社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

位相限定相関法に基づく高精度波形解析とそのサイドチャネル攻撃への応用

今井　裕一† 　本間　尚文† 　長嶋　聖† 　青木　孝文† 　佐藤　証††

† 東北大学大学院情報科学研究科　〒 980–8579 仙台市青葉区荒巻字青葉 6–6–05
†† 日本アイ・ビー・エム株式会社 東京基礎研究所　〒 242-8502 神奈川県大和市下鶴間 1623-14
E-mail: †{imai,homma}@aoki.ecei.tohoku.ac.jp, ††akashi@jp.ibm.com

あらまし　本稿では，位相限定相関法を用いた高精度な波形位置あわせ手法とそのサイドチャネル攻撃への応用について述べる．一般に SPA や DPA のような電力解析攻撃では，ノイズ成分の低減や秘密情報の抽出のため電力波形データへの統計的な処理を必要とする．しかし，一連の電力波形データには，しばしば測定時の取り込み誤差による位置ずれが含まれる．提案する手法は，離散フーリエ変換した波形より得られる位相成分から，サンプリング分解能を越える精度で信号波形間の位置ずれ量を推定する．波形間の位置ずれを高精度に補正することで電力解析攻撃の効果を高めることができる．本稿では，Z80 プロセッサ上の DES のソフトウェア実装に対する DPA によりその可能性を示す．
キーワード　サイドチャネル攻撃，差分電力解析，波形位置合わせ，位相限定相関

A High-Resolution Waveform Analysis Based on Phase-Only Correlation and Its Application to Side-Channel Attacks

Yuichi IMAI†, Naofumi HOMMA†, Sei NAGASHIMA†, Takafumi AOKI†, and Akashi SATOH††

† Graduate School of Information Sciences, Tohoku University
Aoba 6–6–05, Aramaki, Aoba-ku, Sendai-shi, Miyagi, 980–8579, Japan
†† IBM Research, Tokyo Research Laboratory, IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi, Kanagawa, 242-8502, Japan
E-mail: †{imai,homma}@aoki.ecei.tohoku.ac.jp, ††akashi@jp.ibm.com

Abstract　This paper presents a high-resolution waveform alignment method using a Phase-Only Correlation (POC) technique and its application to side-channel attacks against cryptosystems. In general, power analysis attacks, such as SPA and DPA, require a statistical analysis of power waveforms to reduce noise and to retrieve secret information. However, the waveform data often include displacement errors in the measurement. The use of phase components in discrete Fourier transforms of waveforms makes it possible to estimate the displacements between signal waveforms with higher resolution than the sampling resolution. The effectiveness of power analysis attacks can be enhanced using the super-resolution alignment method. In this paper, we demonstrate the potential of the enhanced attacks through a set of experimental DPAs against DES software implementation on a Z80 processor.
Key words　Side channel attacks, Differential Power analysis, Waveform alignment, Phase-only correlation

1. はじめに

近年，暗号処理システムのサイドチャネル情報（消費電力，電磁波放射，処理時間など）から秘密情報を奪うサイドチャネル攻撃の危険性が指摘されている．身の回りのあらゆる情報機器がネットワークを介して接続されるユビキタス情報社会においては，実装や運用の脆弱性を狙った犯罪が重大な社会的脅威となる可能性が高く，サイドチャネル攻撃に対して頑健な暗号処理システムの開発が要求される．一方で，その開発のためには，想定される攻撃の潜在的な能力および限界を正しく評価する必要があり，安全性評価技術としての攻撃技術の確立が不可欠である．

もっとも基本的なサイドチャネル攻撃として，システムの消費電力を利用した電力解析攻撃が知られている [1]．電力解析攻

撃は，暗号処理中の消費電力波形が秘密情報に依存する変化量を含むことに着目した攻撃法である．その攻撃能力の高さに加え，オシロスコープやパソコンといった比較的安価な設備でおこなえることや攻撃の痕跡が残らないことから，スマートカードや組み込み機器に搭載されたシステムへの現実的な脅威となり得る．電力の代わりに電磁波を用いても同様の解析で攻撃が可能であることが示されている [2]．暗号処理システムの安全性を評価する上で，電力解析攻撃への耐性は重要な指標の一つとなる．

本稿では，電力解析攻撃の高精度な波形解析手法を提案し，その有効性を検証する．電力解析攻撃では，一般にノイズ成分の低減や秘密情報の抽出のため電力波形データへの統計的な処理を必要とする．このとき，入力データの異なる複数の電力波形を，同じ処理が行われる正確なタイミングで取得しなければならない．しかし，実際の測定で完全に同一のタイミングを実現することは難しい．まず，暗号処理に同期した都合のよいトリガ信号が得られるとは限らない．PLL を実装した LSI では内部クロックが外部クロック等の制御信号と必ずしも同期している保証はない．また，トリガを得られたとしても，そのジッタ等により取り込み誤差が生じる．結果として，取得された電力波形データには常に位置ずれが含まれていることになる．その位置ずれは，測定機器のサンプリング間隔以下と微小な場合でもしばしば解析結果に大きな影響を与える．電力波形間の位置ずれを高精度に補正することができれば，波形取得のタイミング精度に影響されない強力な電力解析攻撃を実現できると考えられる．

上記の観点から，位相限定相関法に基づく高精度波形位置合わせ手法を提案する．位相限定相関法は，離散フーリエ変換した波形より得られる位相成分に着目した相関法である [3]〜[5]．これまで画像マッチングに適用され，画像の平行移動量を 0.01 ピクセル，回転量を 0.03 度，拡大縮小率を 0.02 %と極めて高い精度で推定できることが示されている [3]．位相限定相関法の中心となる位相限定相関関数は，類似した信号波形間でデルタ関数に近いピーク特性を示すため，ノイズに対して頑健な位置ずれ量推定を可能とする．さらに，相関ピークモデルのフィッティング等により，サンプリング分解能を越える精度で位置ずれ量を推定できる．本稿では，INSTAC-8 準拠プラットフォーム [6] の Z80 プロセッサ上にソフトウェアで実装された DES への差分電力解析（Differential Power Analysis: DPA）により，提案する波形位置合わせ手法の有効性を示す．

2. 位相限定相関法に基づく高精度波形位置合わせ

本章では，位相限定相関法を用いた高精度な波形位置合わせ手法について述べる．まず，位相限定相関（Phase-Only Correlation: POC）関数を用いた信号波形間の移動量（位置ずれ量）推定およびその高精度化手法を示す．その上で，波形位置合わせとその適用例を示す．

2.1 位相限定相関関数による移動量推定

N 点の 2 つの信号波形を $f(n)$ および $g(n)$ とする．ただし，定式化の便宜上，離散時間のインデックスを $n = -M, \cdots, M$ とし，信号波形の長さを $N = 2M + 1$ とする．これらの信号波形の離散フーリエ変換 (Discrete Fourier Transform: DFT) をそれぞれ $F(k)$ および $G(k)$ として次式で与える．

$$F(k) = \sum_{n=-M}^{M} f(n) W_N^{kn} = A_F(k) e^{j\theta_F(k)} \tag{1}$$

$$G(k) = \sum_{n=-M}^{M} g(n) W_N^{kn} = A_G(k) e^{j\theta_G(k)} \tag{2}$$

ただし，$W_N = e^{-j\frac{2\pi}{N}}$ である．ここで，$A_F(k)$ および $A_G(k)$ は，それぞれ信号波形 $f(n)$ および $g(n)$ の振幅成分，$e^{j\theta_F(k)}$ および $e^{j\theta_G(k)}$ はそれぞれの信号波形の位相成分である．一般性を失うことなく離散周波数のインデックスを $k = -M, \cdots, M$ とすることができる．このとき，合成位相スペクトル $R_{FG}(k)$ は，

$$R_{FG}(k) = \frac{F(k)\overline{G(k)}}{\left|F(k)\overline{G(k)}\right|} = e^{j\theta_{FG}(k)} \tag{3}$$

ここで，$\overline{G(k)}$ は $G(k)$ の複素共役であり，$\theta_{FG}(k) = \theta_F(k) - \theta_G(k)$ である．$f(n)$ と $g(n)$ の POC 関数 $r_{fg}(n)$ は $R_{FG}(k)$ の逆離散フーリエ変換 (Inverse Discrete Fourier Transform: IDFT) として，次のように表される．

$$r_{fg}(n) = \frac{1}{N} \sum_{k=-M}^{M} R_{FG}(k) W_N^{-kn} \tag{4}$$

次に連続時間で定義された信号波形 $f_c(t)$ を考える．ここで，t は実数であり，δ を t に関する微小移動量を表す実数とすると，連続時間で t を δ だけ微小移動した波形は $f_c(t-\delta)$ と表現できる．これらの連続時間信号 $f_c(t)$ および $f_c(t-\delta)$ を標本化間隔 T で標本化した離散時間信号をそれぞれ $f(n)$ および $g(n)$ とし，次式で定義する．

$$f(n) \;=\; f_c(t)|_{t=nT} \tag{5}$$

$$g(n) \;=\; f_c(t-\delta)|_{t=nT} \tag{6}$$

ただし，$n = -M, \cdots, M$ とする．以下では単純化するため，$T = 1$ とする．このとき，離散時間信号 $f(n)$ および $g(n)$ に関する POC 関数を用いて， 連続時間での微小移動量 δ を推定する問題を考える．ただし，δ は，離散時間においてサンプリング間隔以下の移動量に対応するものと考える．ここで，$f(n)$ および $g(n)$ の DFT$F(k)$ および $G(k)$ の間には次の近似が成り立つ．

$$G(k) \simeq F(k) \cdot e^{-j\frac{2\pi}{N}k\delta} \tag{7}$$

上式が近似であるのは，連続時間信号と離散時間信号に対するフーリエ変換の性質の違いに起因する（連続時間のフーリエ変換においては等式が正確に成立することに注意されたい）．このとき，$f(n)$ および $g(n)$ の合成位相スペクトル $R_{FG}(k)$ および POC 関数 $r_{fg}(n)$ は，次のように表せる．

$$R_{FG}(k) \;=\; \frac{F(k)\overline{G(k)}}{\left|F(k)\overline{G(k)}\right|} \simeq e^{j\frac{2\pi}{N}k\delta} \tag{8}$$

$$r_{fg}(n) = \frac{1}{N}\sum_{k=-M}^{M} R_{FG}(k)W_N^{-kn}$$
$$\simeq \frac{\alpha}{N}\frac{\sin\{\pi(n+\delta)\}}{\sin\left\{\frac{\pi}{N}(n+\delta)\right\}} \quad (9)$$

ここで，$\alpha \leqq 1$ である．上式は，波形間に微小移動量 δ がある場合の POC 関数の一般形を表している．相関ピークの座標は波形間の位置ずれを表し，相関ピークの高さ α は波形間の類似度の指標となる．波形の変化によって α の値は変化する．このように微小移動した 2 つの波形の POC 関数は 1 サンプルの幅の急峻なピークをもつ．以上から，POC 関数の相関ピークを検出することにより，波形間の移動量および類似度を評価することができる．

2.2 移動量推定の高精度化手法

本節では，移動量推定のための高精度化手法について述べる．

(i) 関数フィッティングによる相関ピーク推定

図 1 に POC 関数を計算して得られる相関ピーク近傍のデータの例を示す．2 つの波形 $f(n)$ および $g(n)$ の POC 関数を計算することによって得られる $r_{fg}(n)$ は $n = -M, \cdots, M$ の離散点のみのデータ（黒丸）である．このとき，式 (9) で与えられる相関ピークモデルを実データにフィッティングすることで，波形のサンプル間に存在する真のピーク座標を推定することができる．図 1 の例では，フィッティングにより $\delta = 0.5$ 付近が真のピーク座標（位置ずれ量）として検出される．ここで，関数フィッティングには式 (9) 以外のモデル（2 次関数やガウス関数など）を利用することも可能である．

(ii) 窓関数による波形端の影響の低減

POC 関数の計算に使われる DFT は，取り扱う波形が波形端で循環することを仮定している．そのため，波形端に本来は存在しないはずの不連続性が現れる．この不連続性の影響を低減するために，入力波形 $f(n)$ および $g(n)$ に窓関数を乗じる．本稿では，次式で定義されるハニング窓を乗じる．

$$w(n) = \frac{1+\cos(\frac{\pi n}{M})}{2} \quad (10)$$

窓関数の適用は，信号波形の長さ N が小さい場合に特に有効である．

(iii) スペクトル重み付け関数の適用

実測される波形は，低周波領域に比べて高周波領域の S/N 比が低いことが予測される．そこで，周波数領域の合成位相スペクトル $R_{FG}(k)$ に対して低周波領域を強調するスペクトル重み付け関数 $H(k)$ を適用することで，信頼性の低い高周波領域を除去することができる．本稿では，次式で与えられる低域通過型のスペクトル重み付け関数 $H(k)$ を適用する．

$$H(k) = \begin{cases} 1 & |k| \leqq U \text{ のとき} \\ 0 & \text{その他のとき} \end{cases} \quad (11)$$

ここで，U は $0 < U \leqq M$ を満たす整数である．このとき，式 (9) は次のように表せる．

$$r_{fg}(n) = \frac{1}{N}\sum_{k=-M}^{M} R_{FG}(k)H(k)W_N^{-kn}$$

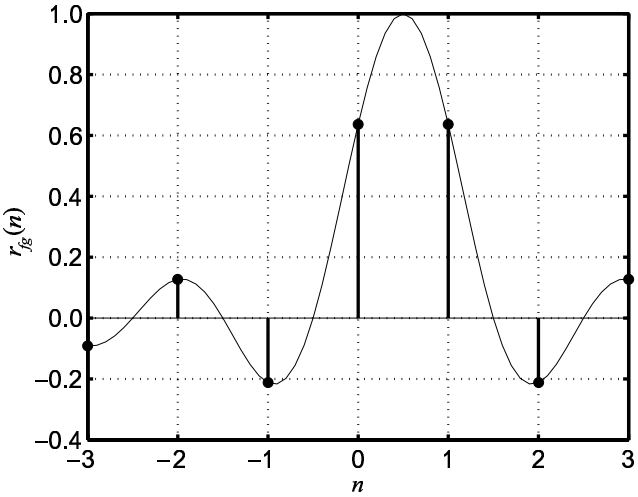

図 1　位相限定相関関数

$$\simeq \frac{\alpha}{N}\frac{\sin\left\{\frac{V}{N}\pi(n+\delta)\right\}}{\sin\left\{\frac{\pi}{N}(n+\delta)\right\}} \quad (12)$$

ただし，$V = 2U+1$ である．ここで，$H(k)$ のカットオフ周波数 U が小さくなるにつれて POC 関数のメインローブの幅は増加する．スペクトル重み付け関数を適用した場合は，フィッティングに式 (9) ではなく式 (12) を用いる．

入力波形の有効な帯域に合わせて，式 (11) 以外に，任意の重み付け関数を利用できる．この場合，相関ピークモデルは重み付け関数の IDFT によって導出可能である．

(iv) 帯域制限位相限定相関関数

信頼性の低い高周波領域を除去する高精度化手法には，上記のスペクトル重み付け関数の他に，帯域制限 POC (Band-Limited POC: BLPOC) 関数 [5] の利用が考えられる．

波形の持っている有効な周波数成分 $k = -K, \cdots, K$ のみを使用する BLPOC 関数は次式で与えられる．

$$r_{fg}^{K}(n) = \frac{1}{L}\sum_{k=-K}^{K} R_{FG}(k)W_L^{-kn}$$
$$\simeq \frac{\alpha}{L}\frac{\sin\{\pi(n+\delta')\}}{\sin\left\{\frac{\pi}{L}(n+\delta')\right\}} \quad (13)$$

ここで，$L = 2K+1$，$n = -K, \cdots, K$，$\delta' = \frac{L}{N}\delta$ である．BLPOC 関数の相関ピーク座標 δ' から位置ずれ量 δ を $\delta = \delta'\frac{N}{L}$ として求めることができる．

BLPOC 関数は，制限する周波数帯域の大きさ L に依存せずに相関ピークモデルの形状が通常の POC 関数と等しくなる．また，通常の POC 関数と比べて BLPOC 関数は信号の長さが短いため，合成位相スペクトル $R(k)$ の IDFT に必要とする計算量を短縮できる．BLPOC 関数と (iii) で述べたスペクトル重み付け関数を組み合わせることも可能である．

2.3 波形位置合わせとその適用例

2.1 節および 2.2 節で述べた方法により検出された位置ずれ量を用いて波形の位置合わせを行う．波形位置合わせとは，2 つの信号波形 $f(n)$ および $g(n)$ の位置ずれ量を δ とすると，$g(n)$ を δ 分だけずらした $g'(n)$ を求めることである．ここでは，周

波数領域で $g(n)$ の位相を回転させることにより $g'(n)$ を導出する方法を示す．

位置ずれ量 δ のとき，$g'(n)$ の DFT $G'(k)$ は次のように近似できる．

$$G'(k) \simeq G(k) \cdot e^{j\frac{2\pi}{N}k\delta} \tag{14}$$

このとき，$g'(n)$ は $G'(k)$ の IDFT として次式で与えられる．

$$g'(n) = \frac{1}{N}\sum_{k=-M}^{M} G'(k)W_N^{-kn} \tag{15}$$

波形位置合わせの方法には，上記以外にも，双三次補間法などの各種補間方法を利用できる．また，測定機器の内部で検出した位置ずれ量 δ を補正することも可能だと考えられる．

提案する手法による波形位置合わせの例を図 2 に示す．図 2(a) は，マイクロプロセッサ（8MHz 動作）の消費電力を 1GSa/s で取得した 2 つの波形である．ここで，取得した波形間には位置ずれが確認できる．位相限定相関法およびその高精度化手法 (i)∼(iii) を適用した結果，2 つの波形の位置ずれ量は $\delta = 1.5555$ であった．図 2(b) に位置合わせ後の波形を示す．このように，同形ではない信号波形間の位置ずれをサンプリング分解能を越える精度で補正することができる．

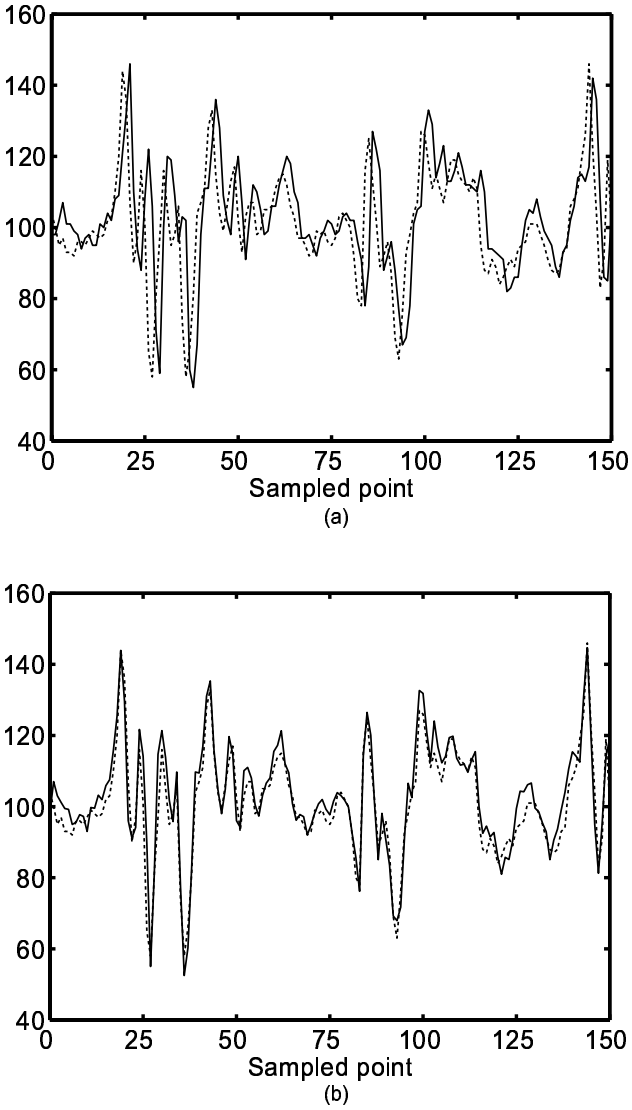

図 2　波形位置合わせの例: (a) 位置合わせ前，(b) 位置合わせ後

3.　差分電力解析への応用

本章では，提案する波形位置合わせ手法を用いた DPA について述べる．まず，提案する DPA の概要について述べる．次に，暗号のソフトウェアモジュールの評価プラットフォームである INSTAC-8 を用いた実験環境について述べる．最後に，共通鍵暗号の一つである DES に対して提案する DPA をおこなった結果を示す．

3.1　波形位置合わせを用いた差分電力解析

電力解析攻撃は，暗号モジュールの処理データによって変化する消費電力に着目して鍵などの秘密情報を読み取る攻撃である．しかし，その消費電力の変化が小さく，測定誤差やノイズなどの影響で測定波形から秘密情報を直接見分けることは困難な場合も多い．DPA は，数千から数万パターンの消費電力波形を統計処理して，わずかな秘密情報を増幅させる攻撃法である．鍵のビットパターンの違いが公開鍵暗号ほど電力波形に現れない共通鍵暗号の実装に対して，単純電力解析（Simple Power Analysis: SPA）よりも有効である．

本稿で提案する DPA の概要を図 3 に示す．従来の DPA では，クロックやトリガ信号によって計測時に波形の位置を合わせている．提案手法はこれに加えて，波形取得後さらに位相限定相関法で極めて高い精度の位置合わせをおこなっている．極端な場合は，計測用のクロックやトリガ信号ですら必要としない．具体的には，まず，取得した波形の中から位置合わせの基準となる波形を一つ決める．次に，位相限定相関およびその高精度化手法（i）〜（iii）を用いて，基準波形と他の波形との位置ずれ量を検出する．得られた位置ずれ量を用いて 2.3 節に示す波形リサンプリングをおこない，位置ずれ補正した波形を生成する．

補正後の処理は従来の DPA と同様である．まず秘密鍵を予測し，その秘密鍵で得られるはずの中間データを計算する．次に，その中間データのうち 1 ビットが 0 か 1 かで消費電力波形を 2 グループに分けて平均を取る．このとき用いる中間データを選択関数と呼ぶ．秘密鍵の予想が合っており，数千から数万パターンの消費電力波形を正しく振り分けることができれば，それを集めた波形にピークが現れる．予想が誤っているとランダムに振り分けられた波形の平均をとることになるため，そのようなピークは現れない．

3.2　測 定 環 境

本実験では，INSTAC-8 準拠プラットフォームの Z80 プロセッサ上にソフトウェア実装した DES を DPA の対象とした．中間データを決定する選択関数には，最終 16 ラウンドの F 関数に含まれる S-box の出力を用いる．F 関数には 8 種類の S-box があり，それぞれの S-box は 6 ビットを入力し，4 ビットを出力する．8 種類の S-box すべての出力 32 ビットを選択関数とし，それぞれで鍵の推定をおこなう．このとき，各 S-box の出力 1 ビットごとに，6 ビットの S-box 入力に XOR される 64(=2^6)

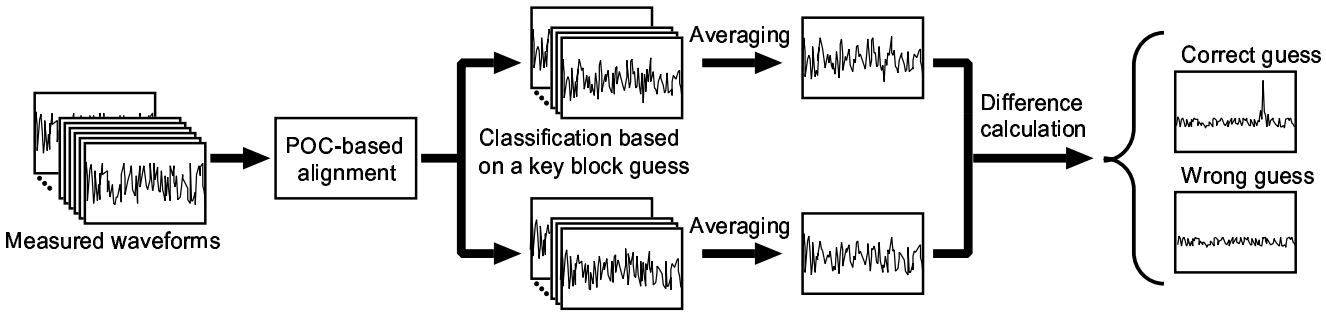

図 3　波形位置合わせを用いた DPA

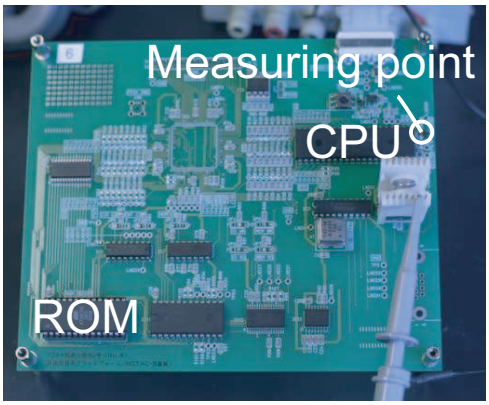

図 4　INSTAC-8 の概観

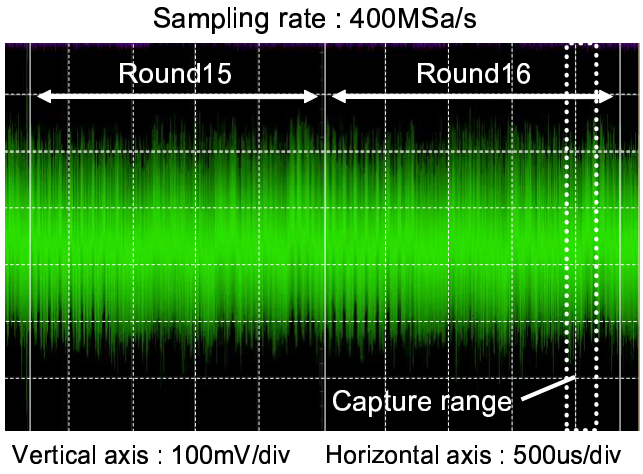

図 5　取得した消費電力波形（波形捕捉範囲は白破線の枠内）

通りの部分鍵候補を試すことになる．DES への DPA についての詳細は文献 [6] を参照されたい．

消費電力波形は，Z80 プロセッサとグランドとの間に挿入された抵抗部分で測定した．INSTAC-8 ボードの概観と測定箇所を図 4 に示す．Agilent 社のディジタルオシロスコープ（DSO6104A）を用い，100MSa/s，200MSa/s，400MSa/s および 1GSa/s それぞれのサンプリングレートにおいて，15 ラウンド開始時のトリガ信号で波形の取得をおこなった． 波形補足の範囲は，S-box1 から 8 までの演算が含まれるトリガ信号発生後 4.22ms からの 0.2ms 間である（図 5）．1 波形の測定ポイント数は，100MSa/s，200MSa/s，400MSa/s，1GSa/s でそれぞれ 20,000，40,000，80,000，200,000 である．波形サンプル数は 1,000 とした．平文には，コンパイラ（LSIC-80）のライブラリ関数（rand 関数）で生成される乱数を使用している．

3.3　結果と考察

位相限定相関法により検出した波形データの位置ずれ量を図 6 に示す．縦軸は位置ずれ量であり，1 ポイントは 5ns（サンプリングレート 200MSa/s）である．横軸は波形サンプルのインデックスである．図 6 に示すように，同一のタイミングで発生させたトリガ信号を用いて取得した波形データにも関わらず，サンプリング間隔以下の微小な位置ずれが観測された．また同時に，位置ずれ量が得られない波形がいくつか観測された．位置ずれはサンプリングレートによらず常に確認された．

図 6 の位置ずれを検出したときの相関ピーク値を図 7 に示す．鍵は同一であるが，異なる平文に対する処理の消費電力波形間の相関であるためピーク値の高さは 0.2 程度となる（完全に同形な波形間の相関ピークは 1 となる）．しかし，図 8(a) のような急峻なピーク特性のため位置ずれ量を検出できる．一方，図 7 で相関ピークが他と比べて大幅に低い波形は，何らかの原因で取得に失敗した全く異なる波形であった．このときに得られた相関値を図 8(b) に示す．このように位置ずれ量の検出により波形取得の成否も判定が可能で，統計処理に悪影響を与える波形はサンプルから除外することができる．これに対して，従来の DPA では取得に失敗した波形も平均されてしまっていることになる．

図 9，10 にそれぞれ位置合わせなしと位置合わせありの DPA 結果を示す．いずれも Sbox1 の同出力の結果である．ここでは，200MSa/s で取得した波形の場合を示す．図 9 のように，位置合わせなしでは誤った鍵の推定時にもっとも高いピークが現れた．一方，位置合わせありでは，正しい鍵推定の場合にのみ高いピークが現れた．ここで，図 9 の方が図 10 と比べてピークとノイズの比が低下していることにも注意されたい．この傾向はすべてのサンプリングレートに共通して観測された．

各サンプリング周波数における DPA 成功率と波形サンプル数の関係を図 11，12 に示す．図 11 は位置合わせなし，図 12 は位置合わせありの結果である．縦軸のエラービット数は，8 つの S-box の出力 32 ビットのうち鍵推定に誤ったビットの数を示す．32 の出力すべてで推定を誤った場合のエラービット数は 32 となる．各 S-box の 4 ビット出力からは，秘密鍵の一部

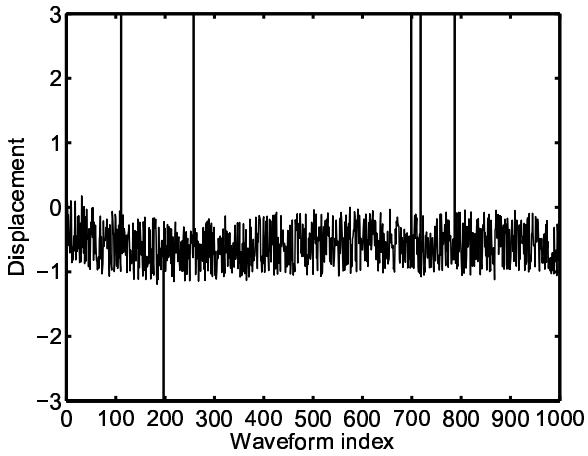

図 6　検出した位置ずれ量

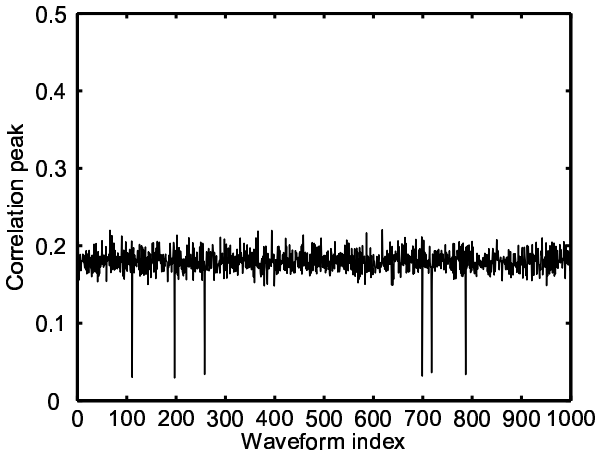

図 7　相関ピークの値

である 6 ビットに対する 4 つの候補が求まる．このうち 2 つ以上が一致していた場合は多数決で鍵候補を絞ることができるので，エラービット数は 0 に下がらなくても問題はない．横軸は統計処理に用いた波形サンプル数である．図 11，12 から，位置合わせありの DPA がすべてのサンプリングレートで位置合わせなしの DPA よりも高い精度で鍵の推定に成功している．200MSa/s および 400MSa/s の DPA 結果をそれぞれ表 1，2 に示す．波形サンプル数は 1,000 である．200MSa/s とサンプリング分解能が低く従来法ではまったく鍵が求まらないような場合でも，位置合わせによって多数決で 50%以上の鍵推定に成功した．また，400MSa/s の場合，位置合わせありのみ多数決によりすべての鍵を正しく推定することができた．鍵推定の精度を同じとする場合は，本手法は従来の 2/3 程度と少ないサンプル数しか必要としないことも図 11,12 からわかる．

1GSa/s で取得した波形では，消費電力の変化に対して十分なサンプリング分解能であることから，位置合わせの有無によらずすべての鍵を推定することができた．一方，100MSa/s で取得した波形では，位置合わせの有無によらず正しい鍵を推定できなかった．これは消費電力の変化に対して十分なサンプリング分解能が得られなかったためと考えられる．なお，文献 [6]

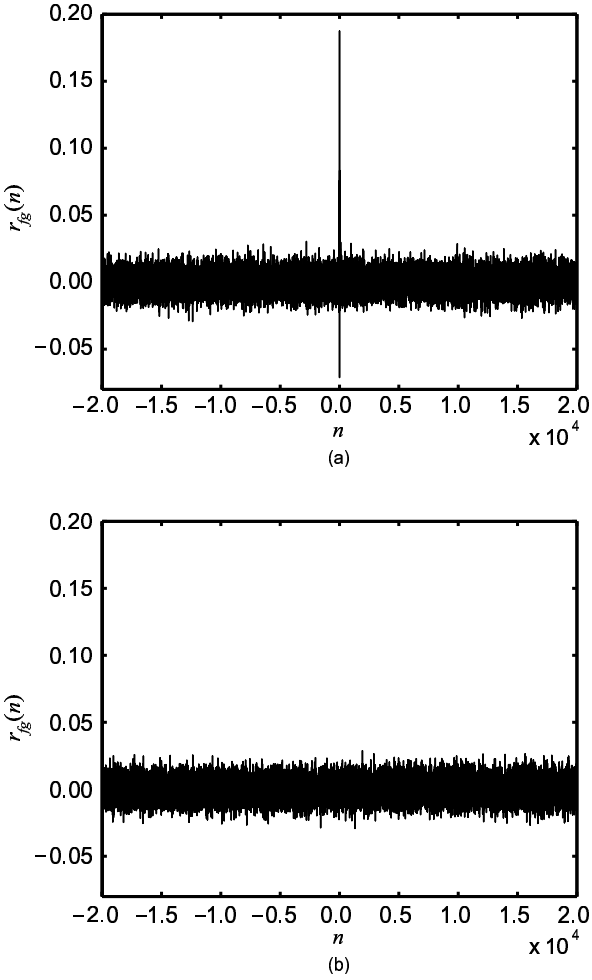

図 8　位相限定相関関数: (a) 相関が高い波形の場合，(b) 相関が低い波形の場合

表 1　200MSa/s の DPA 結果

	Number of successful outputs in 200MSa/s							
	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
DPA	1	1	1	1	0	1	1	1
DPA with POC	1	3	3	1	1	2	2	2

表 2　400MSa/s の DPA 結果

	Number of successful outputs in 400MSa/s							
	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
DPA	2	3	4	2	3	2	3	1
DPA with POC	4	3	4	3	3	3	3	4

では 500MSa/s 以上でのみ DPA の成功が確認されている．

4. おわりに

本稿では，位相限定相関法を用いた高精度な波形位置あわせ手法を提案し，その電力解析攻撃への応用について述べた．提案する手法は，離散フーリエ変換した波形より得られる位相成分から，サンプリング分解能を越える精度で信号波形間の位置

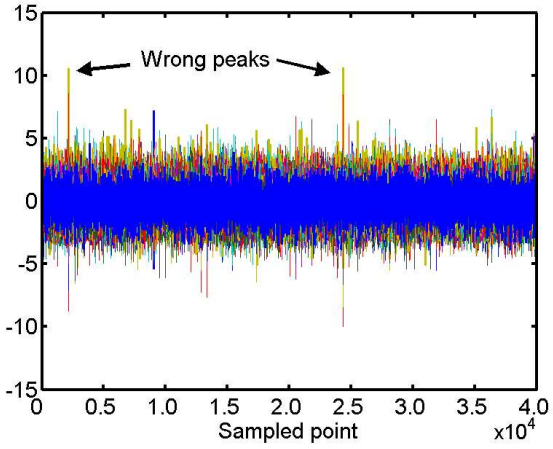

図 9　DPA 結果（位置合わせなし，200MSa/s）

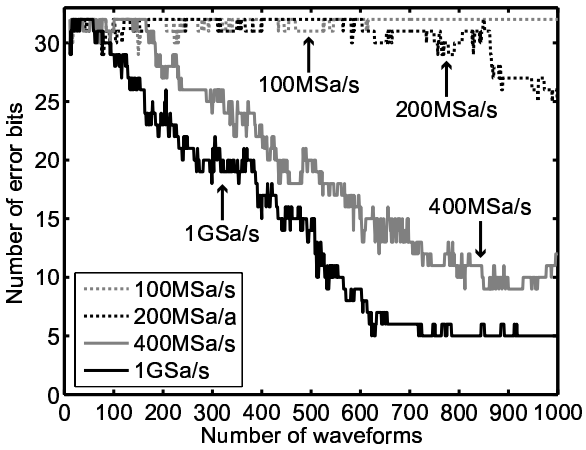

図 11　DPA 成功率と波形サンプル数の関係（位置合わせなし）

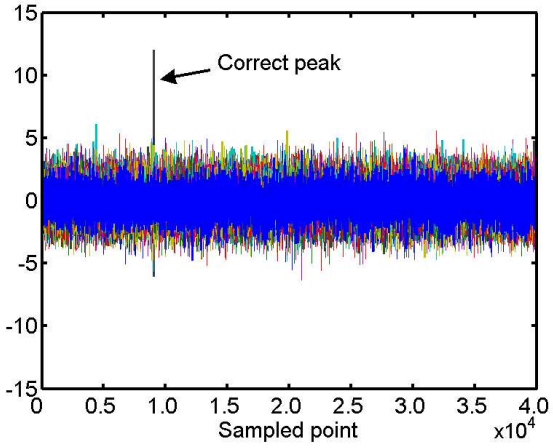

図 10　DPA 結果（位置合わせあり，200MSa/s）

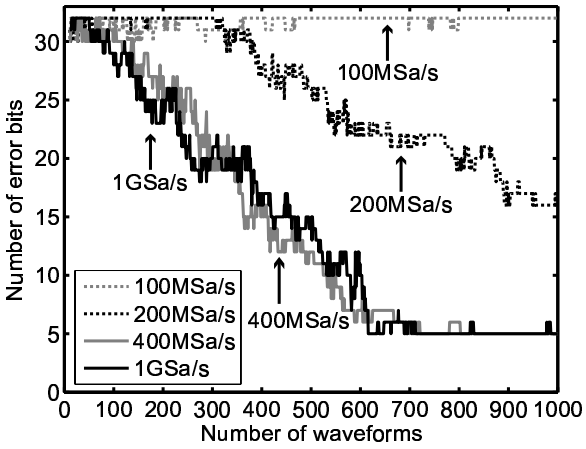

図 12　DPA 成功率と波形サンプル数の関係（位置合わせあり）

ずれ量を補正することができ，また取得のタイミングが大きくずれて DPA の統計処理に悪影響を与える波形を排除することが可能である．この位相限定相関法を用いた DPA を Z80 プロセッサ上の DES のソフトウェア実装に対する DPA に適用した結果，大幅な精度向上を図ることができ，従来の位置合わせを行わない場合には失敗してしまうような低いサンプリングレートでも，あるいは同じサンプリングレートではより少ない波形サンプル数での攻撃に成功した．本稿で提案した位相限定相関法による波形位置合わせ手法は，DES 以外の暗号アルゴリズム，ソフトウェアだけでなくハードウェア実装，電磁波解析攻撃にも大きな効果を発揮し，さらにはトリガ信号やシステムクロックが陽に得られないような場合であっても高い精度での統計処理が期待される汎用性に優れた手法である．今回の DES への応用では，波形位置合わせにより 200MSa/s のサンプリングレートで 2 倍以上成功率が向上した．

文　　献

[1] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. pp. 388–397. Springer-Verlag, 1999. LNCS 1666.

[2] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. pp. 251–261. Springer-Verlag, 2001. LNCS 2162.

[3] K. Takita, T. Aoki, Y. Sasaki, T. Higuchi, and K. Kobayashi. High-accuracy subpixel image registration based on phase-only correlation. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E86-A, No. 8, pp. 1925–1934, August 2003.

[4] K. Takita, M. A. Muquit, T. Aoki, and T. Higuchi. A sub-pixel correspondence search technique for computer vision applications. *IEICE Trans. Fundamentals*, Vol. E87-A, No. 8, pp. 1913–1923, August 2004.

[5] K. Ito, H. Nakajima, K. Kobayashi, T. Aoki, and T. Higuchi. A fingerprint matching algorithm using phase-only correlation. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E87-A, No. 3, pp. 682 – 691, March 2004.

[6] INSTAC 平成 15 年度調査研究報告書 耐タンパー性に関する標準化調査研究開発実証実験報告書 第二部． 2004. http://www.jsa.or.jp/domestic/instac/committe/H15report/report-contents/01_06_02.PDF.