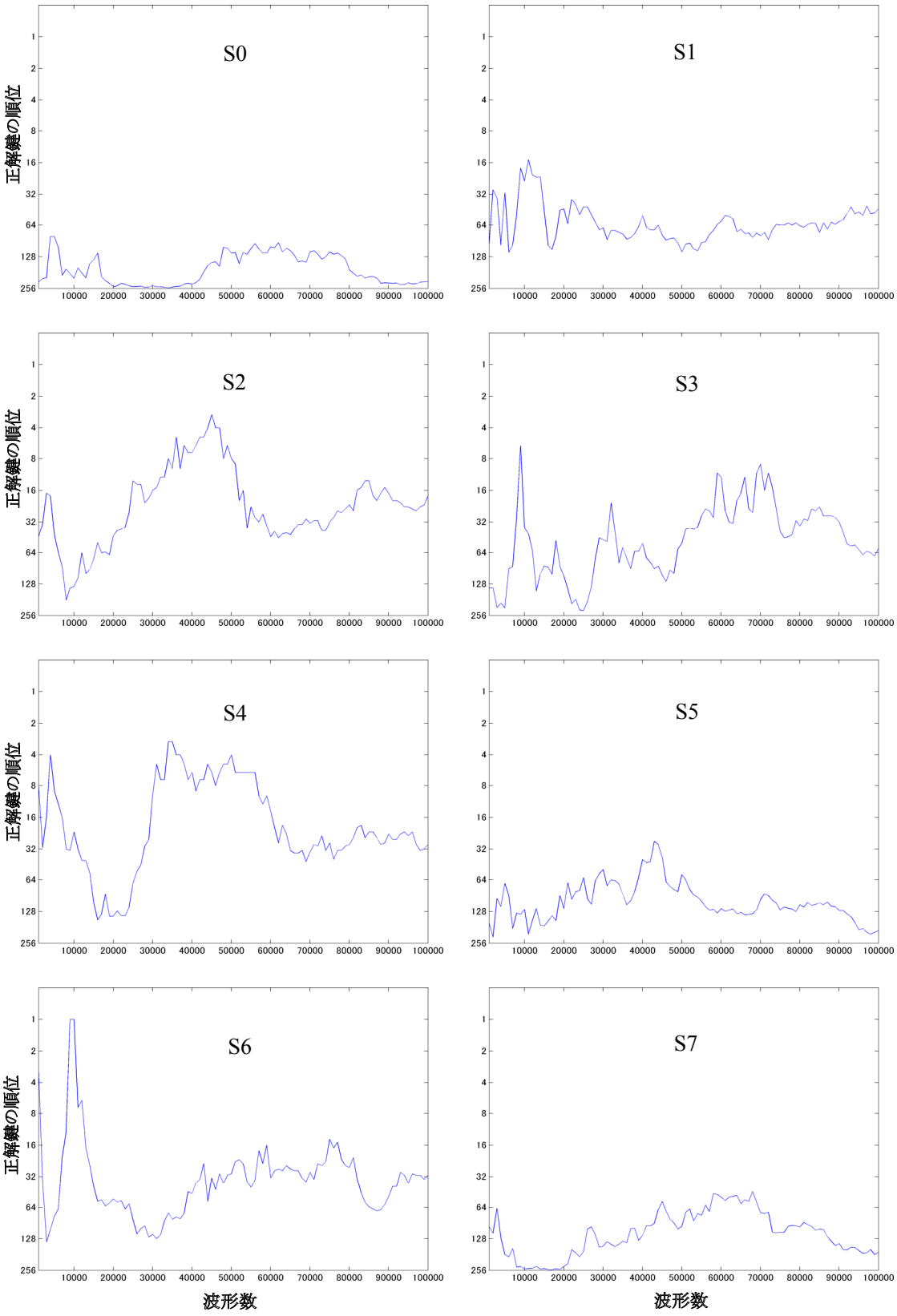

図 21-1　SASEBO-G 上の AES 回路(MAO)に対する W2-DPA の精度と波形数の関係

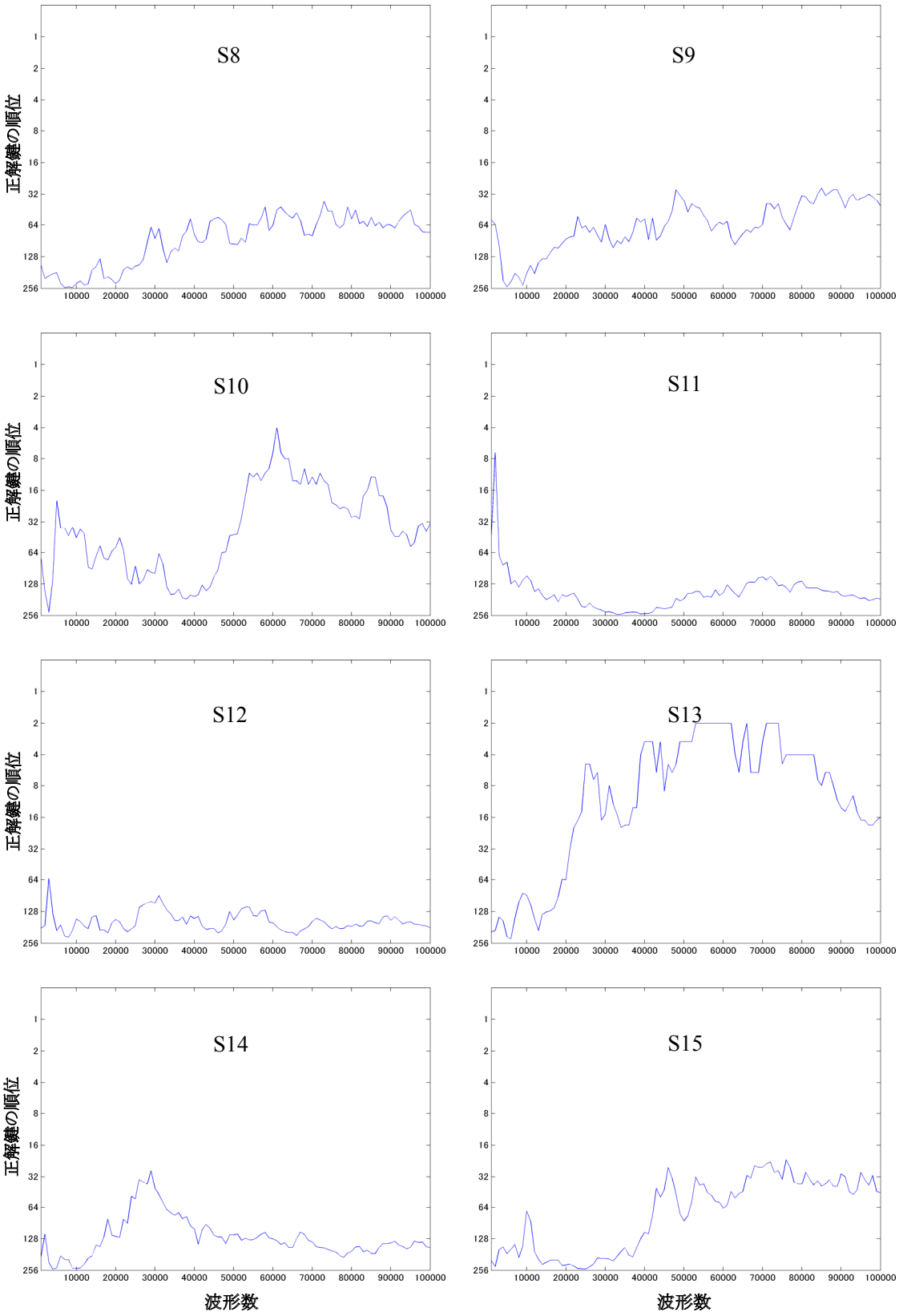

図 21-2　SASEBO-G 上の AES 回路(MAO)に対する W2-DPA の精度と波形数の関係

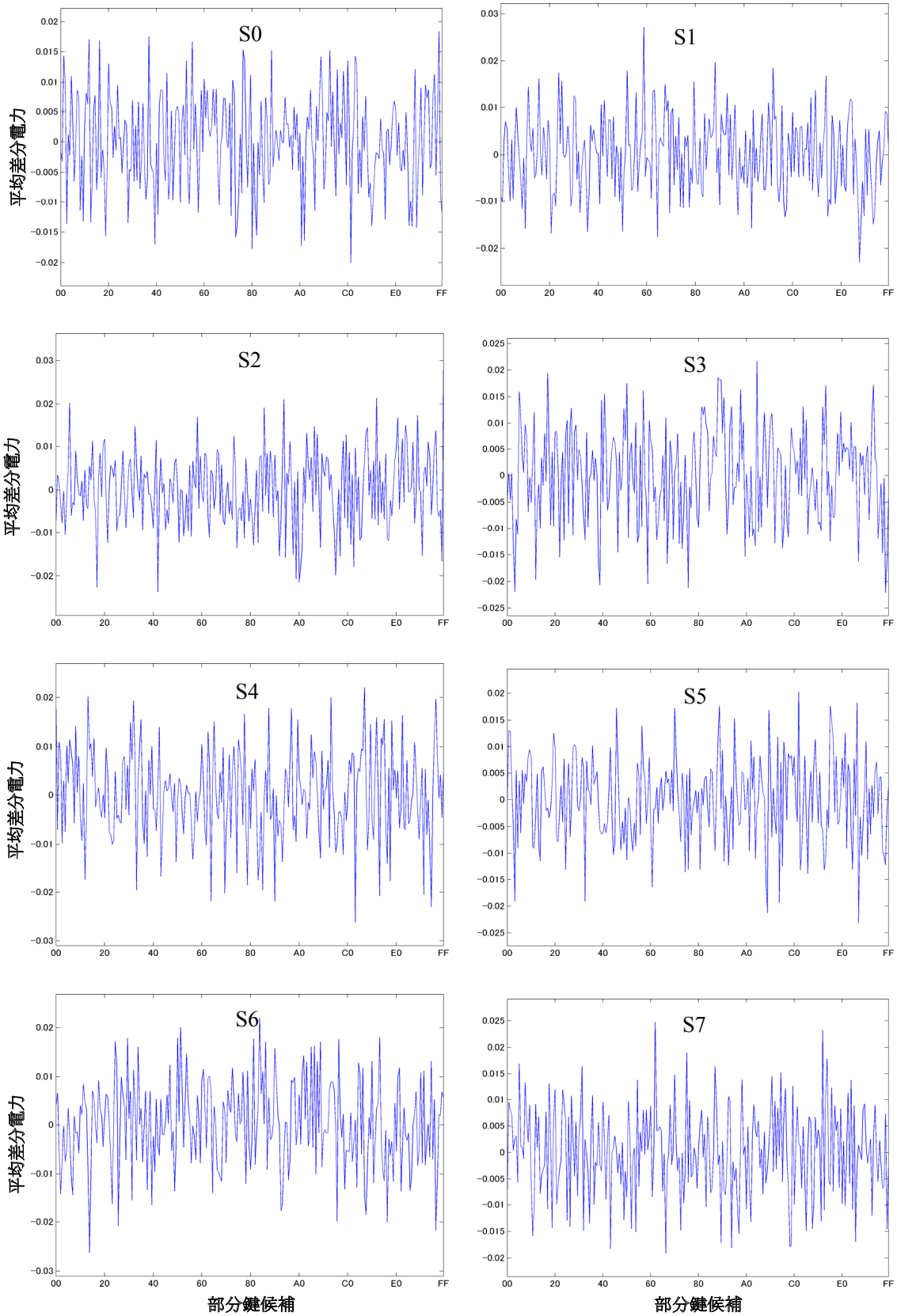

図 22-1　SASEBO-G 上の AES 回路(MAO)に対する CPA の平均差分電力

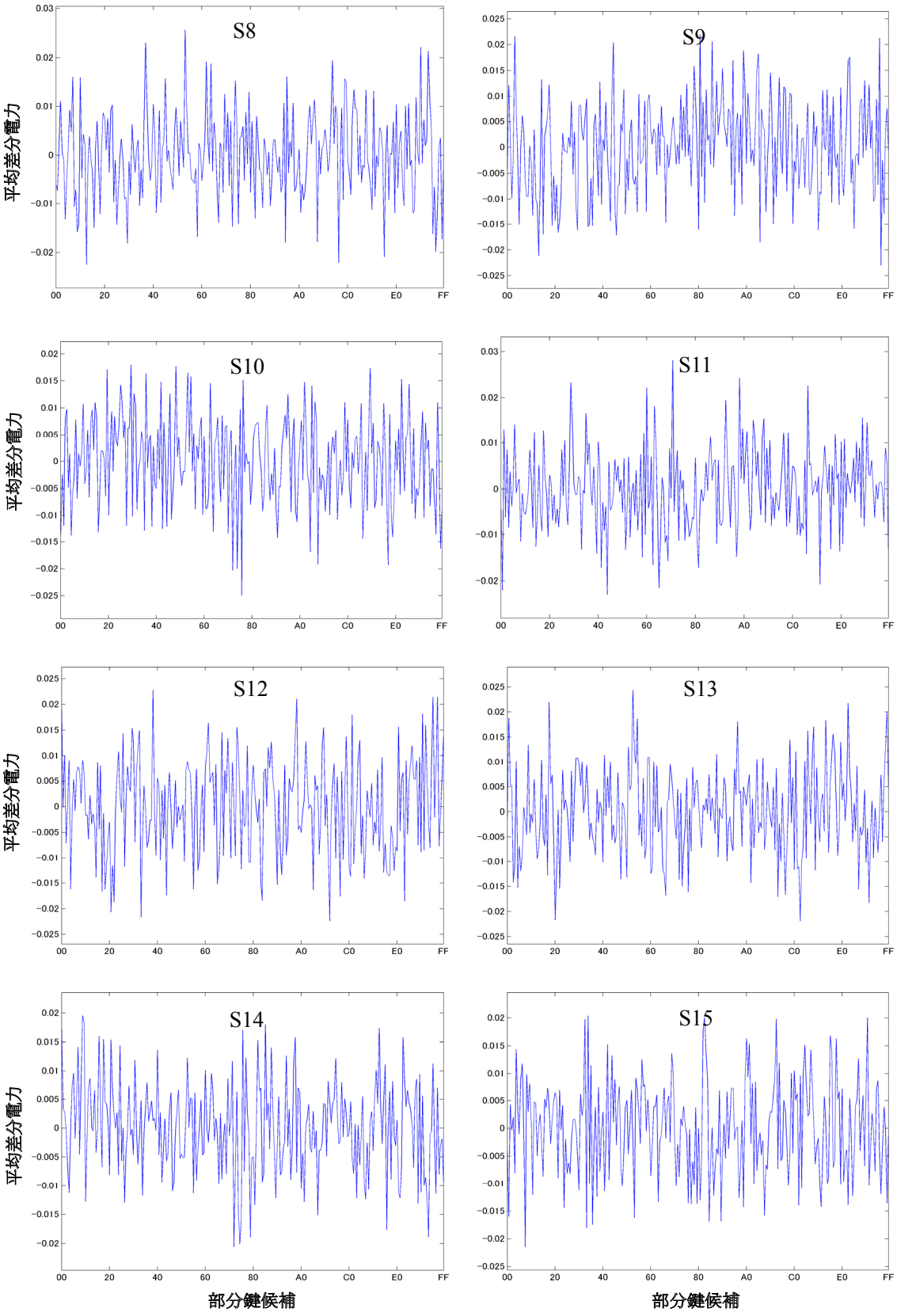

図 22-2　SASEBO-G 上の AES 回路(MAO)に対する CPA の平均差分電力

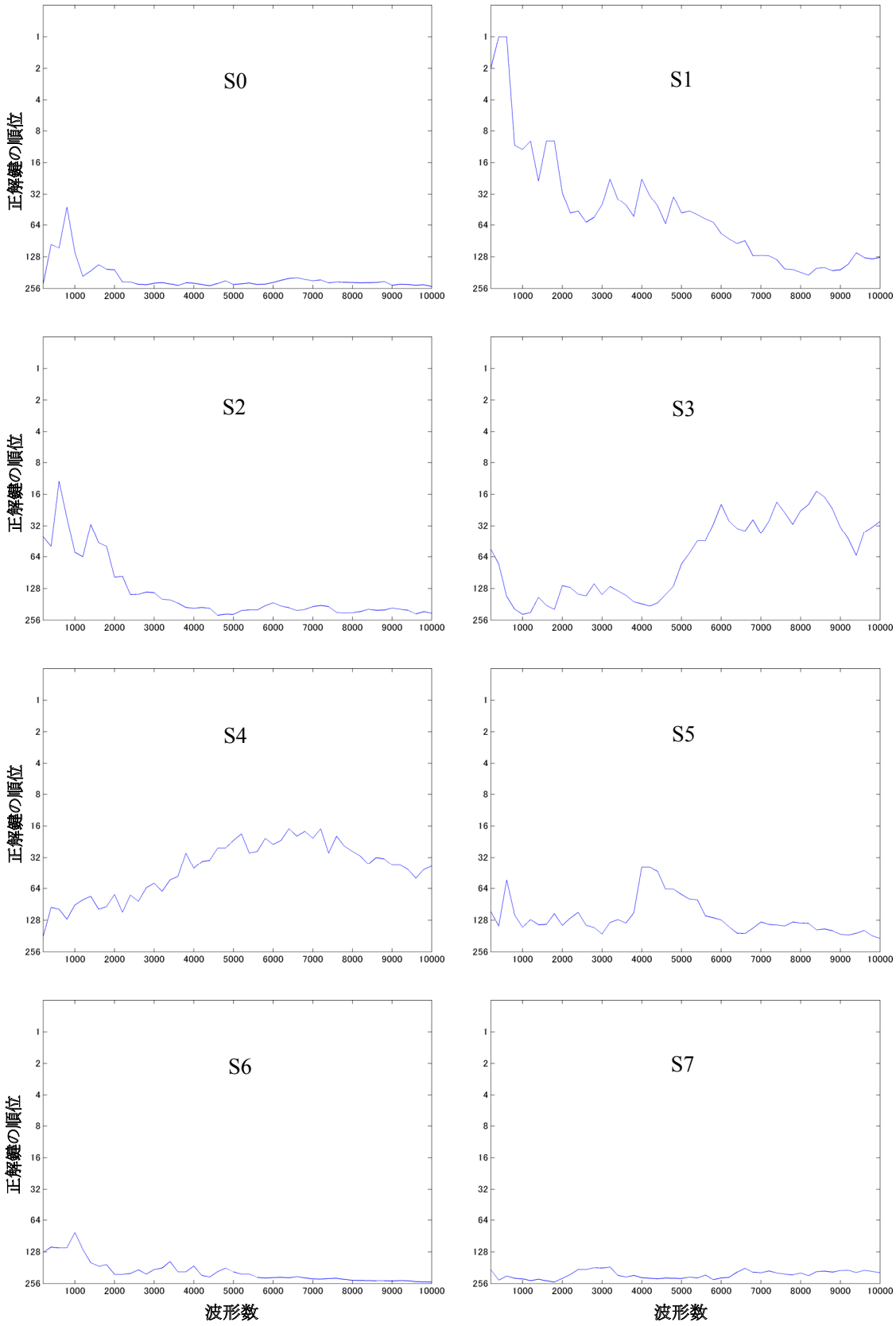

図 23-1　SASEBO-G 上の AES 回路(MAO)に対する CPA の精度と波形数の関係

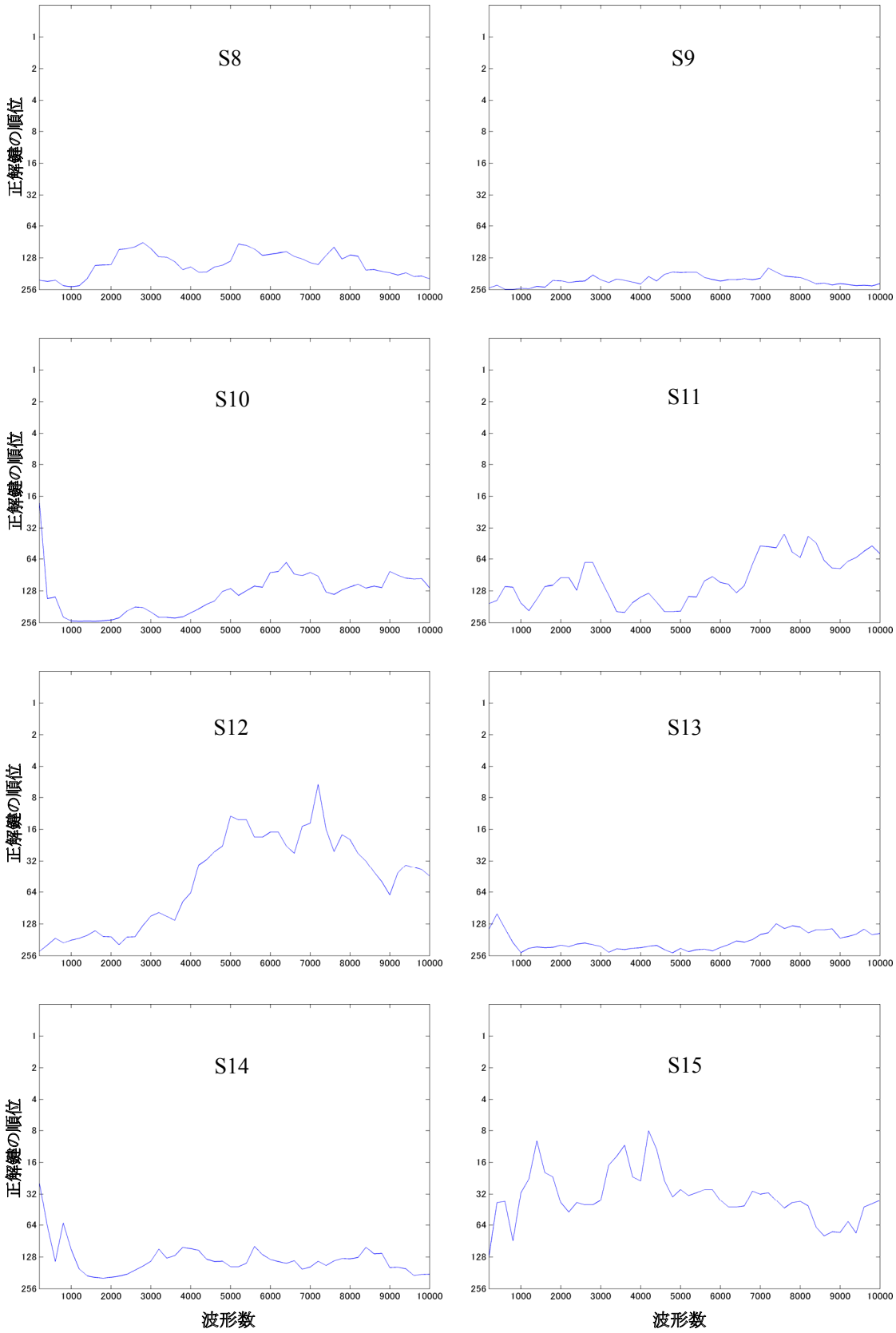

図 23-2　SASEBO-G 上の AES 回路(MAO)に対する CPA の精度と波形数の関係

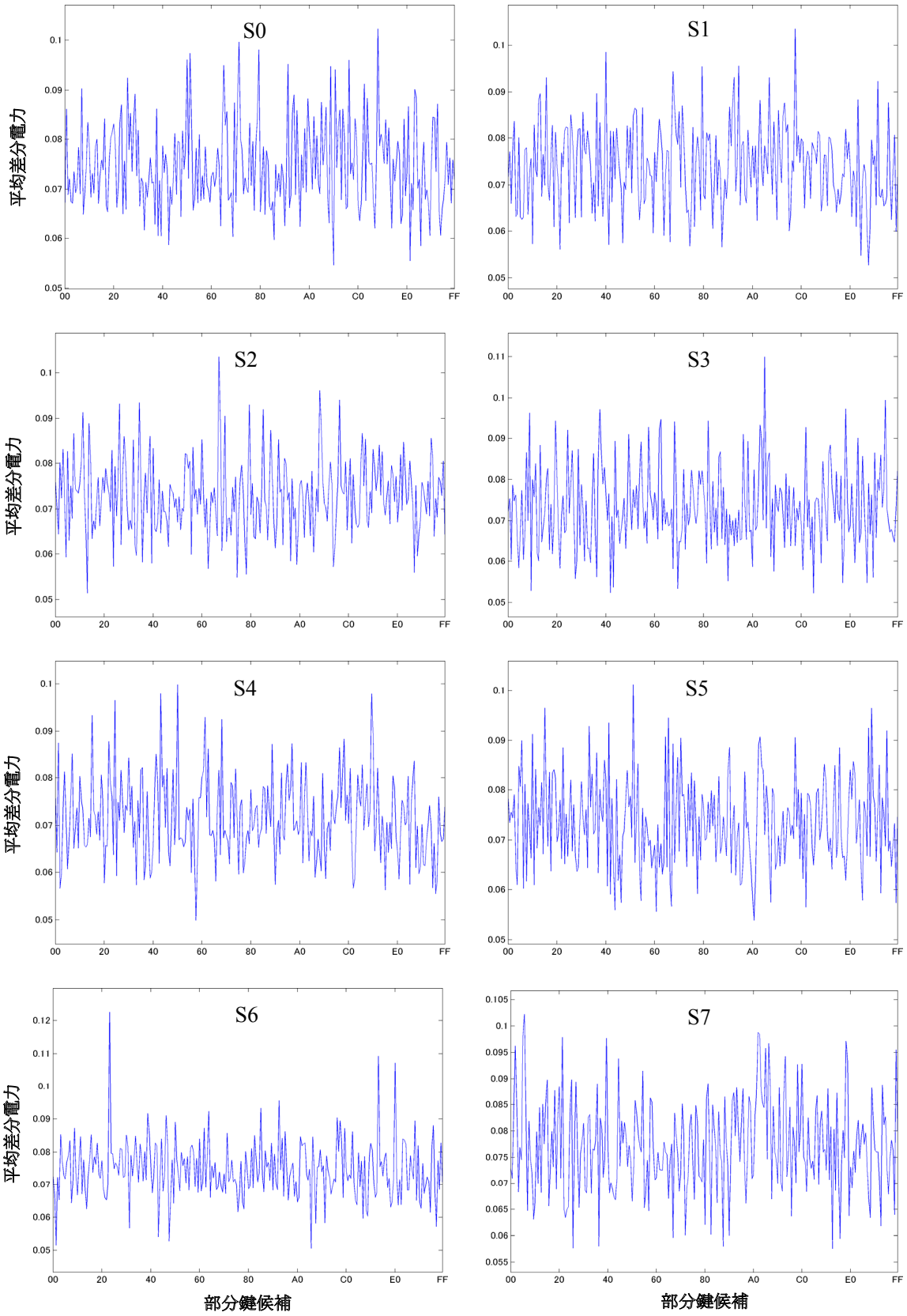

図 24-1 SASEBO-G 上の AES 回路(WDDL)に対する DPA の平均差分電力(Precharge フェーズ)

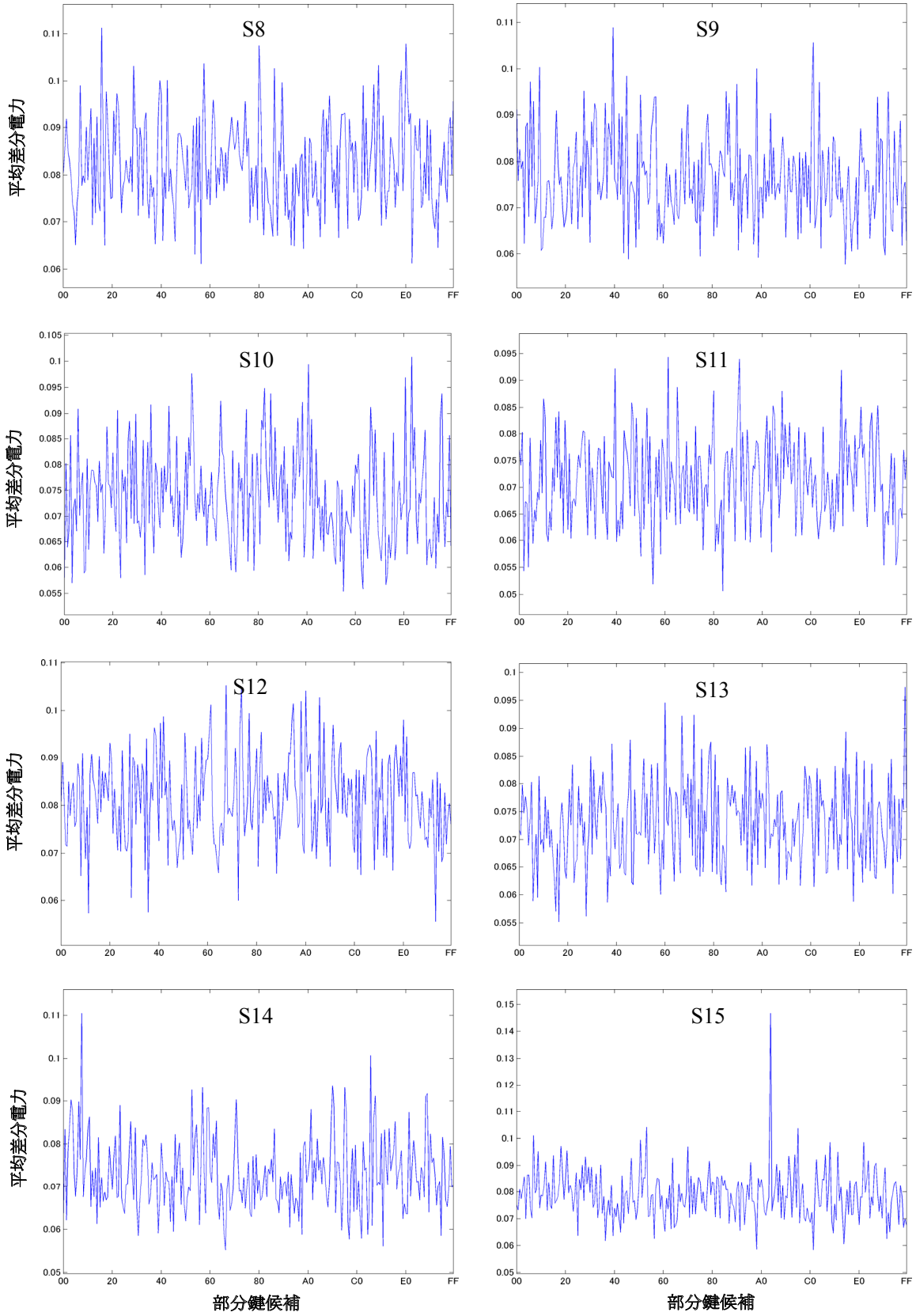

図 24-2 SASEBO-G 上の AES 回路(WDDL)に対する DPA の平均差分電力(Precharge フェーズ)

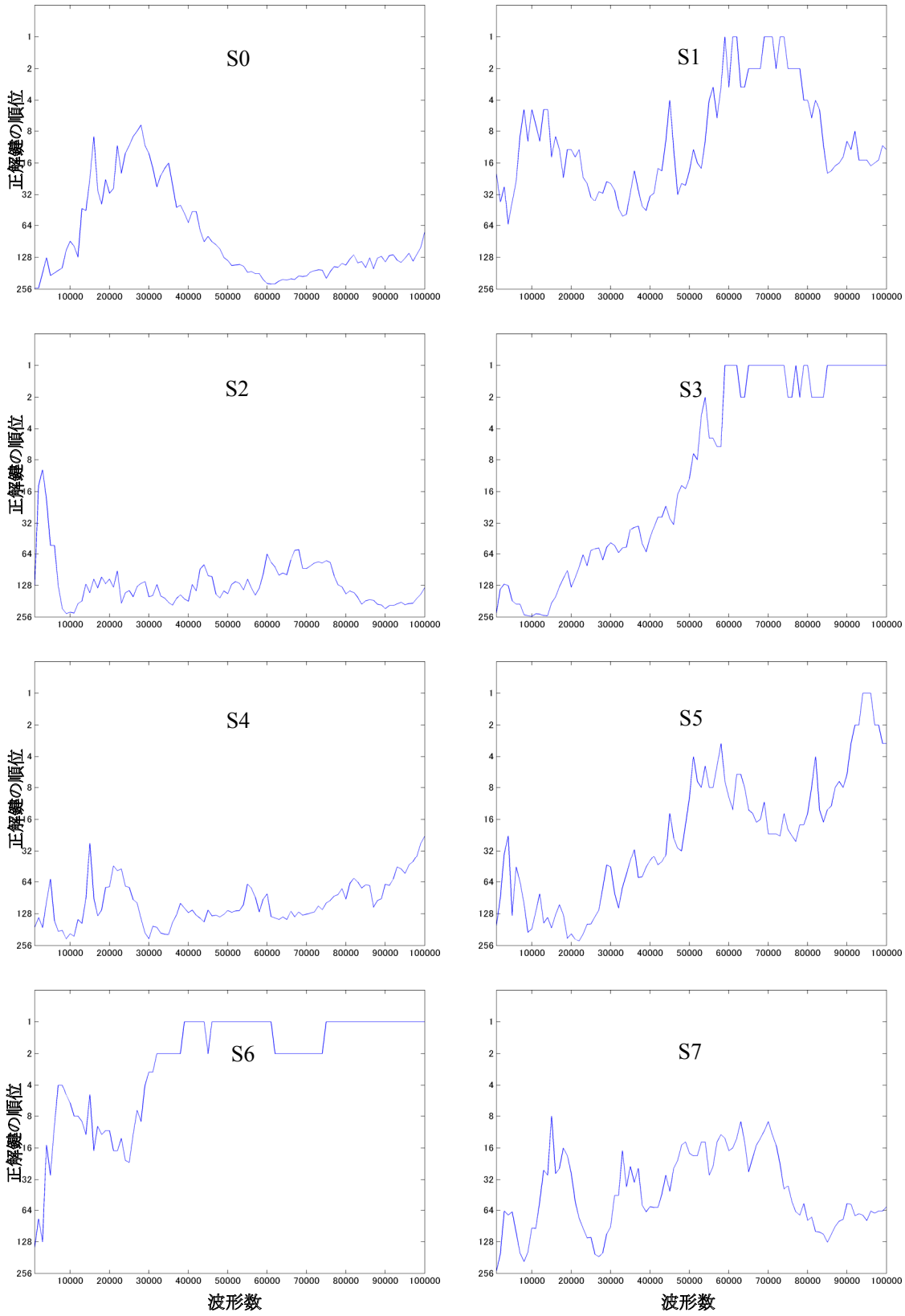

図 25-1　SASEBO-G 上の AES 回路(WDDL)に対する DPA の精度と波形数の関係
(Precharge フェーズ)

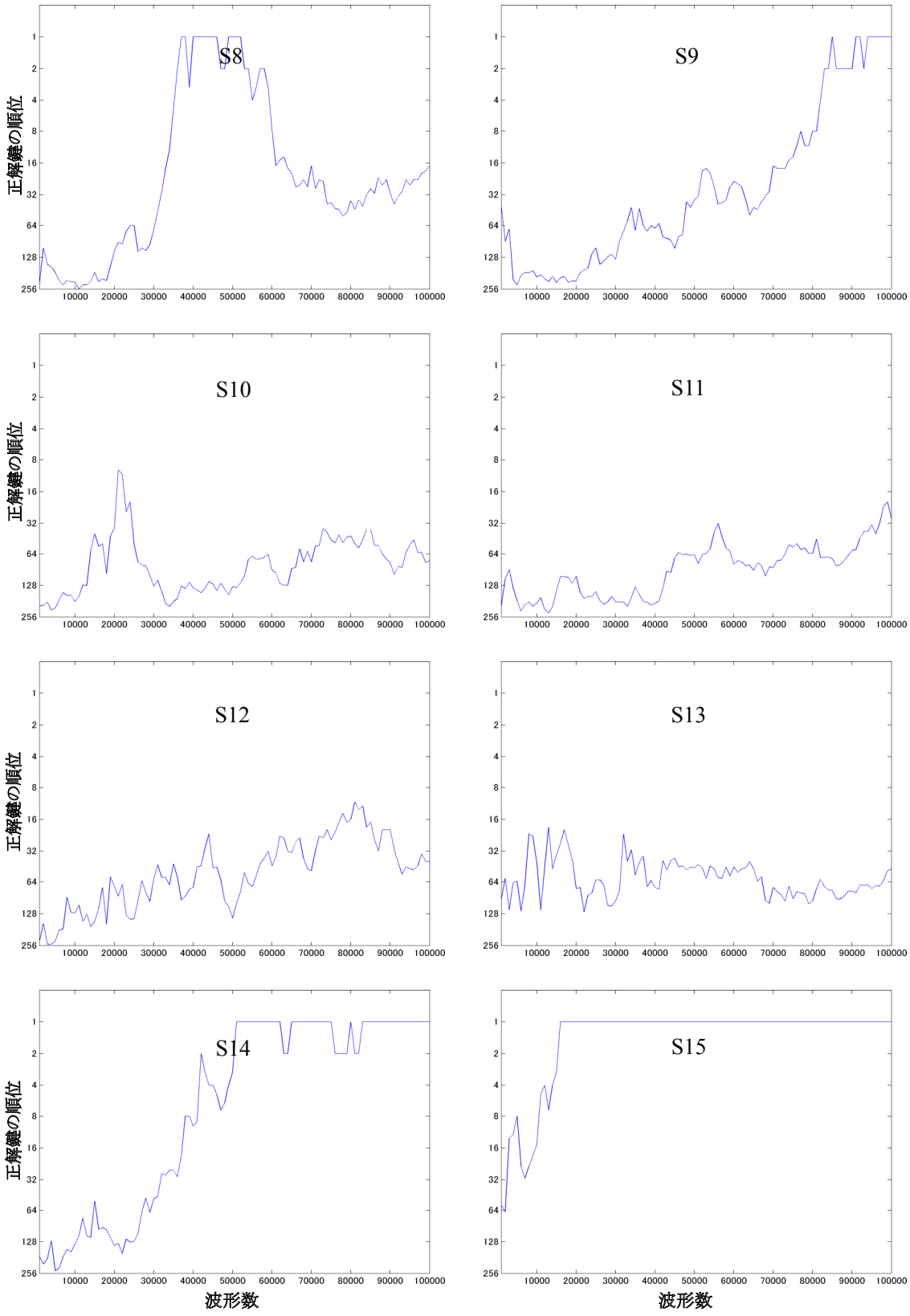

図 25-2　SASEBO-G 上の AES 回路(WDDL)に対する DPA の精度と波形数の関係
(Precharge フェーズ)

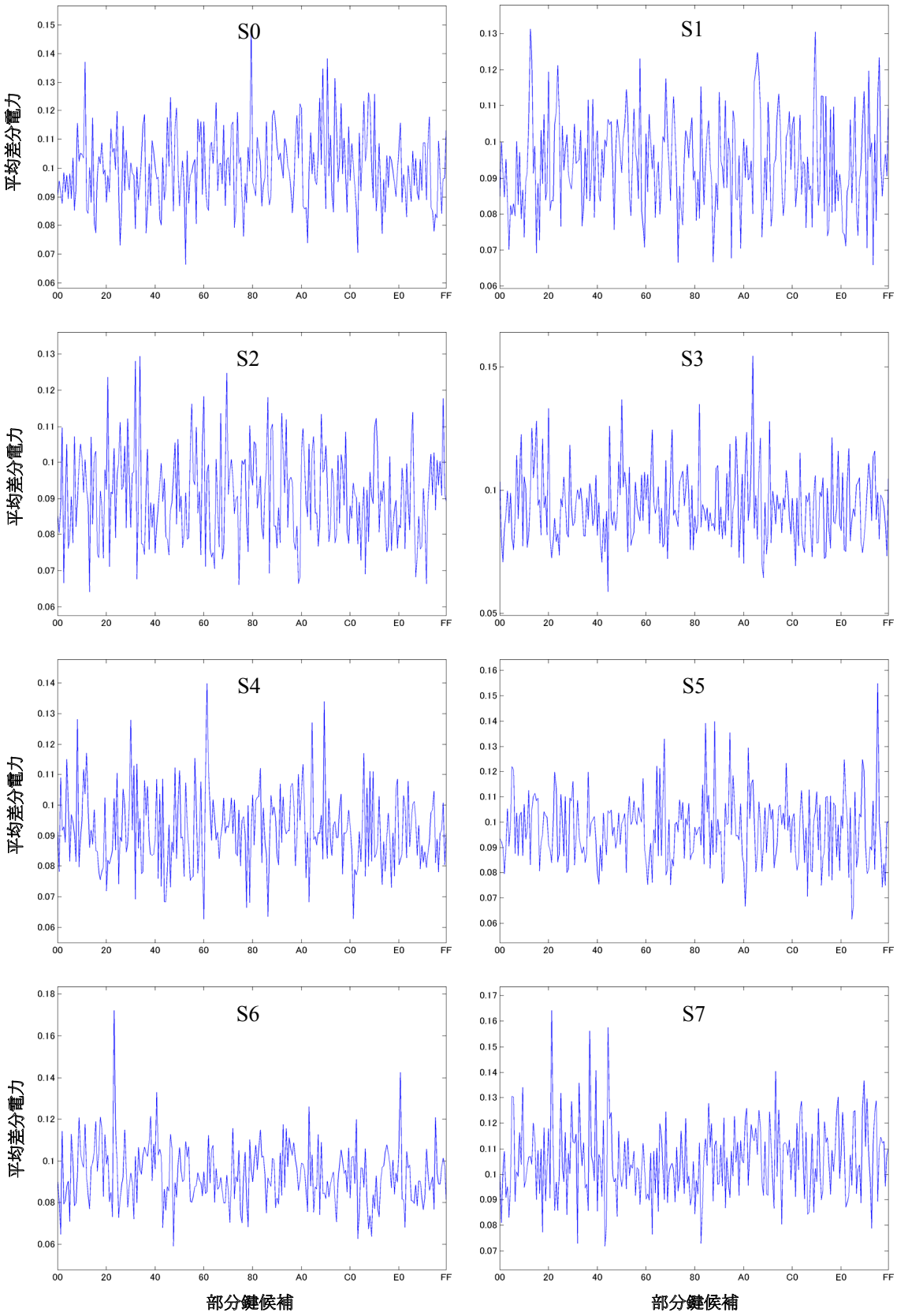

図 26-1 SASEBO-G 上の AES 回路(WDDL)に対する DPA の平均差分電力(Evaluation フェーズ)

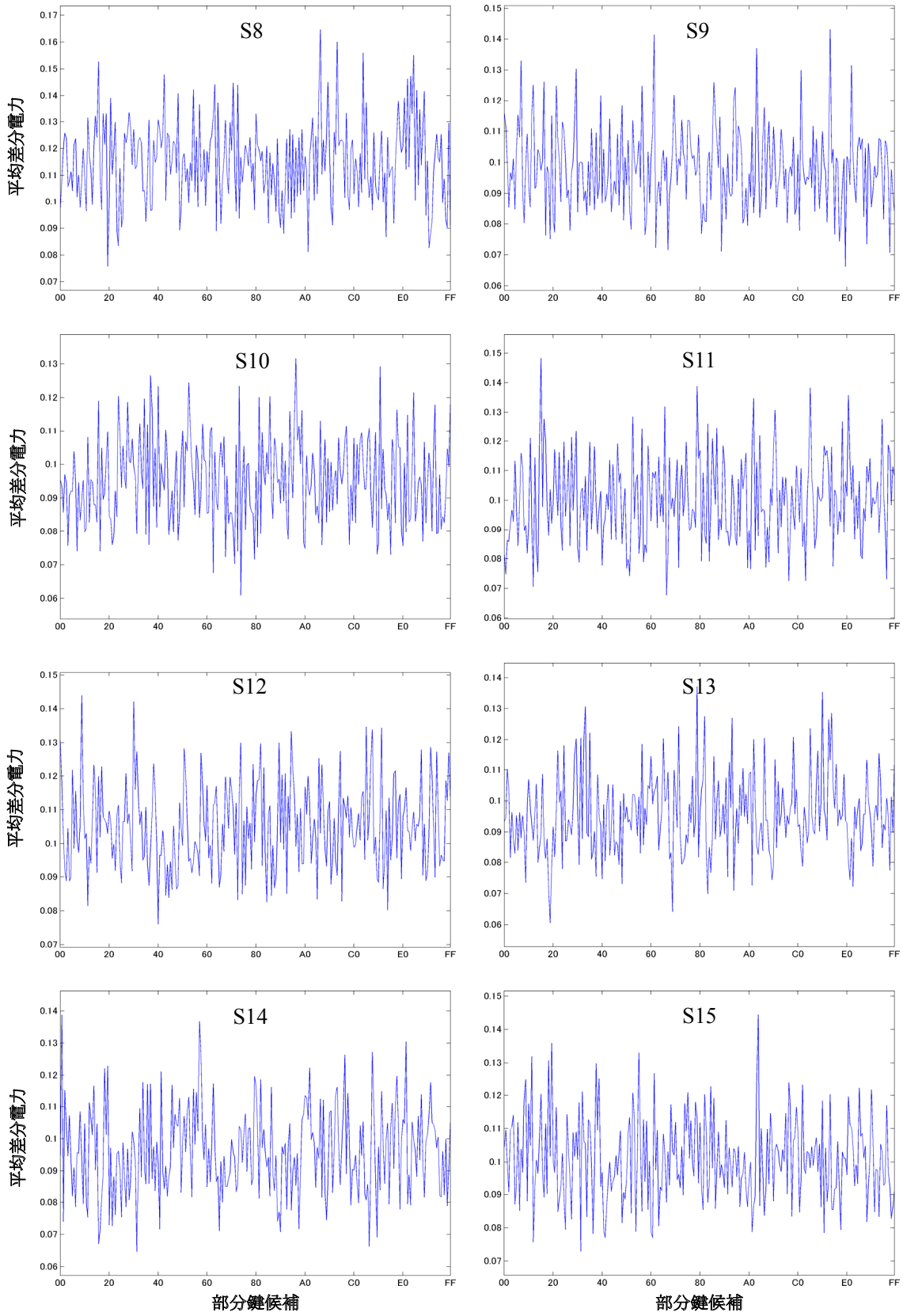

図 26-2 SASEBO-G 上の AES 回路(WDDL)に対する DPA の平均差分電力(Evaluation フェーズ)

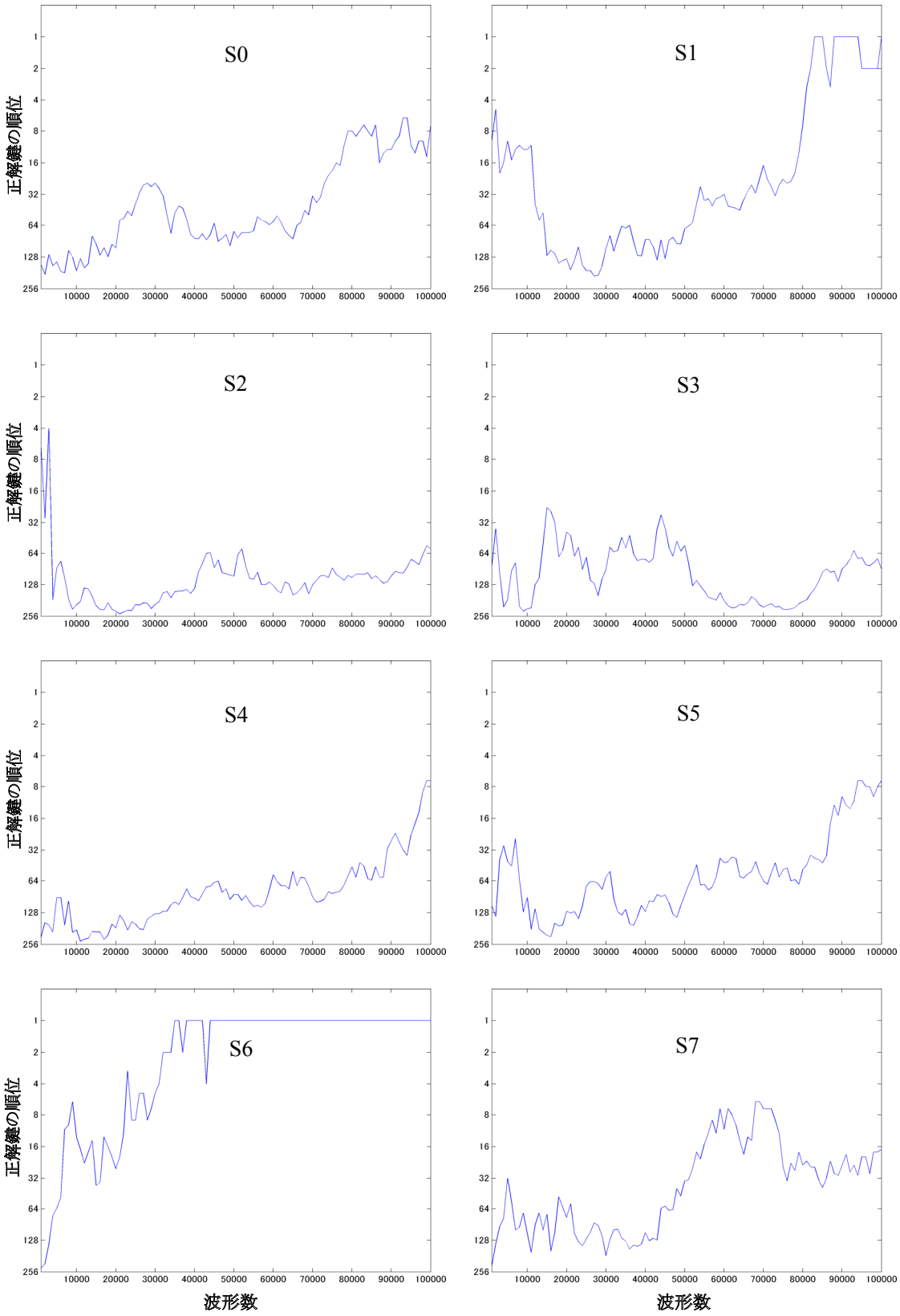

図 27-1　SASEBO-G 上の AES 回路(WDDL)に対する DPA の精度と波形数の関係
(Evaluate フェーズ)

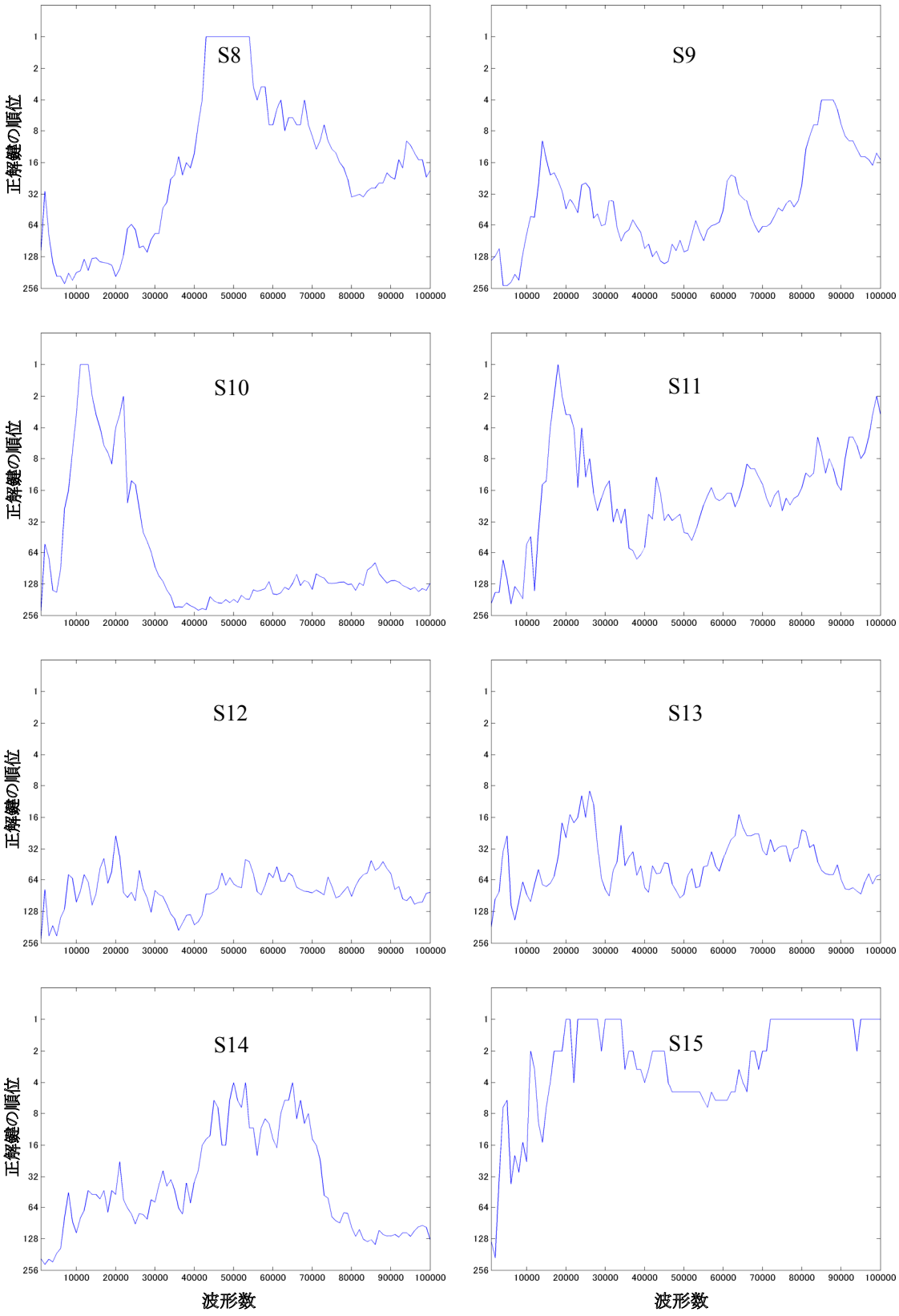

図 27-2　SASEBO-G 上の AES 回路(WDDL)に対する DPA の精度と波形数の関係
(Evaluate フェーズ)

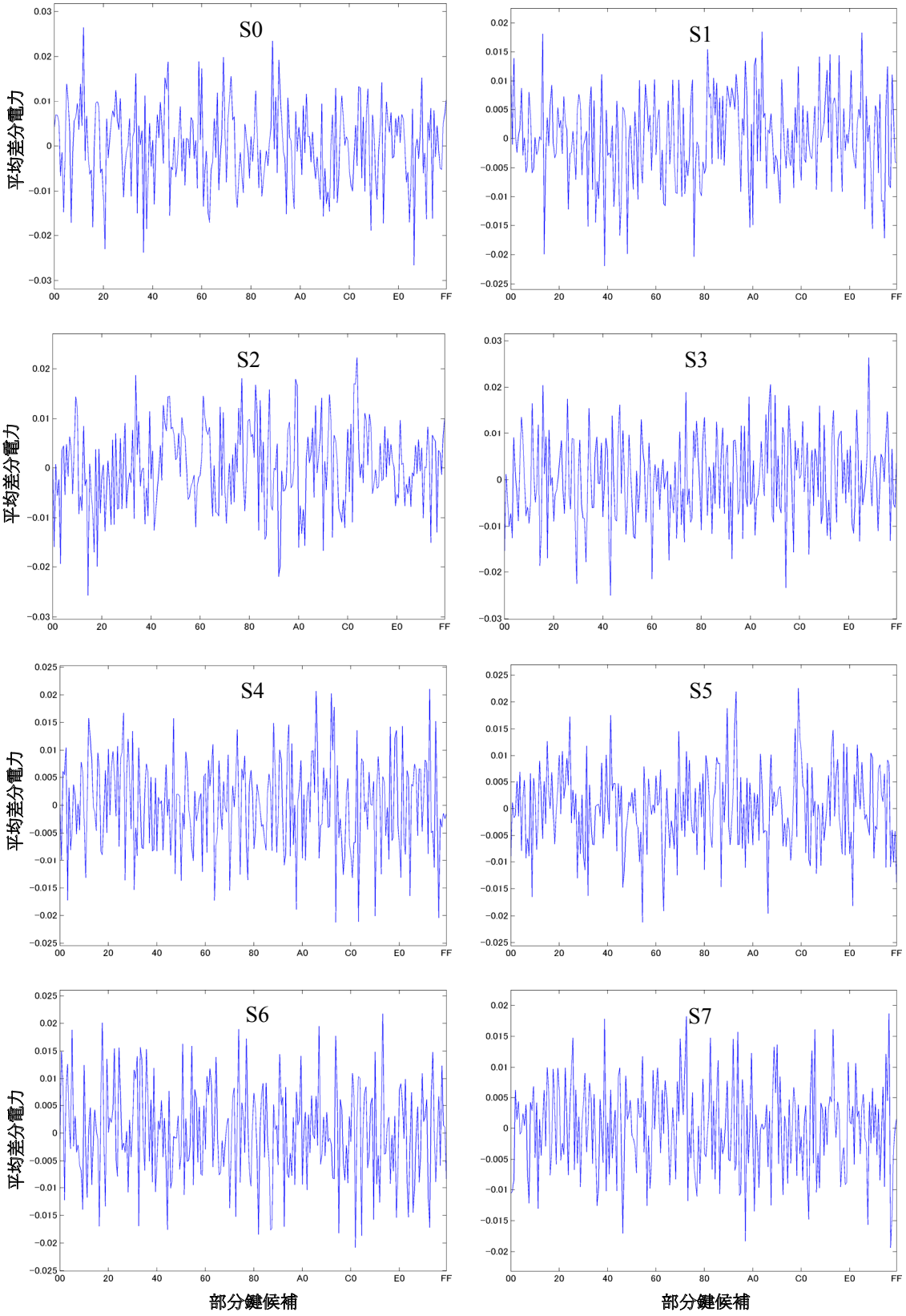

図 28-1 SASEBO-G 上の AES 回路(WDDL)に対する CPA の相関値
(Evaluate フェーズ)

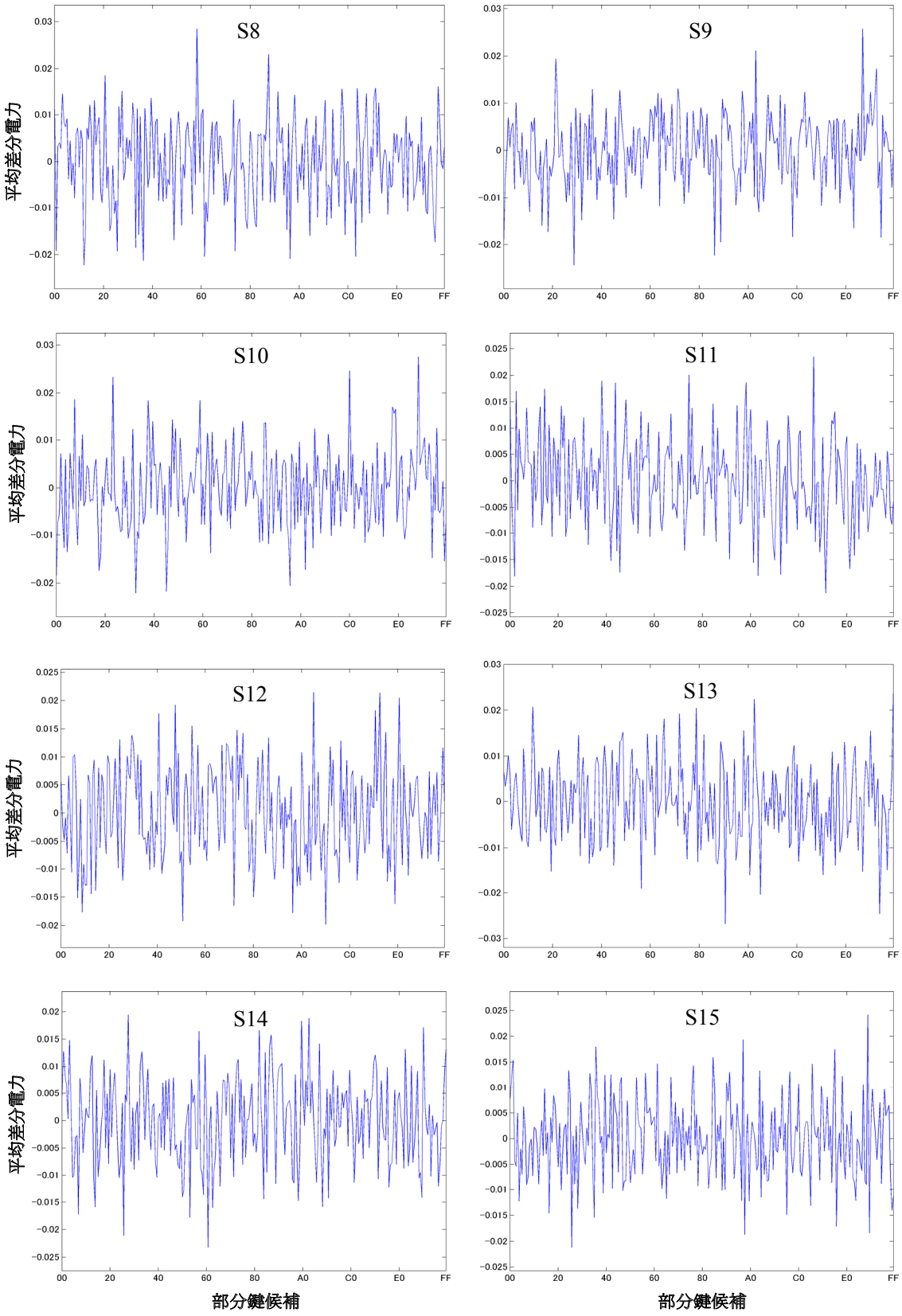

図 28-2 SASEBO-G 上の AES 回路(WDDL)に対する CPA の相関値
(Evaluate フェーズ)

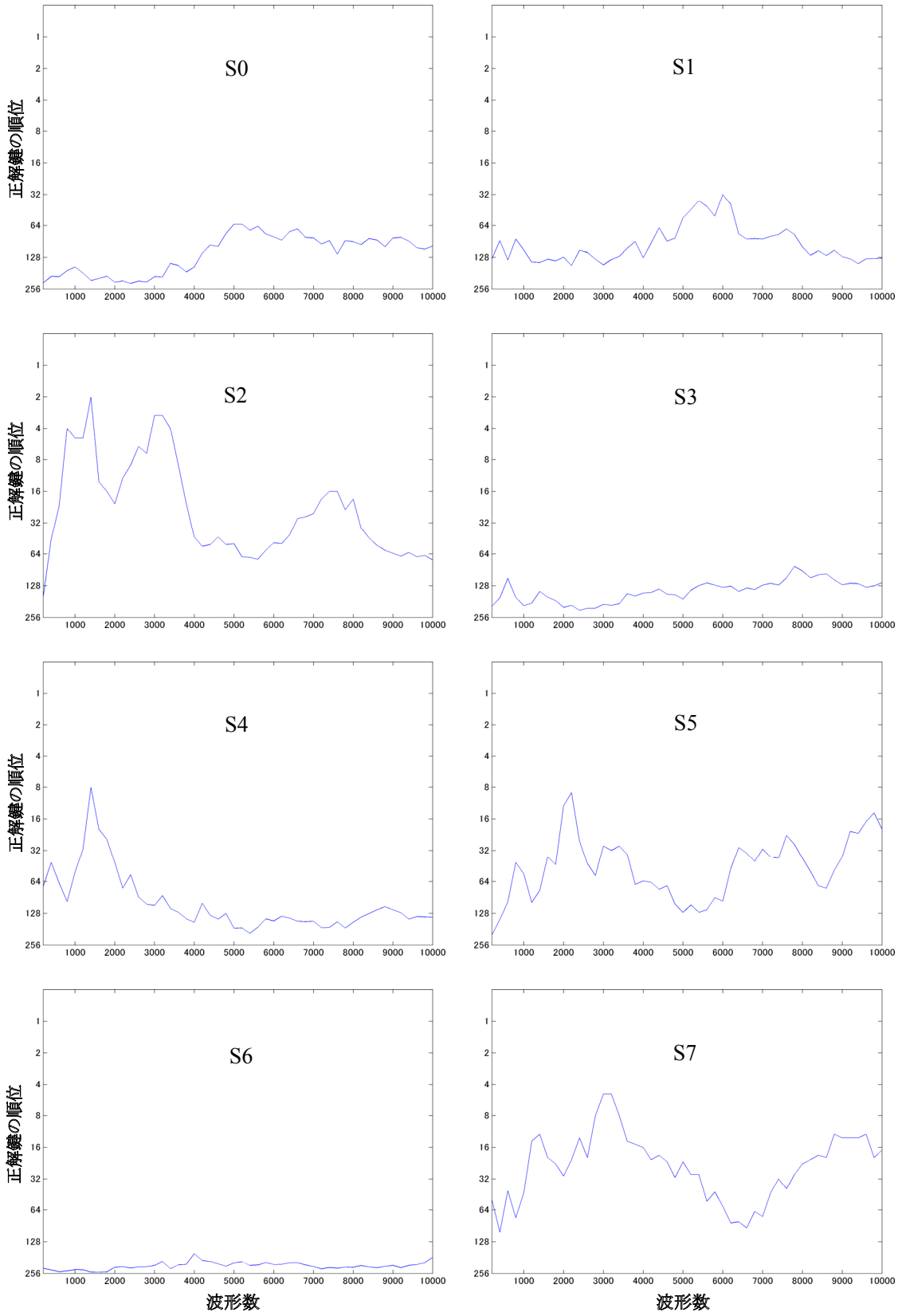

図 29-1　SASEBO-G 上の AES 回路(WDDL)に対する CPA の精度と波形数の関係
(Evaluate フェーズ)

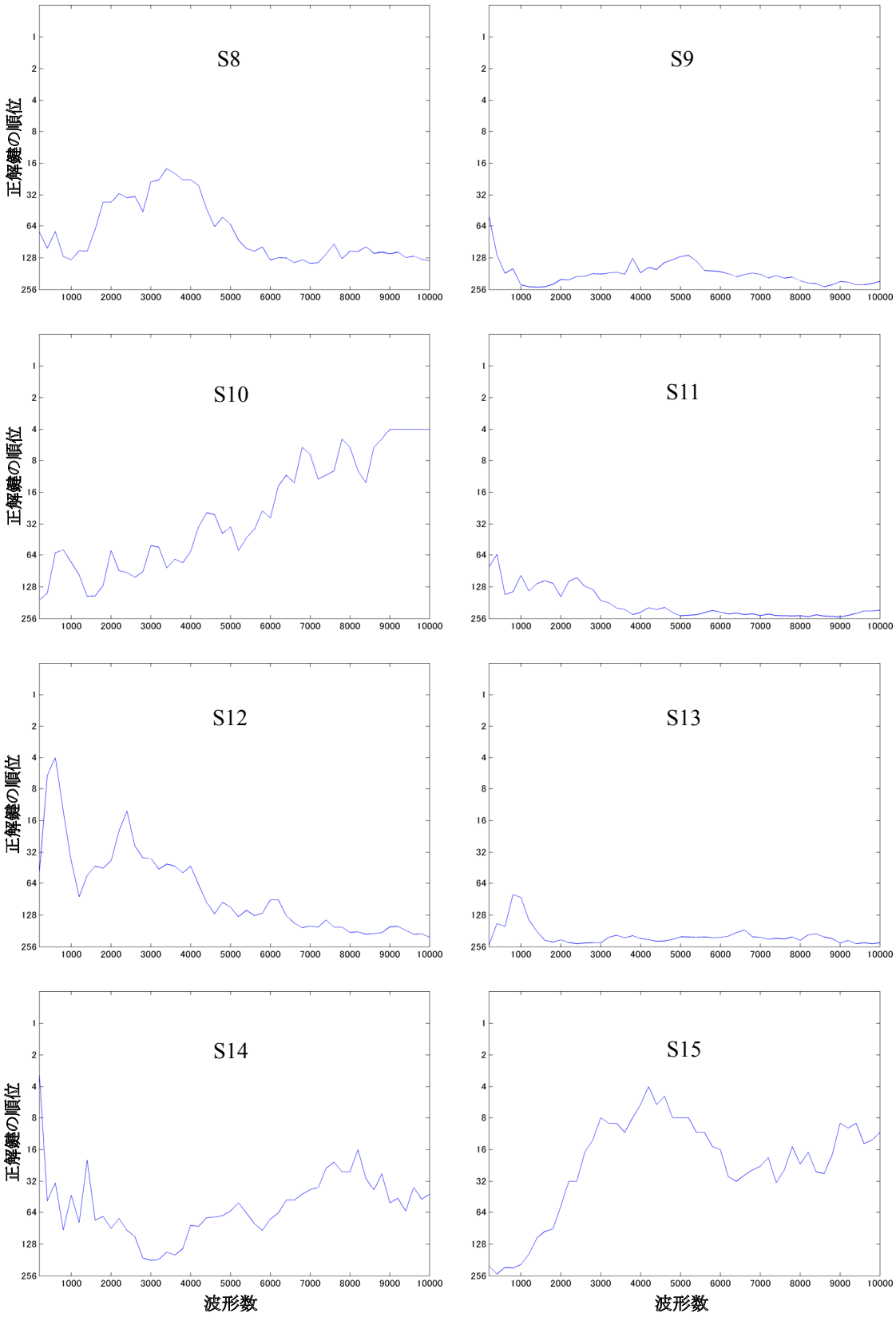

図 29-2　SASEBO-G 上の AES 回路(WDDL)に対する CPA の精度と波形数の関係
(Evaluate フェーズ)

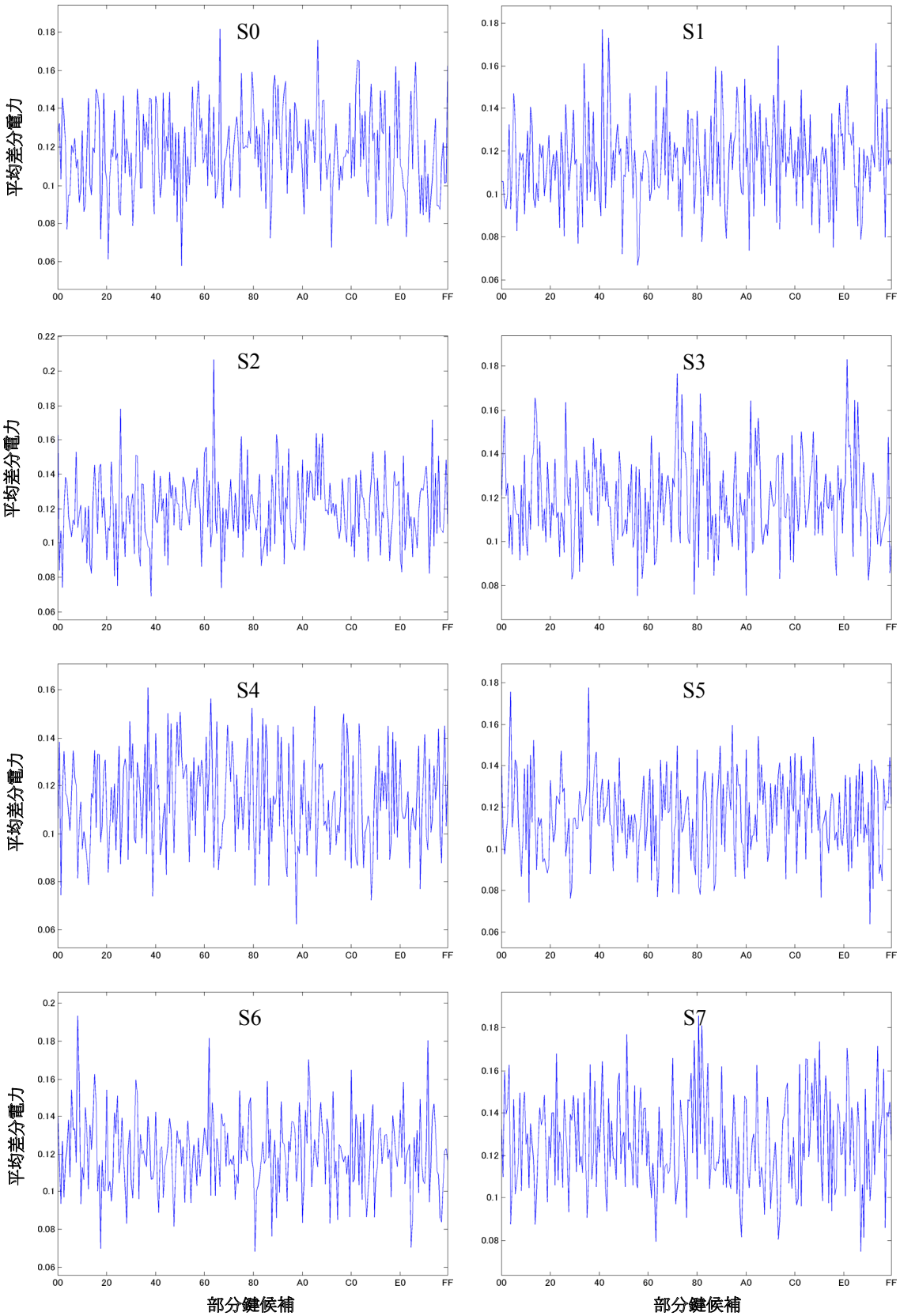

図 30-1 SASEBO-G 上の AES 回路(MDPL)に対する DPA の平均差分電力

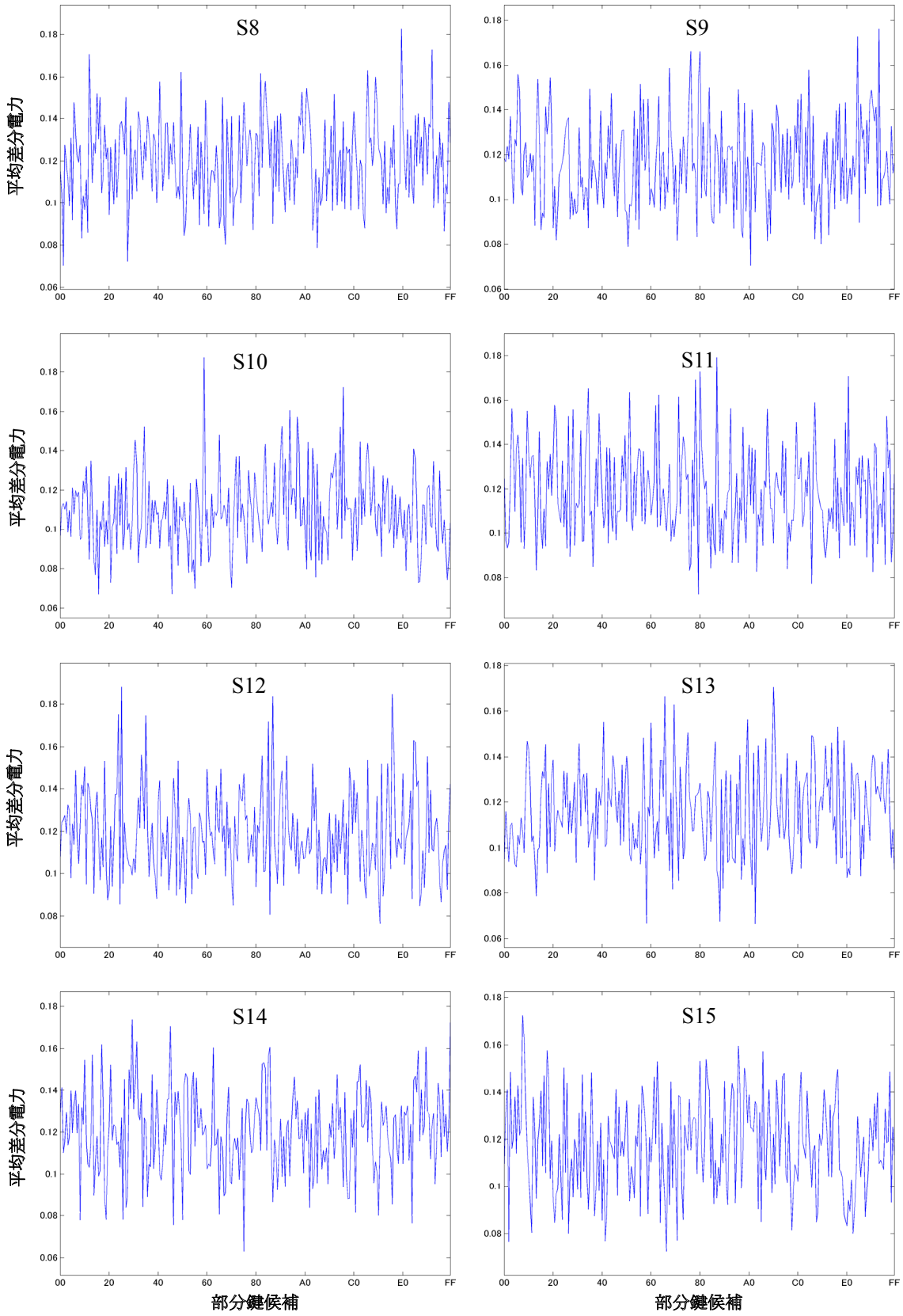

図 30-2 SASEBO-G 上の AES 回路(MDPL)に対する DPA の平均差分電力

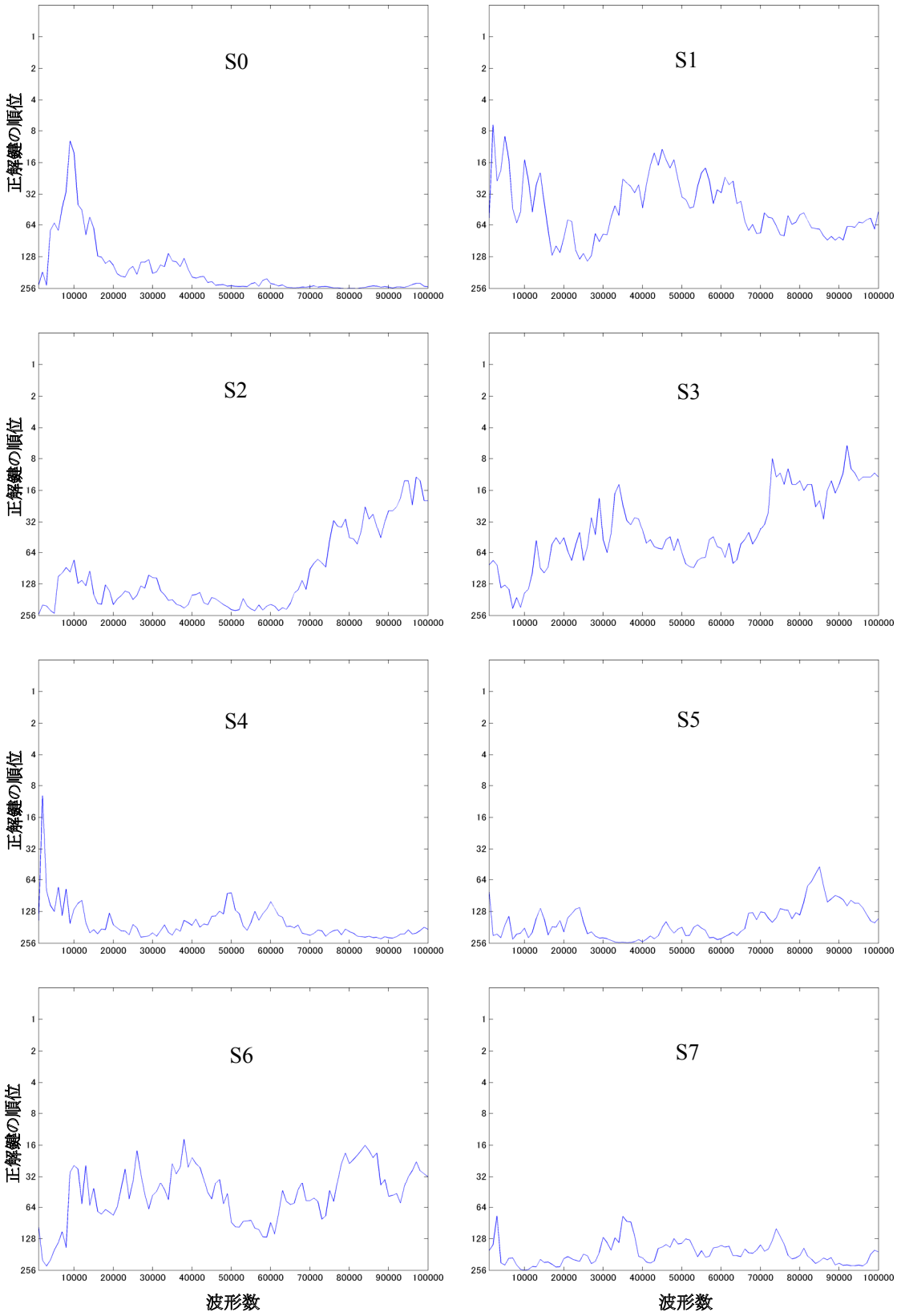

図 31-1　SASEBO-G 上の AES 回路(MDPL)に対する DPA の精度と波形数の関係

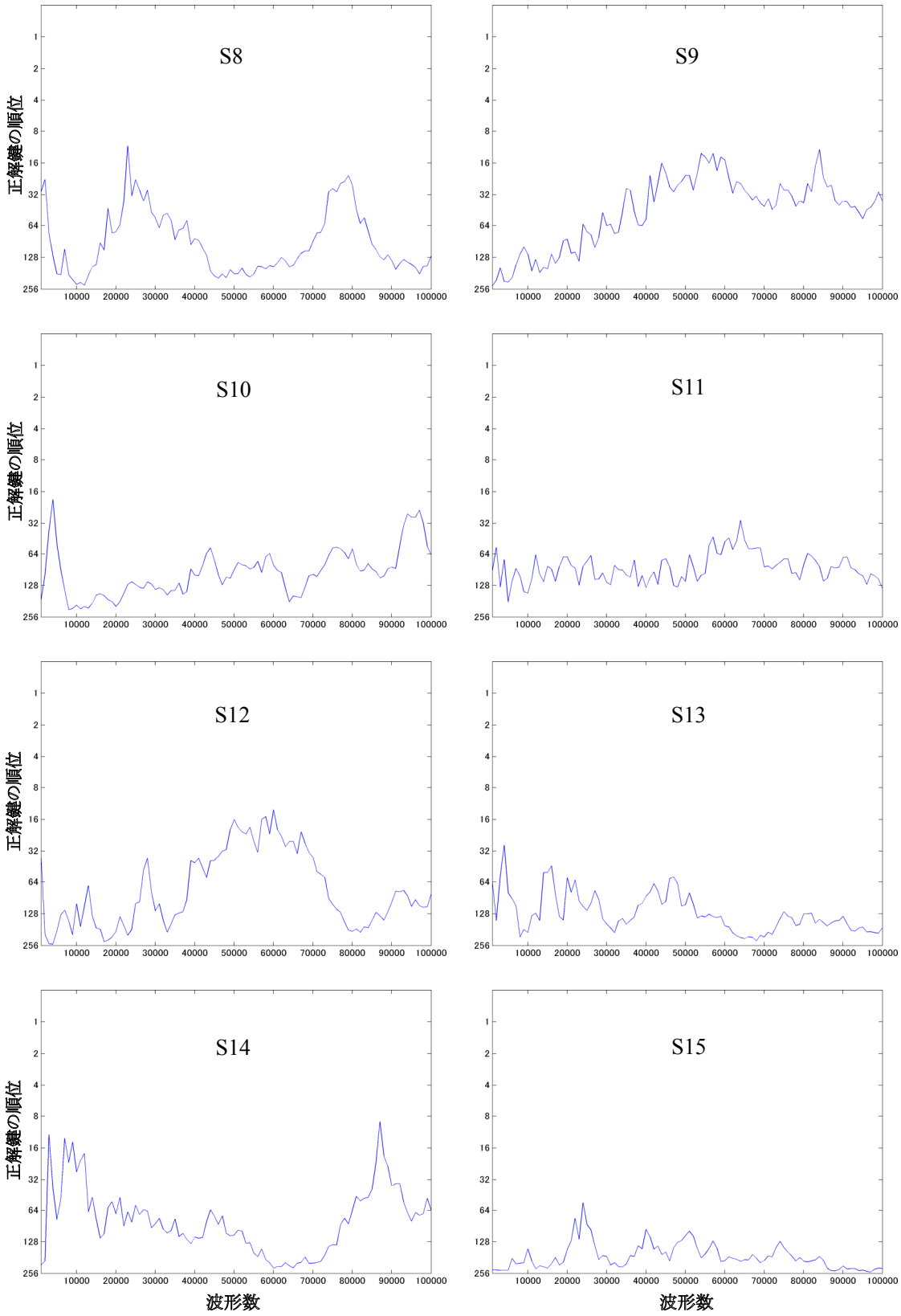

図 31-2　SASEBO-G 上の AES 回路(MDPL)に対する DPA の精度と波形数の関係

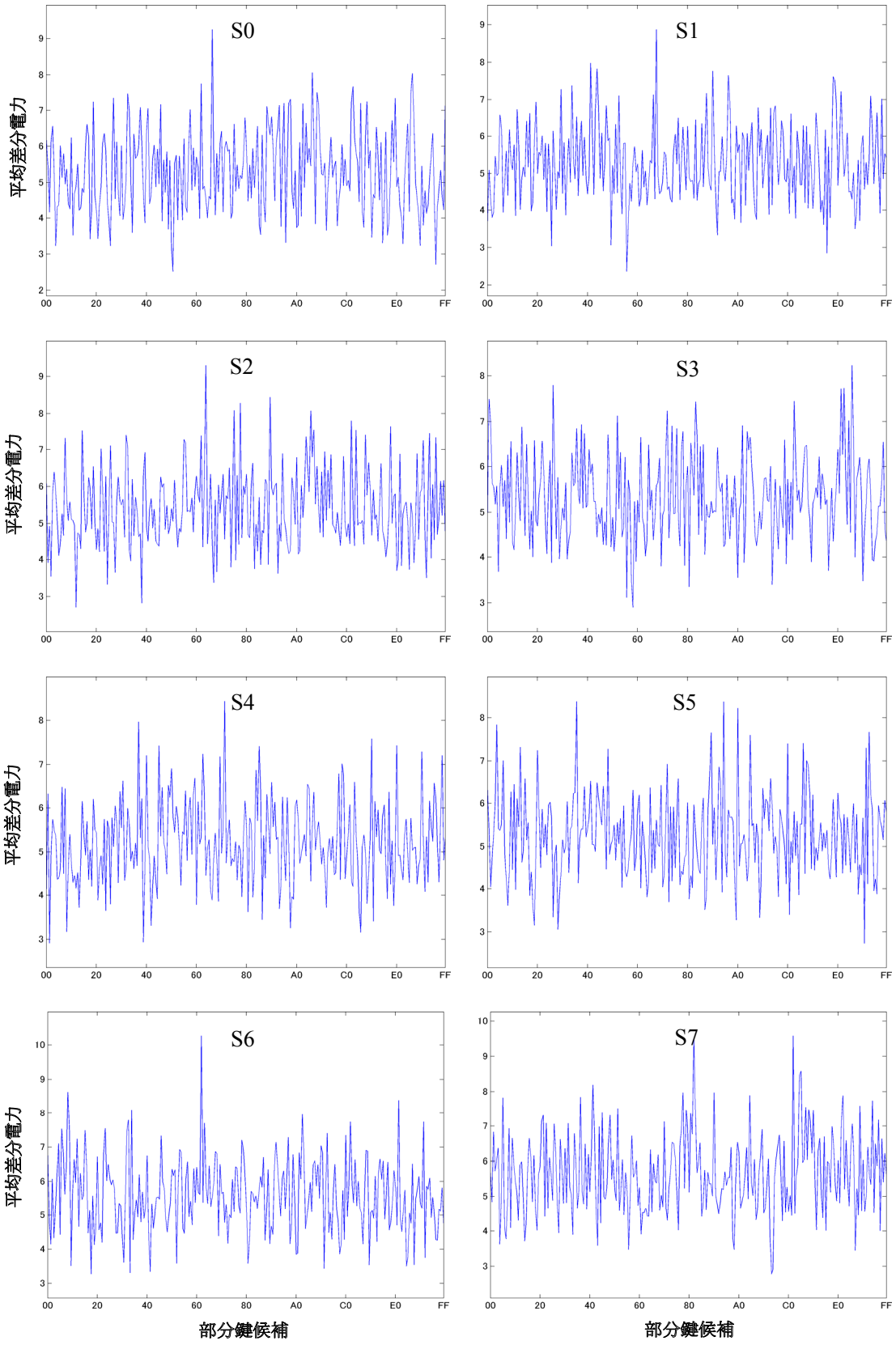

図 32-1　SASEBO-G 上の AES 回路(MDPL)に対する W2-DPA の平均差分電力

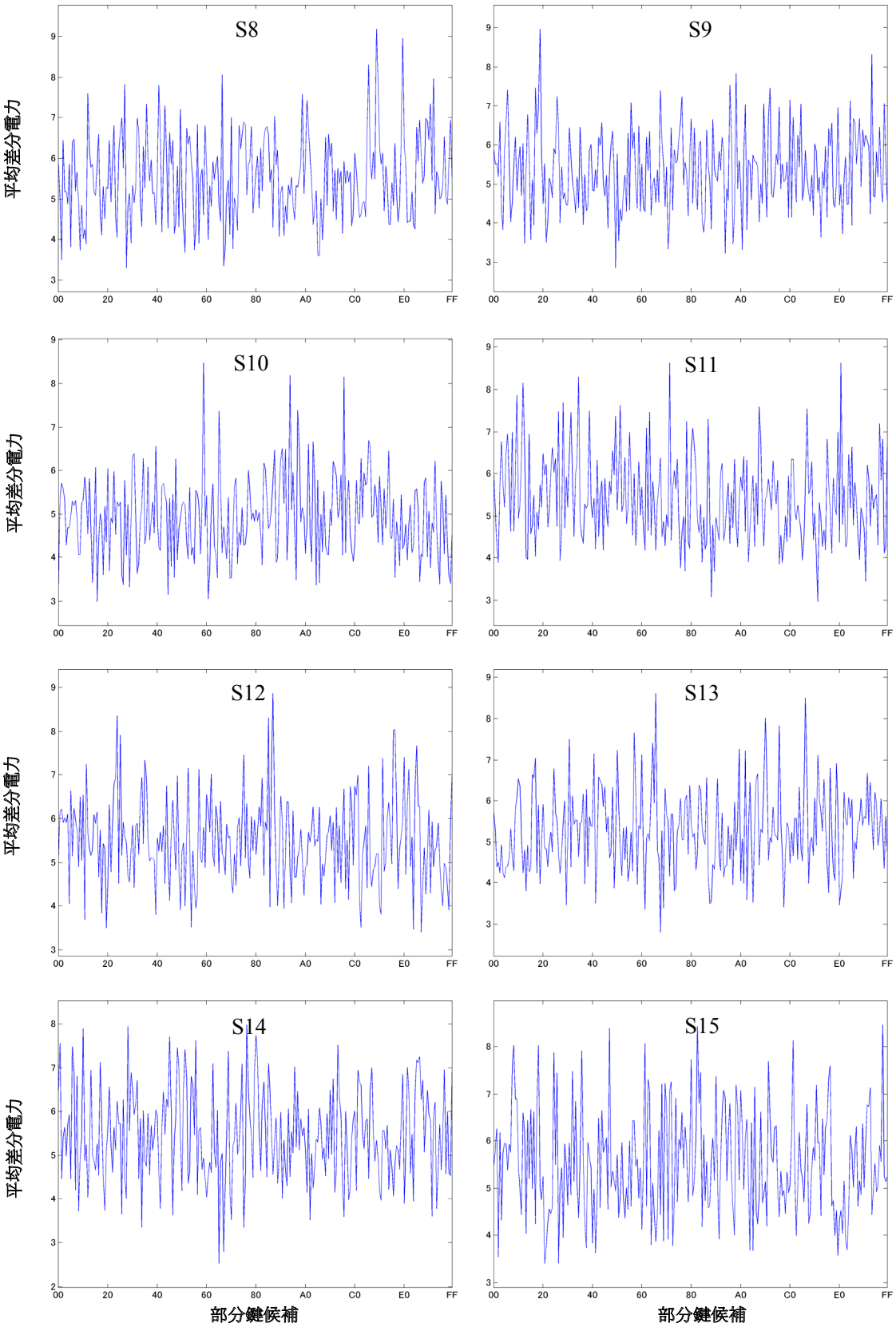

図 32-2　SASEBO-G 上の AES 回路(MDPL)に対する W2-DPA の平均差分電力

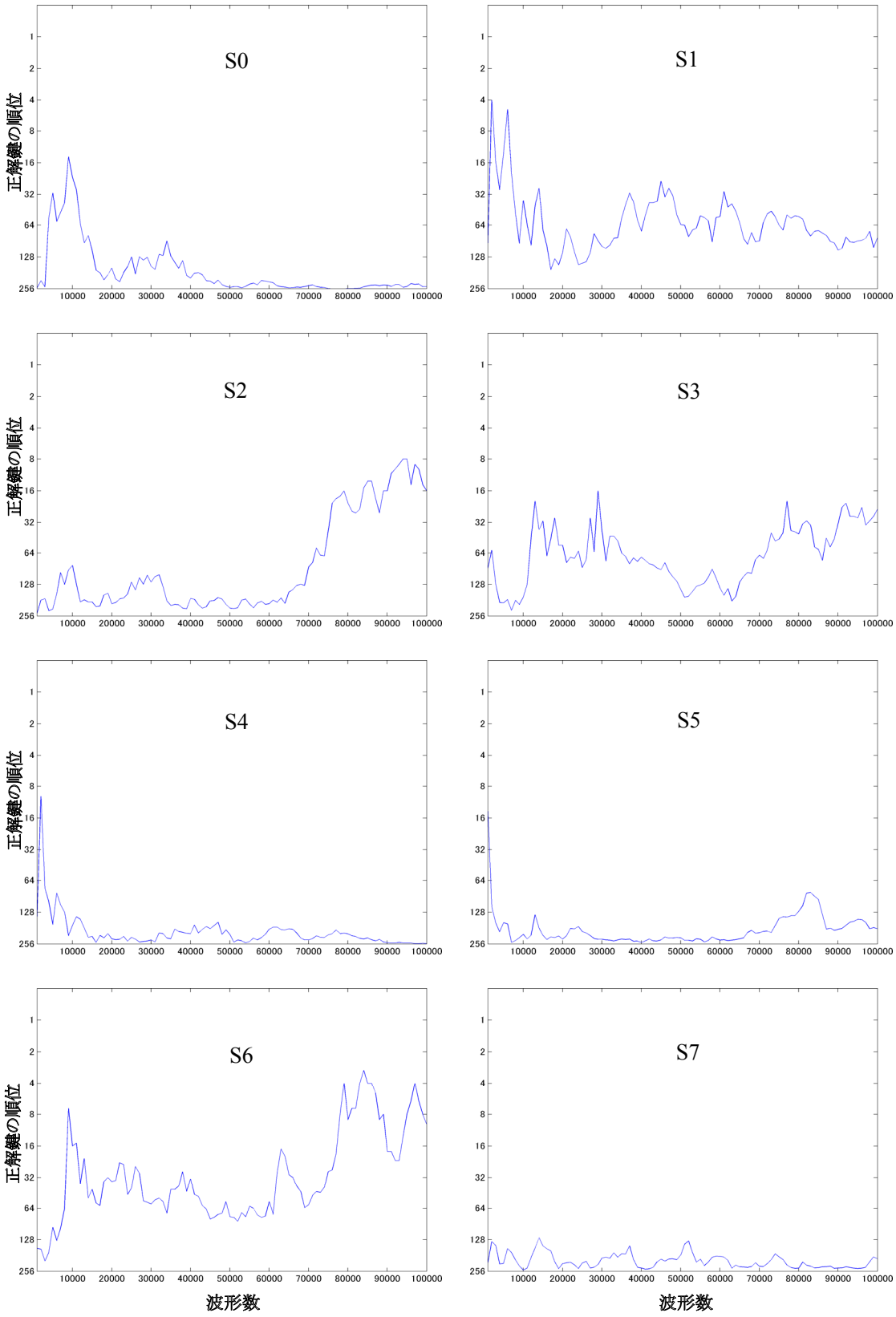

図 33-1　SASEBO-G 上の AES 回路(MDPL)に対する W2-DPA の精度と波形数の関係

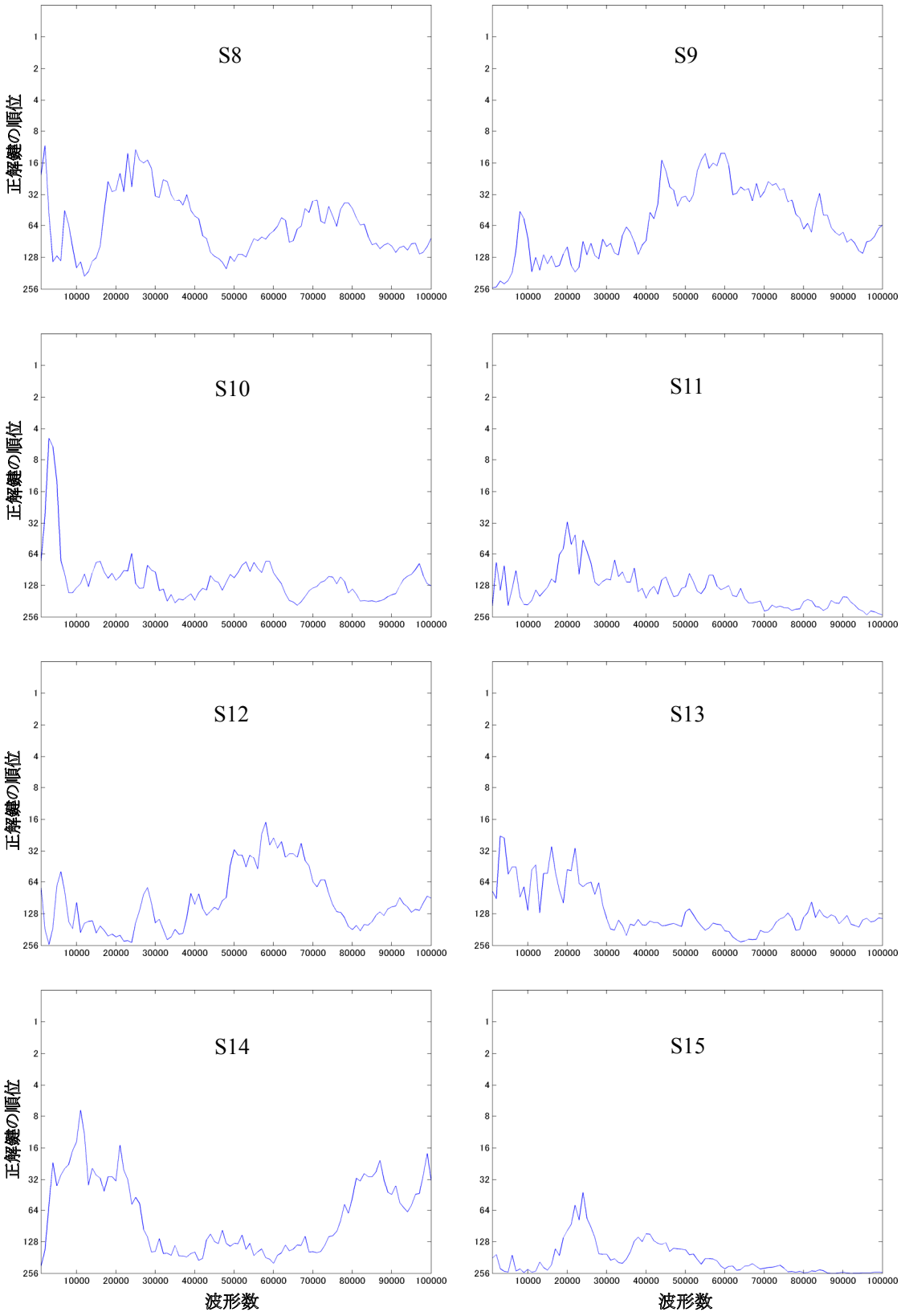

図 33-2　SASEBO-G 上の AES 回路(MDPL)に対する W2-DPA の精度と波形数の関係

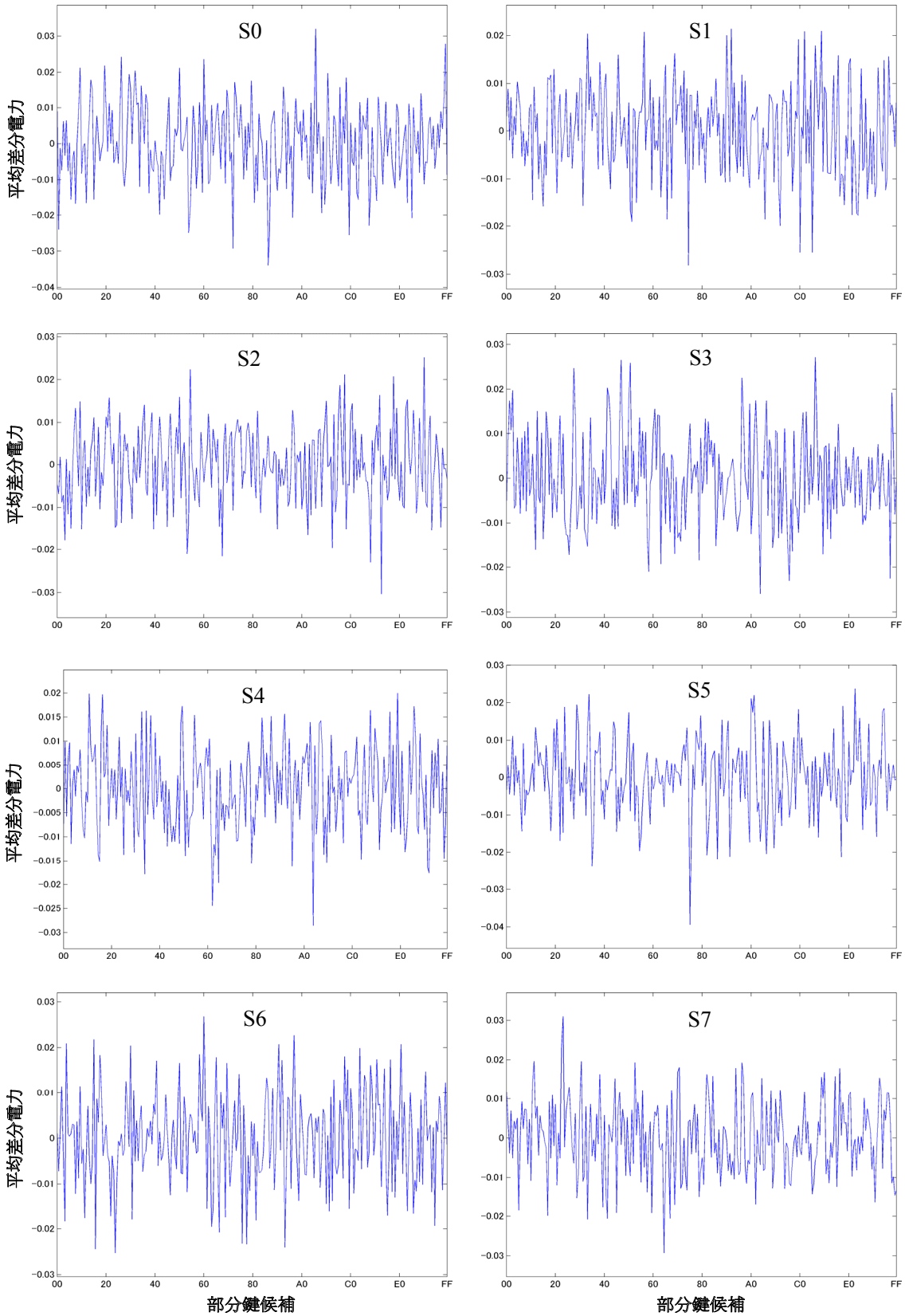

図 34-1　SASEBO-G 上の AES 回路(MDPL)に対する CPA の相関値

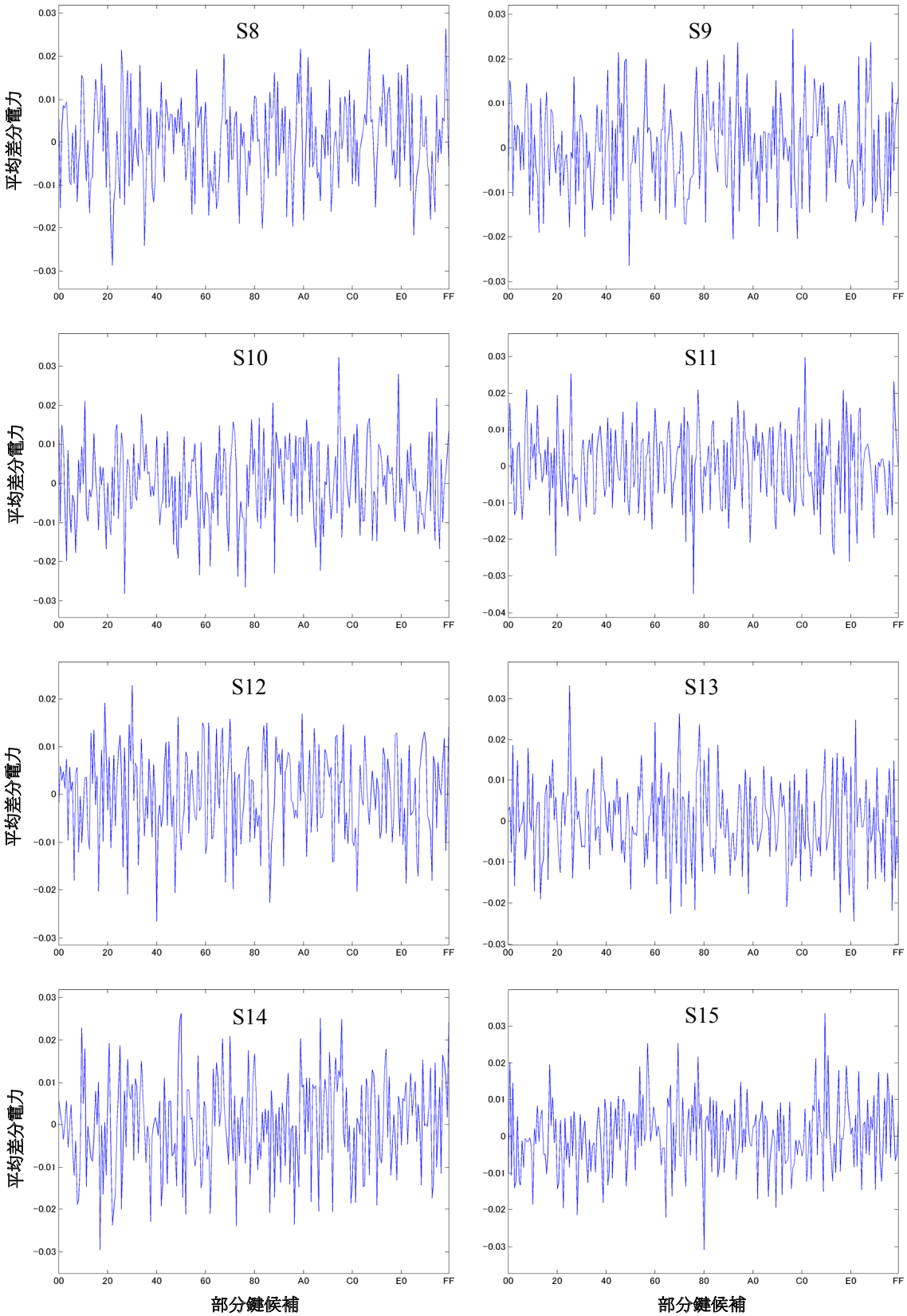

図 34-2　SASEBO-G 上の AES 回路(MDPL)に対する CPA の相関値

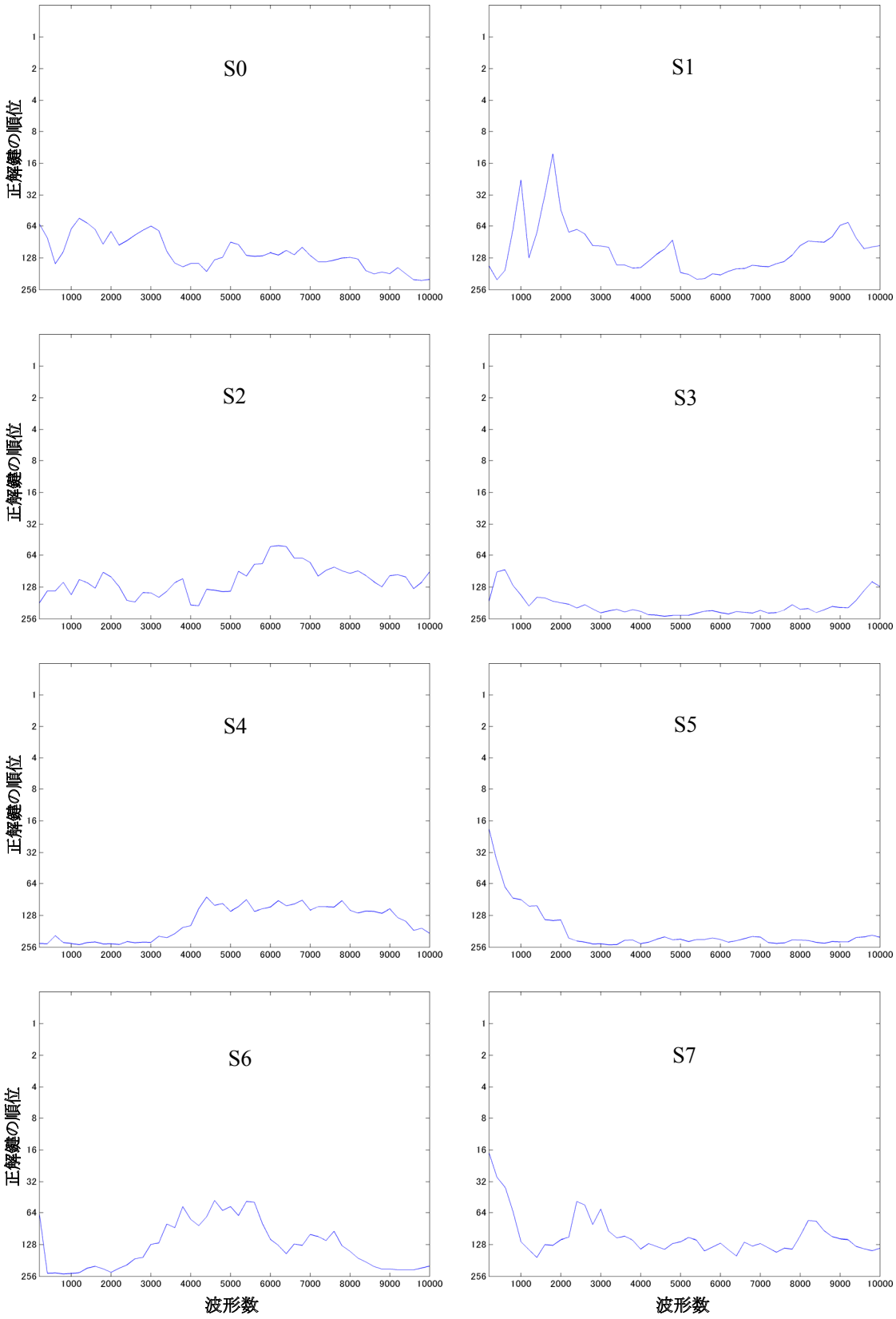

図 35-1　SASEBO-G 上の AES 回路(MDPL)に対する CPA の精度と波形数の関係

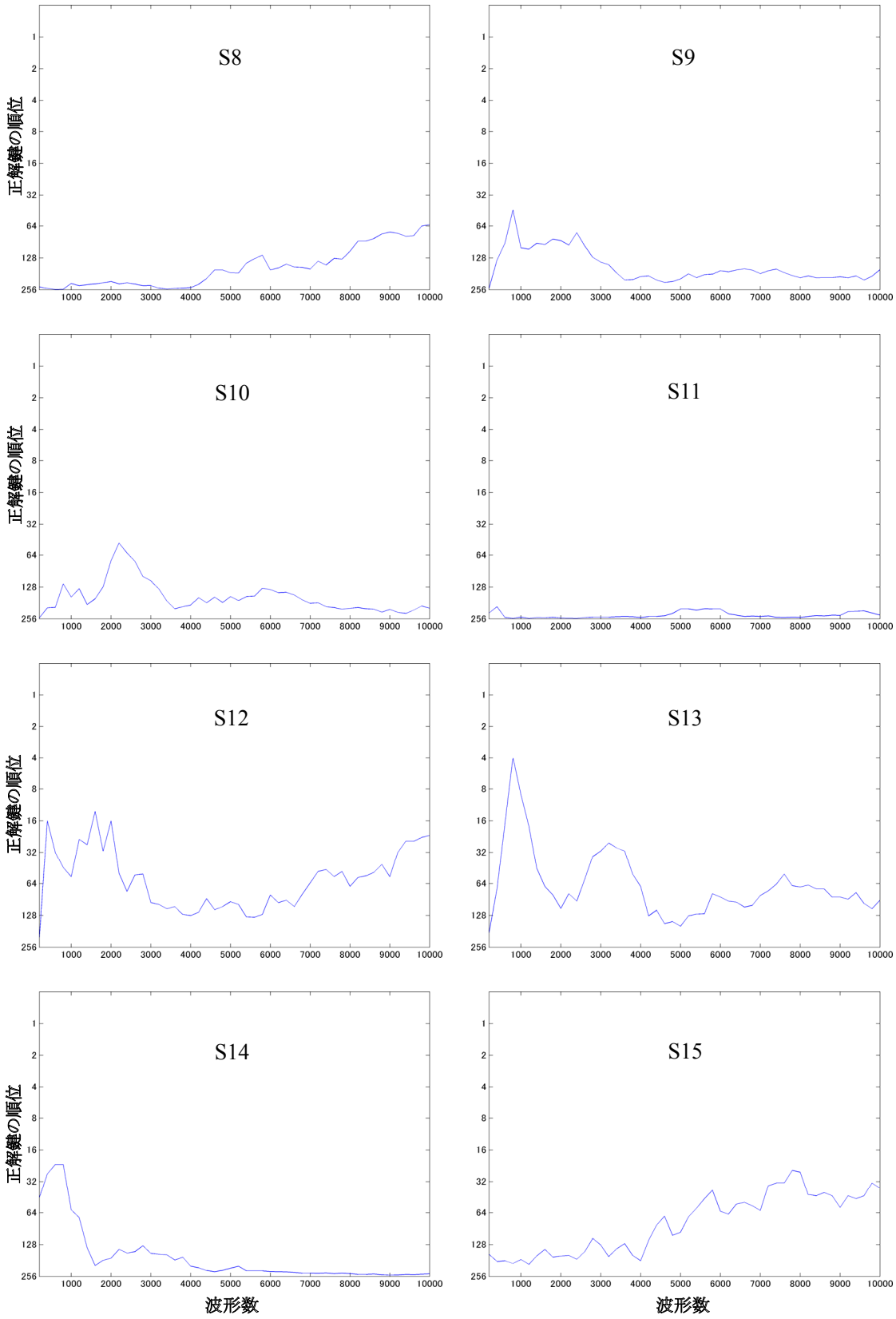

図 35-2　SASEBO-G 上の AES 回路(MDPL)に対する CPA の精度と波形数の関係

3 RSA 暗号への電力解析攻撃

3.1 概要

本節では公開鍵暗号法への攻撃として, RSA 暗号への単純電力解析(SPA: Simple Power Analisys)とその様々なバリエーションの解説を行う. また表3に示した測定環境において, 暗号LSIと FPGA に実装した RSA 回路に対する実験を通じてその効果を検証する.

RSA 暗号は, べき乗剰余演算により暗号化･復号処理を実行する公開鍵暗号である. P を元のデータ(平文), C を暗号文, E と N を公開鍵, D を秘密鍵とすると, 暗号化と復号はそれぞれ以下のような式で表される.

暗号化: $C = P^E \bmod N$
復号: $P = C^D \bmod N$

鍵である法 N や秘密鍵 D には, 安全性の観点から通常は1,024 ビット以上の多倍長整数が利用されることが多く, 平文 P や暗号文 C も法 N と同一の語長が用いられる. RSA 暗号のべき乗剰余演算は, 指数 E, あるいは D のビットパターンに応じて自乗算と乗算の乗剰余演算(以下, 簡単のためそれぞれ単に自乗算と乗算と呼ぶ)を繰り返すことによって実現される. その最も基本的なアルゴリズムがバイナリ法である. バイナリ法は演算を始める位置で左バイナリ法と右バイナリ法の2通りに分類される. 左バイナリ法は, 指数ビットの左側(最上位)から始め, 右バイナリ法は, 指数ビットの右側(最下位)から始める. どちらの手法でも, ビットが'0' ならば自乗算サイクル, '1' ならば自乗算と乗算のサイクルを実行し, それらを鍵のビット数だけ繰り返すことでべき乗剰余演算を実行する. 左バイナリ法では中間変数が 1 つで済むがのに対し, 右バイナリ法では中間変数が 2 つ必要となるため, 通常は実装効率の点で有利な左バイナリ法が用いられる. そこで, 以下では主に左バイナリ法を対象とした攻撃手法について述べる.

表 3 測定条件

項目	条件
デジタルオシロスコープ	Agilent MSO6104A
サンプリング周波数	800MSample/sec
プローブ	Coaxial cable (50 Ω)
安定化電源	3.3 V
動作クロック周波数	24 MHz
測定ポイント	測定対象の暗号 LSI または FPGA のコア電源とボードの GND 線の間に挿入した 1 Ωの抵抗で電圧を測定

3.2 単純電力解析攻撃

単純電力解析(以下 SPA と略記する)[1] は, 最も基本となる電力解析攻撃の一つであり, 暗号処理中の電力波形から直接秘密情報を推測する手法である. RSA 暗号は演算の語長が長いため, 一回の乗剰余演算に専用ハードウェアを用いても数百～数千サイクルを要する. そこで, 図 36 に示すように, RSA 暗号の自乗算と乗算の電力波形を見分けて秘密情報を導出するのが SPA のアイデアである. 消費電力差の要因としては, トランジスタのスイッチングの偏りや演算時間, 制御ロジックの違いなどが考えられる.

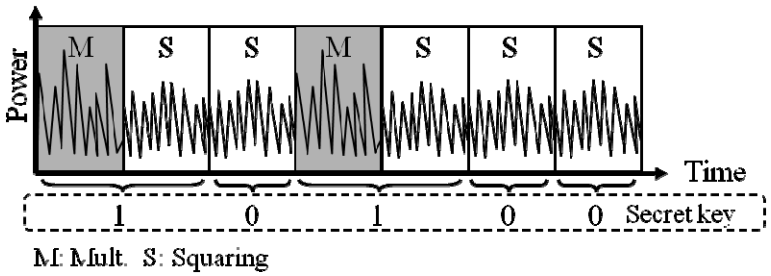

図 36 RSA 暗号への SPA

図 36 (a)は SASEBO-R の ASIC 実装した RSA 暗号ハードウェアの電力波形で, 図 37 (b)は同じ Verilog-HDL コードを SASEBO-G 上の FPGA に実装したときの電力波形である. 入力にはどちらもランダムな値を用いている. FPGA の波形は, ASIC の場合に対して振幅が 5 倍程度大きく, 波形の形状も大きく異なっている. このように, 同一の回路構造であっても実装する形態やデバイスによって得られる電力波形が大きく異なる. 図 37 では, (a)(b)いずれの波形からも自乗算と乗算を見分けることは困難であるが, 低域通過フィルタ(遮断周波数 80MHz)によりノイズ成分をカットすることで, 図 38 のように FPGA では両者を見分けることが可能となった.

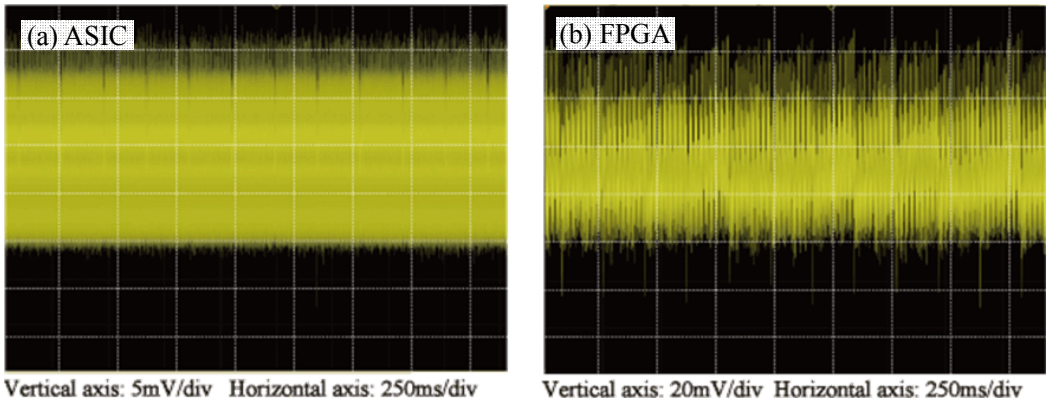

図 37 乱数入力時の電力波形(フィルタリングなし)

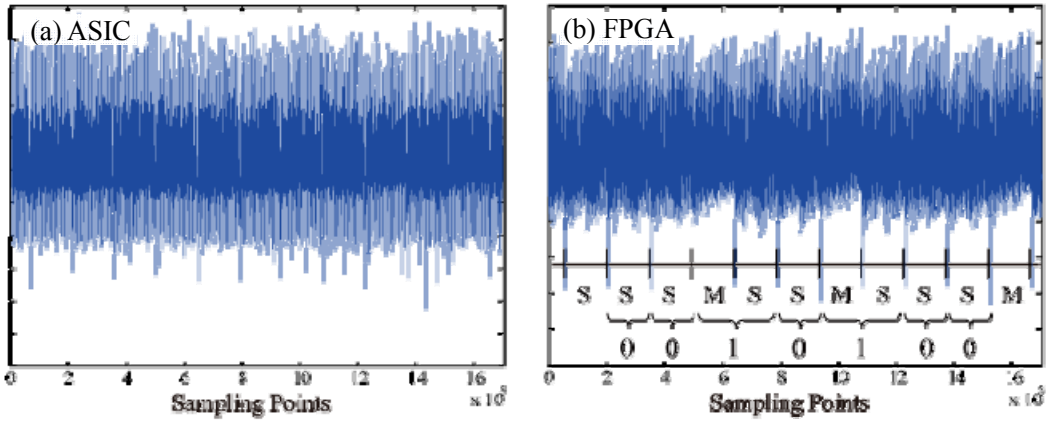

図 38 乱数入力時の電力波形(フィルタリングあり)

3.3 選択平文型単純電力解析攻撃

SPA では, べき乗剰余演算中に生じる自乗剰余算と乗剰余算の波形の違いを見分ける必要があるが, 上記に示した例のようにランダムな入力に対しては, 演算データが毎回異なるのでその差を観測できるとは限らない. 特に, 同一シーケンスによって自乗剰余算と乗剰余算を一つの演算器で実行する場合には, さらに両者の識別が困難である. そこで, 鍵ビットに依存した演算の差を強調するた法として, 平文選択を組み合わせた SPA が提案されている.

- ***N*–1 入力による SPA**

入力を N–1 とすると, 左バイナリ法の演算は, 鍵のビットパターンに応じて, (M)自乗算からの乗算, (S1)乗算からの自乗算, および (S2)自乗算からの自乗算の 3 種類に分類される [13].

$$\text{(M)} \quad 1\times(-1)\bmod N = -1\bmod N$$
$$\text{(S1)} \quad (-1)\times(-1)\bmod N = 1\bmod N$$
$$\text{(S2)} \quad 1\times 1\bmod N = 1\bmod N$$

これは, 左バイナリ法の計算手順において不変であり, 乗剰余演算の高速演算手法であるモンゴメリ乗算を用いた場合にも当てはまる. モンゴメリ乗算では, 演算の基底をモンゴメリドメイン ($\times 2^k \bmod N$) に変換されるため, 上記の式は以下のようになる.

$$\text{(M)} \quad 2^k\times(-2^k)\times 2^{-k}\bmod N = -2^k \bmod N$$
$$\text{(S1)} \quad (-2^k)\times(-2^k)\times 2^{-k}\bmod N = 2^k \bmod N$$
$$\text{(S2)} \quad 2^k\times 2^k\times 2^{-k}\bmod N = 2^k \bmod N$$

本攻撃は, M, S1, S2 の消費電力差から鍵のビットパターンを推定するため, 実装する乗剰余演算アルゴリズムや回路アーキテクチャに関する詳細な知識を必要としない. また, 波形は 3 種類しかないため, どれが M, S1, S2 に対応するかは容易に判別することができる. この同定は, 既知の公開鍵を用いても可能である.

図 39 に入力データ N–1 に対する SPA の概念図を示す. 左バイナリ法では, M と S1 は必ずペアで出現し, 連続して出現するのは S2 だけとなる. そのため, 3 種類全てを識別する必要はなく, どれか一つを差異化できれば高い確率で鍵を推定することが可能となる. このように, 出現順序を利用することも N–1 入力を用いた攻撃の重要な特徴の一つである.

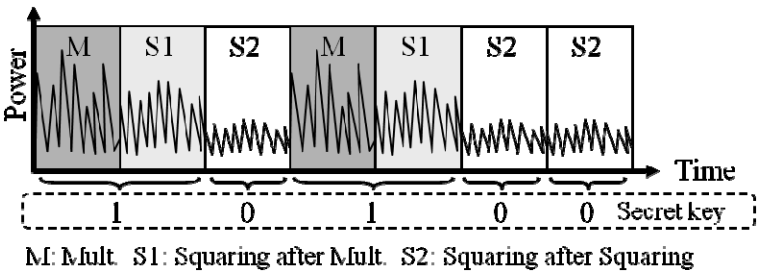

図 39 (N–1)-入力による平文選択 SPA

図 40 は ASIC 実装と FPGA 実装の RSA 暗号回路に N–1 を入力したときの電力波形で, いずれにおいても自乗算と乗算を識別することができる. さらに図 38 と同様, 低域通過フィルタでノイズ成分をカットすることで, 図 41 に示すようにより演算がより明確に区別できるようになる.

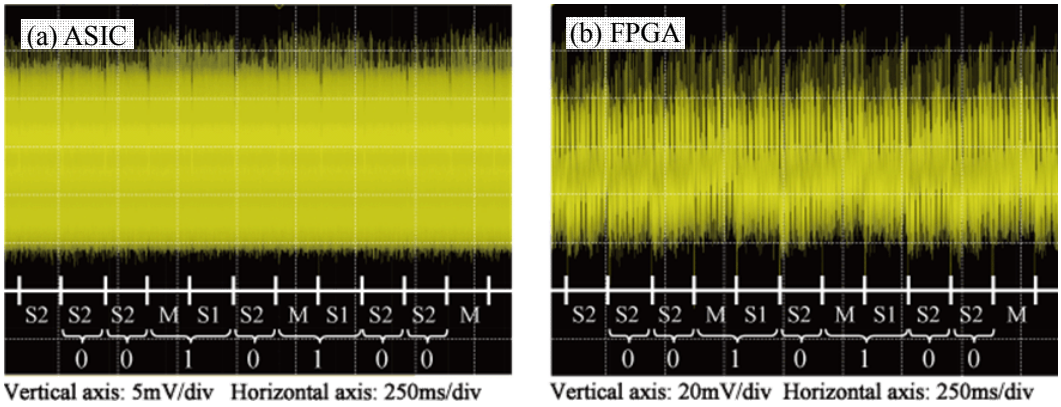

図 40 (*N*–1)-入力の電力波形(フィルタリングなし)

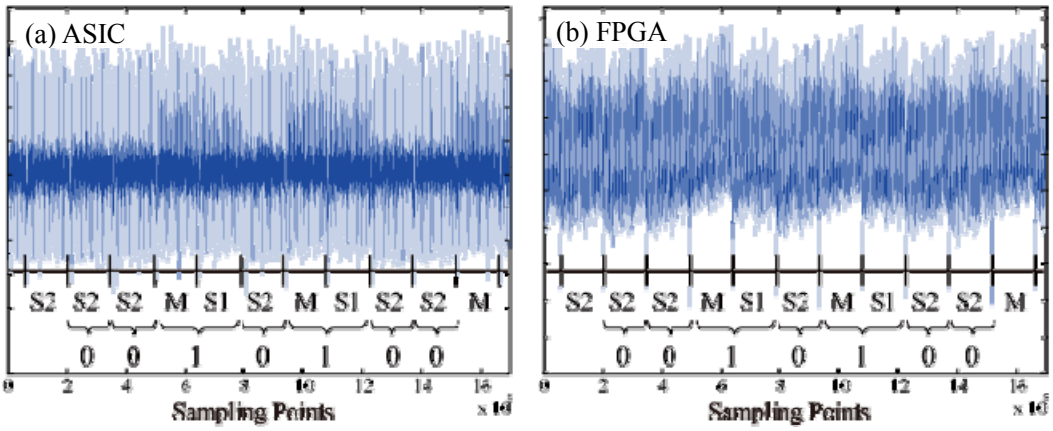

図 41 (*N*–1)-入力の電力波形(フィルタリングあり)

また, *N*–1 入力を用いた攻撃は, ダミー乗算を挿入する典型的な SPA 対策も無効化することができる. この対策は鍵のビットが'0'のときにもダミーの乗算を行うことで, 常に自乗算と乗算をペアで実行する. したがって図 36 の SPA では, 秘密鍵であるべき指数を推定することができない. しかし, *N*–1 を入力データとした場合は図 42 のように, ダミー乗算 DM の後は必ず自乗算 S2 となる. 通常の乗算 M の後は必ず自乗算 S1 が実行されるので, この M→S2 という順序の波形が観測されたならば, それはダミー乗算であると判別できる. 図 43 にダミー演算の対策を施した FPGA 実装に対する *N*–1 入力の電力波形を示す.

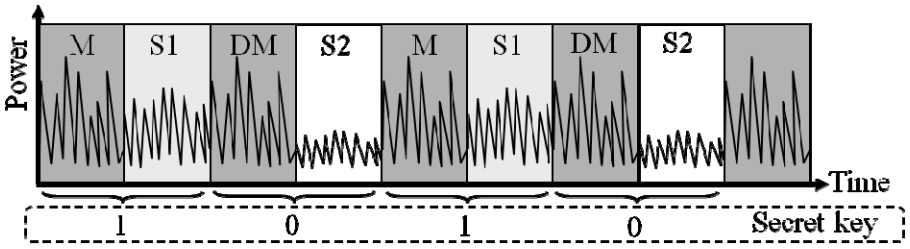

図 42 ダミー乗算の対策済み RSA 実装における(*N*–1)-入力による SPA

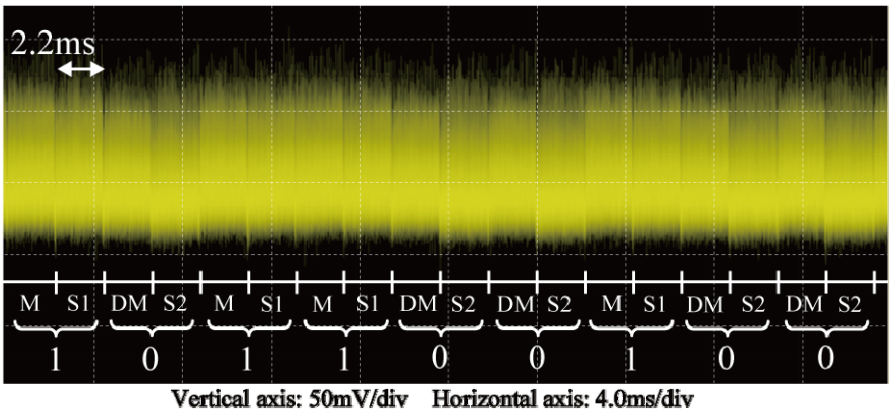

図 43　ダミー乗算の対策済み FPGA 実装における N–1 入力の電力波形(フィルタリングなし)

- **1-入力(2^{-k}-入力)による SPA**

左バイナリ法における乗算は，常に中間値と入力データとの間の演算となる．そのため，特殊なビット系列の入力を与えることで，その入力に依存した乗算の消費電力を相対的に低下させることができる．例えば，入力の系列が一桁目以外は全て“0”となるような 1 mod N 入力(Montgomery 乗算適用時には，2^{-k} mod N 入力)などである [14]．

図 44 は Montgomery 乗算適用時に，2^{-k} を入力したときの電力波形，図 45 はそれに低域通過フィルタを施したものである．ASIC と FPGA 共に N-1 入力よりも明確に，自乗算と乗算を識別することができている．

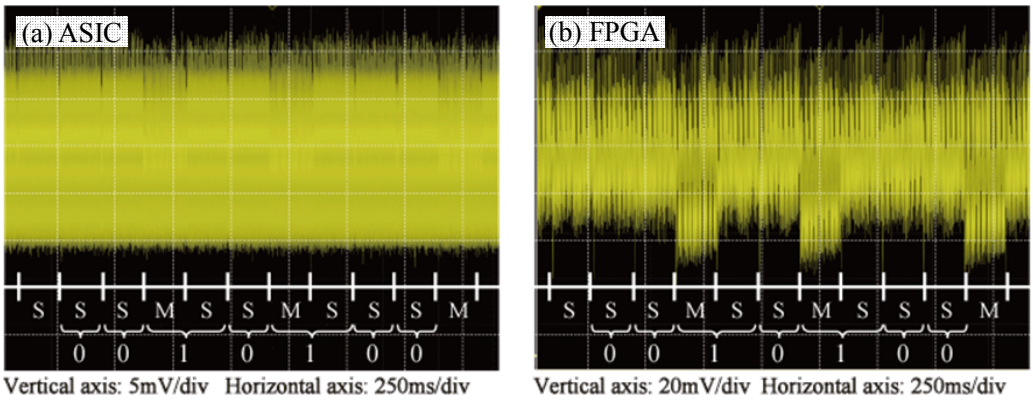

図 44　2^{-k}-入力の電力波形(フィルタリング前)

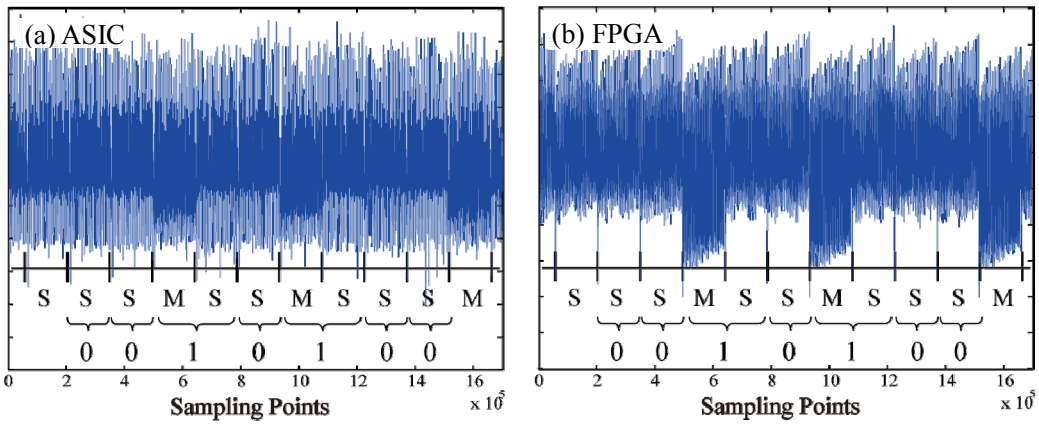

図 45　2^{-k}-入力の電力波形(フィルタリング後)

この結果は，ビット0とビット1の割合が偏った入力を与えても，自乗算と乗算の電力に差が現われることを示唆している．このため，2^{-k} 以外にも脅威となる入力パターンが考えられる．SASEBO-Gによる実験では，1,024 ビット入力の演算において，‘0’または‘1’が 800 ビット程度と偏った場合も乗算と自乗算の消費電力の差を観測することができた．したがって，N-1 や 2^{-k} といった特殊な入力を排除したとしても，$2^{224=1024-800}\times 2$ パターンの入力に対して，RSA 暗号実装が脆弱となる可能性がある．

3.4 選択平文ペアを用いた単純電力解析攻撃

強力な平文選択型の電力解析の 1 つに，特殊な入力ペアから得られた 2 つの電力波形の比較により鍵推定を行う手法がある．Fouque らが提案した Doubling attack(べき乗剰余演算では，Squaring attack) [15] は，入力ペア X, X^2 から得られる 2 つの消費電力波形を用いて鍵を推定する．図 46 は，左バイナリ法への Doubling attack の例である．図中の M と S は，それぞれ乗算と自乗算を表す．ここで，X と X^2 を入力とする消費電力波形 P_X と $P_X{}^2$ の間で，1 つずれた演算サイクルで生じる自乗算(○で囲んだ $P_X{}^2$ の S と P_X の S) の入出力が一致することになる．したがって，鍵のビット列によって決まる演算の種類を，この自乗算 S の類似性で判定する．

一方，Yen らは，この攻撃のバリエーションとして，X と $-X$ の入力ペアを用いて鍵を推定する攻撃を提案している [13]．この場合，図 47 のように同じ演算サイクルで生じる S の入出力が一致することを用いて鍵を推定する．

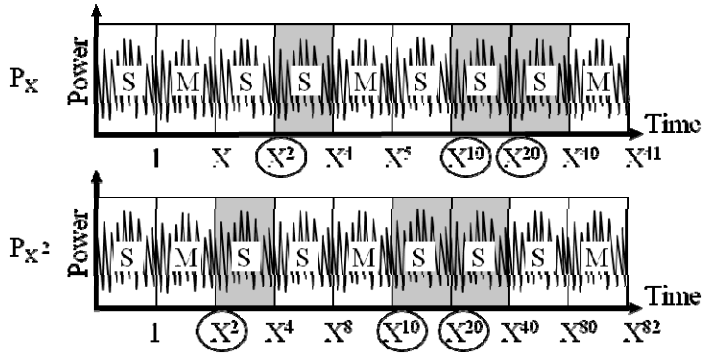

図 46 選択平文ペア(X, X^2)を用いた SPA (Doubling attack)

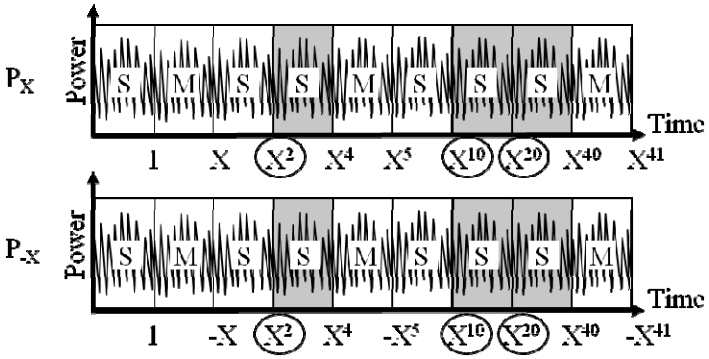

図 47 選択平文ペア(X, $-X$)を用いた SPA

図 48 に平文ペア X, $-X$ を入力して得られた 2 つの電力波形の差分波形を，またそれに低域通過フィルタを適用した波形を図 49 示す．同じ演算の差分電力は他に比べて小さくなり，さらにフィルタでノイズ成分がカットすることで，乗算と自乗算を容易に判別可能となっている．

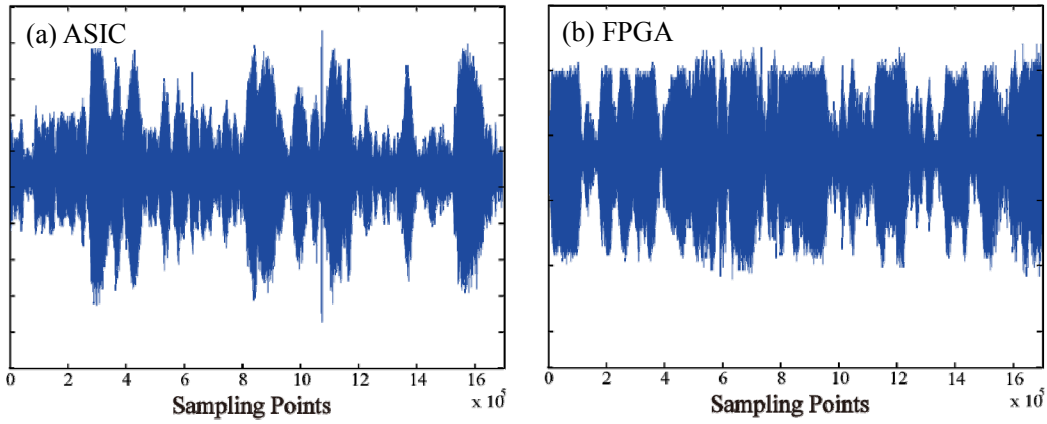

図 48　選択平文ペア(X, $-X$)の差分電力波形(フィルタリング前)

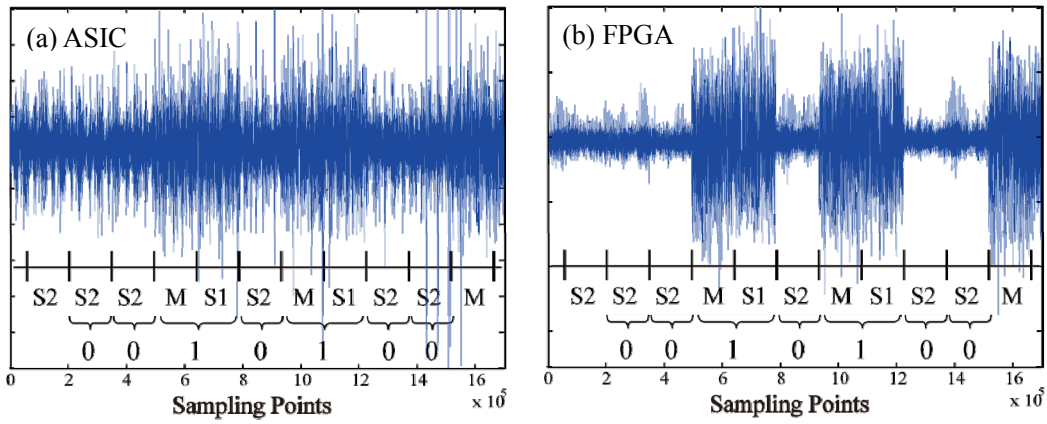

図 49　選択平文ペア(X, $-X$)の差分電力波形(フィルタリング後)

Fouque および Yen らの手法は，演算の出現順序を考慮することで，ダミー乗算を用いた上述の対策への適用も可能となる．しかし，その適用は左バイナリ法に限られる．これに対して，Homma らは，2 つの消費電力波形中の任意のサイクルで生じる自乗算を用いて鍵推定を行う手法を提案している [16]．この手法は X, X^2 や X, $-X$ だけでなく，入力データの自由度を高くできるためより柔軟な鍵推定が行え．左バイナリ法だけでなく右バイナリ法やそれ以外のアルゴリズム(window 法や Sliding Window 法)への適用も可能である．

図 50 にその左バイナリ法への適用例を示す．$Y^{\alpha}=Z^{\beta}(Y\neq Z)$ となる Y と Z を入力として，鍵 $E=\{e_{k-1}\ e_{k-2}...\ e_1e_0\}_2$ を最上位から順番に決定していく．部分鍵 $E^{(j)}=\{e_{k-1}e_{k-2}...e_{k-j}\}_2$ が既知のとき，Y^{α}を未知の鍵ビット $e_{k-(j+1)}$ による演算(対象演算)の入力値，Z^{β}を既知の自乗算(参照演算)の入力値となるように入力 Y と Z を与える．$e_{k-(j+1)}=0$ のとき，対象演算は自乗算となり Z^{β}を入力とする自乗算と一致する．一方で，$e_{k-(j+1)}=1$ のときは，対象演算は乗算となり Z^{β}を入力とする自乗算とは一致しない．この波形パターンの類似性を判定することで $e_{k-(j+1)}$が決定できる．$e_{k-(j+1)}$の値から α の値を更新し，同様の判定を繰り返すことで鍵系列を順次決定する．ここで，$Y^{\alpha}=Z^{\beta}$ となる入力の組み合わせは，$Y=r^{\beta} \bmod N$ と $Z=r^{\alpha} \bmod N$(r は任意の整数)から容易に求まる．べき指数 α および β は，部分鍵 $E_{(j)}$ が既知のとき，$\alpha=2E^{(j)}$, $\beta=E^{(t)}$ $(1\leq t\leq j)$ で与えられる．

図 50 に $Y^{\alpha}=Z^{\beta}$となる平文ペアを用いた SPA のイメージを示す．ここでは，部分鍵 $E^{(4)}=\{1100\}_2$ までが既知であり，次の e_{k-5} を推定する．このとき $\alpha=2E^{(4)}=24$, $\beta=E^{(2)}=3$ として，$Y^{24}=Z^3$ から Y^{24} を入力とする演算と，Z^3 を入力とする演算の比較を行う．図 51 および図 52 に SASEBO-G を用いた実験結果を示す．図 51 は推定対象となる波形(推定波形)と参照波形が同一の場合，図 52 は推定波形と参照が異なる場合である．差分波形の違いから，正しく鍵を推定できていることが分かる．

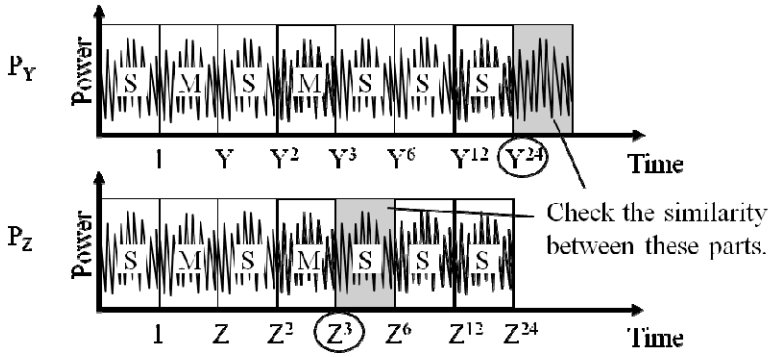

図 50　$Y^{\alpha}=Z^{\beta}$となる平文ペアを用いた SPA

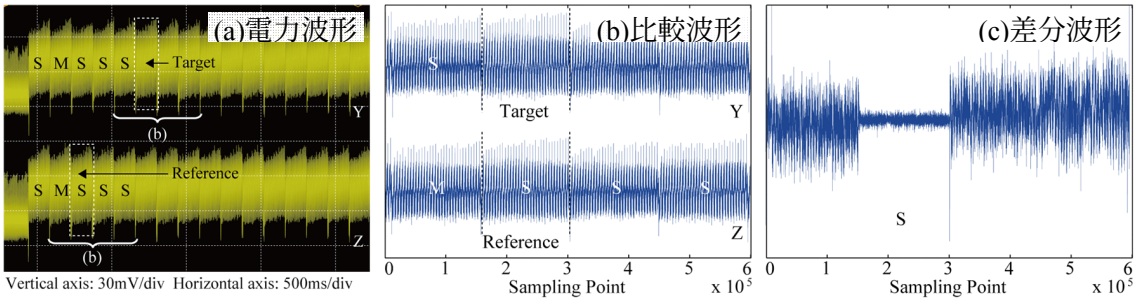

図 51　$Y^{24} = Z^{3}$ となる入力 Y, Z の電力波形(推定波形=参照波形)

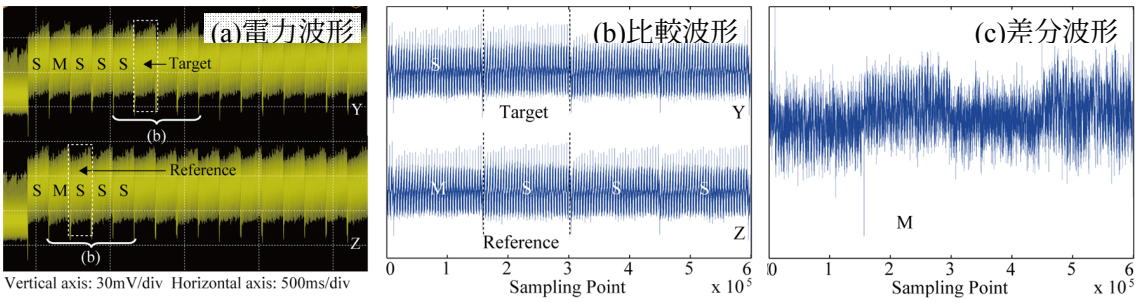

図 52　$Y^{24} = Z^{3}$ となる入力 Y, Z の電力波形(推定波形≠参照波形)

3.5 その他の実装に対する単純電力解析攻撃

上記の SPA では RSA のハードウェア実装に対する結果を示したが，ソフトウェア実装に対しても適用可能である．図 53 と図 54 は SASEBO-G の FPGA に内蔵される PowerPC プロセッサ上に RSA を C 言語実装し，$Y^{\alpha}=Z^{\beta}$となる平文ペアを用いた SPA を行ったときの電力波形であり，差分波形から正しく鍵を推定でることがわかる．上記の他の SPA もソフトウェア実装に対して同様に適用できることも確認されている．なお，本ソフトウェア実装は SPA が困難となるよう, 命令シーケンスやメモリアクセス等が乗算か自乗算かによらず一定になるようプログラムされており，通常のソフトウェア実装に比べて演算時間や消費電力の差が小さい．一般に，ソフトウェア実装では，条件分岐に伴う処理時間の違いから演算の差が露呈するほか，演算ごとに異なるシーケンス・メモリアクセスとなる場合も多く，ハードウェア実装に比べて電力波形の違いを観測することは容易である．

平文選択型 SPA は，乗算と自乗算の入出力データに注目しているため，回路アーキテクチャの内部構成に関する知識は不要である．本実験では RSA 回路に乗算器ベースのシンプルな実装を用いたが，加算器ベースのものや，Montgomery 乗算アルゴリズム，中国の剰余定理(CRT: Chinese Remeinder Theorem）を使った実装にも適用可能である．特に CRT 実装に関しては上記の SPA 以外にも, 専用の平文選択型 SPA がいくつか提案されている [17) 18) 19) 20)].

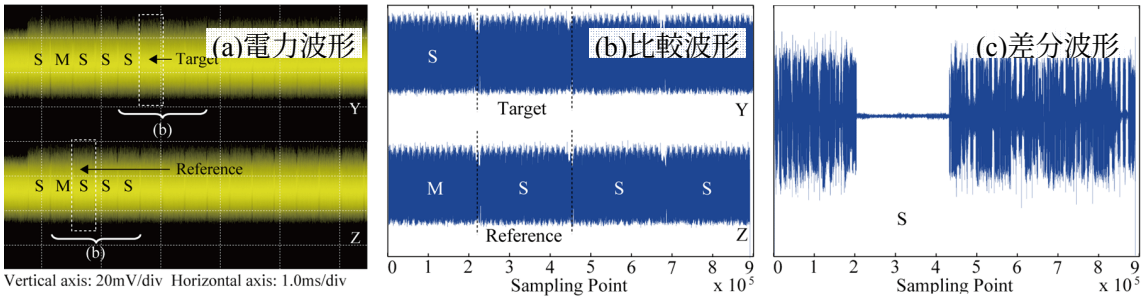

図 53　ソフトウェア実装の電力波形(推定波形=参照波形)

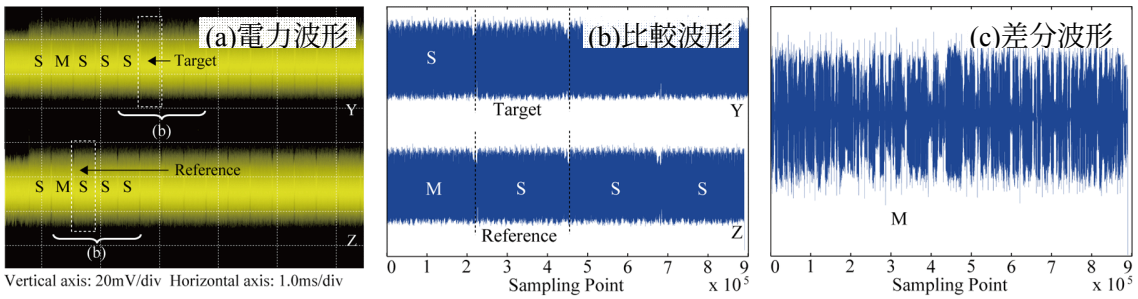

図 54　ソフトウェア実装の電力波形(推定波形≠参照波形)

3.6 単純電力解析攻撃への対策と耐性評価

SPA への対策は, 回路レベルとアルゴリズムレベルに大別される. 回路レベルの対策では, 特殊な論理を用いた回路実装により，消費電力と秘密鍵の依存性を解消する．WDDL (Wave Dynamic Differential Logic)や，SABL (Sense Amplifier Based Logic)，SDBL (Simple Dynamic Based Logic)などが知られている [21]．一方，アルゴリズムレベルの対策では，演算シーケンスやデータの操作や変更により依存性を解消する．演算シーケンスへの対策として，上述したダミー演算を挿入する Square-and-multiply always method [22] やそのアイデアを発展させた Montgomery Powering Ladder [23] などがある．また，データへの対策には，メッセージや鍵などのマスキング手法が提案されている [24].

乱数入力を用いた一般的な SPA に対しては, 演算シーケンスへの対策(Square-and-multiply always method や Montgomery Powering Ladder）が有効となる．しかしながら，N–1 や選択平文ペアを用いた SPA によって，それらを無効化することが可能である．これは，べき乗算中の自乗算の入力値が秘密情報(秘密鍵）の値を直接反映していることに起因している．これらの平文選択型 SPA を防ぐには，自乗算の位置や演算をシーケンスレベルで秘密情報と無関係なものとする工夫が必要である．一方で，データへの対策も平文選択型 SPA に対して有効となると考えられる．特に，平文データへのマスキングは平文選択を直接的に不可能にする効果がある．さらに，べき指数のマスキングを組み合わせることで，より有効な対策となる．ただし，これらの対策の有効性はマスク(乱数）の大きさや生成・更新方法に依存することに注意が必要である．一部の実装方法は，平文選択型 SPA により無効化されることが知られている [15].

SPA 耐性の評価には, 攻撃手法のや入力データの選択だけではなく, 観測された電力波形が各演算の特徴を十分に表していることが重要となる．逆に対策を特に施さなくとも，暗号モジュールの電力波形から十分な観測データ(各演算の情報量や特徴量）が得られなければ，耐性を有していることになる．そこで，その十分な観測データの指標として，電力波形の“質”を $S \times C \times 1/F$ で与えることとする．ここで S は測定機器(デジタルオシロスコープ）のサンプリング周波数(Samples/s)，C は一回の演算(乗算または自乗算）のクロックサイクル数(cycles)，F はモジュールの動作周波数(Hz）である．この値は一演算あたりのサン

プル数であり，値が大きいほど耐性評価に用いる情報や特徴が増えることになるが，その分測定時間や処理時間といった攻撃コストも増大する．これまでに示してきた実験における波形の質は，ハードウェア実装(ASIC および FPGA)で 1.5×10^5 ポイント，ソフトウェア実装(PowerPC)で 2.2×10^5 ポイントである．

文献

1) P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” Advances in Cryptology (*CRYPTO 1999*), LNCS 1666, pp. 388-397, Springer-Verlag, Aug. 1999.
2) D. Suzuki, M. Saeki, and T. Ichikawa “DPA Lekage Models for CMOS Logic Circuits,” Cryptographic Hardware and Embedded Systems (*CHES 2005*), LNCS 3659, pp. 366-382, Springer-Verlag, Sep. 2005.
3) S. Mangard, T. Popp, and B. M. Gammel “Side-Channel Leakage of Masked CMOS Gates,” Topics in Cryptology (*CT-RSA 2005*), LNCS 3376, pp. 361-365, Springer-Verlag, Feb. 2005
4) D. Suzuki and M. Saeki: Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style. Cryptographic Hardware and Embedded Systems (*CHES 2006*), LNCS 4249, pp. 255-269, Springer-Verlag, Oct. 2006.
5) S. Mangard, N. Pramstaller, and E. Oswald, “Successfully Attacking Masked AES Hardware Implementations, “Cryptographic Hardware and Embedded Systems (*CHES 2005*), LNCS 3376, pp. 1511, Springer-Verlag, Sep. 2005.
6) 鈴木大輔, 佐伯稔, 清水孝一, “ブロック暗号の回路アーキテクチャに対するサイドチャネル耐性評価 (1)(2),” 暗号と情報セキュリティシンポジウム (*SCIS 2009*), 2009 年 1 月.
7) T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Investigations of Power Analysis Attacks on Smartcards,” USENIX1999, Jun. 1999. http://www.usenix.org/
8) R. Bevan and E. Knudsen, “Ways to Enhance DPA,” International Converence on Information Security and Cryptology (*ICISC 2002*), LNCS 2587, pp.32342, Springer-Verlag, Dec. 2003.
9) E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model,” Cryptographic Hardware and Embedded Systems (*CHES 2004*), LNCS 3156, pp. 16-29, Springer-Verlag, Aug. 2004.
10) T. Le, J. Clediere, C. Canovas, B. Robisson, C. Serviere, and J. Lacoume, “A Proposition for Correlation Power Analysis Enhancement,” Cryptographic Hardware and Embedded Systems (*CHES2006*), LNCS 4249, pp. 14-186, Oct. 2006.
11) T. S. Messerges, “Using Second-Order Power Analysis to Attack DPA Resistant Software,” Cryptographic Hardware and Embedded Systems (*CHES 2000*), LNCS 1965, pp.238-251, Aug. 2000.
12) J. Waddle and D. Wagner, “Towards Efficient Second-Order Power Analysis,” Cryptographic Hardware and Embedded Systems (*CHES 2004*), LNCS 3156, pp. 1-15, Springer-Verlag, Aug. 2004.
13) S. M. Yen, W. C. Lien, S. J.Moon, and J. C. Ha, “Power analysis by exploiting chosen message and internal collisions - vulnerability of checking mechanism for RSA decryption,” Progress in Cryptology (*Mycrypt 2005*), LNCS 315, pp. 183-195, Springer-Verlag, Sep. 2005.
14) A. Miyamoto, N. Homma, T. Aoki, and A. Satoh, “Chosen-message SPA attacks against FPGA-based RSA hardware implementations,” Proc. International Conference on Field Programmable Logic and Applications (*FPL 2008*), pp. 35-40, Sep. 2008.
15) A. P. Fouque and F. Valette, “The doubling attack - why upwards is better than downwards,” Cryptographic Hardware and Embedded Systems (*CHES 2003*), LNCS 2779, Springer-Verlag, pp. 269-280, Set. 2003.
16) N. Homma, A. Miyamoto, T. Aoki, A. Satoh, and A. Shamir, “Collision-based power analysis

of modular exponentiation using chosen-message pairs," Cryptographic Hardware and Embedded Systems (*CHES 2008*), LNCS 5154, pp. 15-29, Aug. 2008.

17) W. Schindler, "A timing attack against RSA with the Chinese remainder theorem," Cryptographic Hardware and Embedded Systems (*CHES 2000*), LNCS 1965, pp. 109-124, Springer-Verlag, Aug. 2000.
18) C. D. Walter and S. Thompson, "Distinguishing exponent digits by observing modular subtractions," Topics in Cryptology (*CT-RSA 2001*), LNCS 2020, pp. 192-207, Springer-Verlag, Apr. 2001.
19) R. Novak, "SPA-based adaptive chosen-ciphertext attack on RSA implementation," Public Key Conference (*PKC 2002*), LNCS 224, pp. 252-262, Springer-Verlag, Feb. 2002.
20) B. D. Boer, K. Lemke, and G. Wicke, "A DPA attack against the modular reduction within a CRT implementation of RSA," Cryptographic Hardware and Embedded Systems (*CHES 2002*), LNCS 2523, pp. 228-243, Springer-Verlag, Aug. 2002.
21) T. Popp, S. Mangard and E. Oswald, "Power Analysis Attacks: Revealing the Secrets of Smart Cards," Springer-Verlag, 2007.
22) J. S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," Cryptographic Hardware and Embedded Systems (*CHES 1999*), LNCS 117, pp. 192–302, Springer-Verlag, 1999.
23) M. Joye and S. M. Yen, "The montgomery powering ladder," Cryptographic Hardware and Embedded Systems (*CHES 2002*), LNCS 2523, pp. 291-302, Springer-Verlag, Aug. 2002.
24) P. Kocher, "Timing attacks on implementations of diffiehellman, RSA, DSS, and other systems," Advances in Cryptology (*CRYPTO 1996*), LNCS 1109, Springer-Verlag, pp. 104-113, Aug. 1996.