L-007

周波数領域での暗号モジュールの電力解析

Power Analysis of Cryptographic Modules in Frequency Domain

菅原 健†, 本間 尚文†, 林 優一†, 水木 敬明†, 青木 孝文†, 曽根 秀昭†, 佐藤 証‡
Takeshi Sugawara Naofumi Homma Yu-ichi Hayashi Takaaki Mizuki
Takafumi Aoki Hideaki Sone Akashi Satoh

1. まえがき

ディジタル回路の生じるノイズが，周辺機器の誤動作を引き起こすことが知られている[1]．その要因の１つとしては，回路の動作にともなう高周波電流が，電源・グランドプレーンに同時スイッングノイズを生じさせることがあげられる．このような現象は Electromagnetic Compatibility (EMC)の分野において広く研究されており，同時スイッチングノイズ発生のメカニズムや，ノイズの影響を抑制する方法に関する成果が発表されてきた[2, 3].

一方，セキュリティ分野において，電源やグランドの過渡的な変動が回路の動作（計算内容）と相関することに注目し，暗号解読を行う手法が注目されている．このような攻撃は，EMC 分野ではノイズとしか見なされていなかったスイッチングノイズに，実際には暗号モジュールの動作に関する情報（秘密情報）が含まれるために可能となる．このような回路の動作に伴う副次的な物理現象（サイドチャネル情報）を利用して暗号解読を行う攻撃をサイドチャネル攻撃と呼び，特に，回路の消費電力に着目した攻撃を電力解析（攻撃）[4, 5]と呼ぶ.

一般的に利用される暗号アルゴリズムは，多くの研究者による安全性評価の後に標準化されているため，非常に信頼性が高い．しかし，現在，このような安全性評価において，物理的な計測に基づく攻撃は想定されていない．そのため，理論上安全なアルゴリズムであっても，サイドチャネル攻撃が脅威となり得る.

電力解析についても，これまで広く研究がなされており，多くの対策法が発表されている．電力解析への対策は，一般的に，LSI に内蔵される回路もしくはそのアルゴリズムレベルで施される[5]．このような対策手法は，非常に高い安全性を提供する一方，性能に大きなオーバーヘッドを生じる．また，特に回路レベルでの対策を行う場合，既製の部品を用いて構成するモジュールには適用が難しい点も問題となる.

これに対して，安価で効率的な対策としてプリント基板(PCB)レベルの対策が考えられる．具体的には，PCB においてノイズを抑制することで，攻撃への対策となり得る．これは，サイドチャネル攻撃はスイッチングノイズに含まれる情報を抽出するため，秘密情報を含むノイズを抑制すれば，攻撃は困難となるためである．このような手法は，コストの面で，従来の対策手法より有利である．また，EMC の分野において蓄積されたノウハウを活用できるという点においても有望である

ノイズ抑制は，特定の周波数帯を選択的に遮断するフィルタとして実現することが多い．そのため，スイッチングノイズ中で，秘密情報を含む周波数帯を同定することがサイドチャネル攻撃の対策を施す上で重要である.

以上の背景より，本稿では，周波数領域における暗号モジュールの電力解析し，有意な情報を含む周波数帯を同定する手法について述べる．提案手法は，差分電力解析(DPA)を，従来の時間領域でなく周波数領域で行い，その結果を有意な情報を含む周波数帯の同定に使用するものである．提案手法は，標準ブロック暗号 AES [6]を対象とした差分電力解析実験により評価する．さらに，提案手法により同定した有意な帯域を，ディジタルフィルタにより遮断することで，電力解析が困難になることを実験的に確かめる.

2. 差分電力解析

電力解析は，暗号モジュールの電源ノイズに含まれる漏洩情報を利用する．しかし，多くの場合，計測波形に含まれる漏洩情報は，その他のノイズ成分に埋もれている．そのため，1 回の暗号処理に対応する過渡波形では暗号解読には不十分であることが多い．Kocher らによって提案された差分電力解析（Differential Power Analysis: DPA）[4]では，複数の暗号処理に対応する大量の波形を収集し，統計処理により秘密情報を抽出する．Differential という言葉は，波形間の差分を求めるという計算方法に由来するものであるが，現在では統計的な手法を用いた電力解析の総称となっている[5]．本稿では，DPA を改良した手法である Correlation Power Analysis (CPA) [7]について主に扱う.

2.1. Correlation Power Analysis

CPA の攻撃の流れを図 1 に示す．図中において，グレーで表示した *Plaintext*, *Secretkey* は攻撃者にとって未知であり，これらを取得することが攻撃者の目的である．今，N 個の平文 P_1～P_N が暗号化されるとき，攻撃者は対応する暗文 C_1～C_N を収集する．また，これと同時に，処理中の暗号モジュールを計測し，電力波形 W_1～W_N を収集する．ここで電力波形とは LSI の消費電流の時間変動であり，ディジタルオシロスコープを用いて計測するのが一般的である．攻撃者は，消費電力モデルと鍵の予測値を用い，暗文 C_1～C_N から予測電力値 E_1～E_N を計算する．消費電力モデルが成立する場合，鍵の予測値が正しい場合に限り，電力波形 W_1～W_N と予測電力値 E_1～E_N は相関を有する．全ての鍵候補について相関値を計算した後，最も高い相関値を鍵の値が，その真値と判定される．この結果，本来秘密にすべきであった鍵が攻撃者の手に渡り，攻撃が完了する.

本手法は鍵を全探索する Brute-force attack と比較して大幅に計算量を短縮できる．Brute-force attack では，鍵長全体の探索が必要である．一般的に用いられる 128 ビットの鍵では 2^{128} ($\approx 10^{38.5}$)の探索が必要であり，これは現実的な時間で実行不可能である．それに対し，例えば共通鍵暗号

† 東北大学
‡ 産業技術総合研究所

AES に対する CPA では，鍵を 8 ビットごとに分割して探索できる．そのため，探索空間は $2^8 \times 8$ ($\approx 10^{3.6}$)に減少し，現実的な時間で実行可能となる．

2.2. 周波数領域での差分電力解析

上述の DPA(CPA でも同様)のアルゴリズムは，取得した N 枚の波形において，計測タイミングが正確にそろっていることを想定している．しかし現実の攻撃では，暗号モジュールと正確に同期したトリガ信号を取得するのは困難である．この結果，計測波形には位置ずれ誤差が含まれる．もし位置ずれが無視できないほど大きい場合，DPA の解析精度が低下し，鍵の導出により多くの波形が必要になることが知られている．そのため，意図的な時間ずれを挿入する防御法[5]や，信号処理により時間ずれ補正を行う攻撃法が提案されている[8]．

特に，文献[9]では，周波数領域において DPA を行う手法が提案されている．この手法では，図 1 の攻撃フローにおいて，時間波形の変わりに，計測波形 $W_1 \sim W_N$ から，離散フーリエ変換(DFT)を用いて計算した振幅スペクトラムを用いる．この時，振幅スペクトラムは時間領域における位置ずれに対して不変であるため，上述した位置ずれの問題を解決できる．本稿では，この手法を応用し，計測波形の振幅スペクトラムから，有意な情報（情報漏洩）を含む周波数帯を同定する．

3. 情報漏洩を含む周波数帯の同定法

従来の電力解析では，対象のプロセッサアーキテクチャのデータパス幅に関わらず，より少ないビット数（AES の場合例えば 8 ビット）で電力値を予測する．鍵を分割して探索できるのはこのためである．

これに対し，対象の暗号モジュールの安全性評価を行うことを想定し，暗号モジュールについて完全な知識を有する評価者を考える．評価者は鍵を有するため，データパス全体を考慮して，より詳細な予測電力値を計算できる[10]．

評価者は，このような詳細な予測電力値と計測波形の相関を求めることで，相関-時間のグラフを計算できる．この手法により得られた結果は，通常の電力解析の予測電力値から求めた値と比較して，より精度の高いものとなる．これは，従来の解析では残りのビット（データパス幅 128 ビットに対し 8 ビットで予測した場合，128-8=120 ビット）分がノイズ源（アルゴリズミックノイズ[11]）として働くためである．このようにして得た相関値は，DPA に要する波形数を推定するのに用いることができることが知られている[10]．以下では，本手法を既知鍵評価と呼ぶことにする．

提案手法は，上述の既知鍵評価を周波数領域で行う．提案手法のフローを図 2 に示す．まず，設計者は 128 ビットのデータパス幅全体を考慮し，詳細な電力予測値 $E'_1 \sim E'_N$ を計算する．これと同時に，計測した電力波形 $W_1 \sim W_N$ を，DFT により振幅スペクトラム $S_1(f) \sim S_N(f)$ に変換する．その後，設計者は電力予測値 $E'_1 \sim E'_N$ と振幅スペクトラム $S_1(f) \sim S_N(f)$ の間の相関値を計算し，相関-周波数のグラフを計算する．この結果得られたグラフにおいて，高い相関値を得た周波数帯が，有意な情報を含む周波数帯として同定される．

4. 実験

4.1 波形取得

提案手法は，実験により評価した．実験システムのブロック図と実験条件を図 3 と表 1 にそれぞれ示す．実験システムは，サイドチャネル攻撃標準評価基板 SASEBO[12]，オシロスコープ，および PC から構成される．SASEBO 上には 2 つの FPGA (Field Programmable Gate Array): FPGA1 と FPGA2 が搭載されている．FPGA1 上には共通鍵暗号 AES のコア[13]を，FPGA2 には制御回路を搭載した．これらの FPGA は，水晶発振器より入力する 24MHz のクロックにより駆動した．これは，スマートカードのような安価な組込システムにおいて用いられる周波数を想定したものである．計測においては，PC から FPGA2 経由で FPGA1 に平文を入力し，そのたびに暗号化を行った．この時，FPGA1 のグランドピンと基板のグランドプレーンの間に挿入された 1Ω の抵抗器の両端での電圧降下を，ディジタルオシロスコープにより記録した．なお，オシロスコープのトリガは，FPGA の IO ピンより取得した．このような実験を 30,000 個の平文に対して繰り返し行い，対応する 30,000 個の波形を収集した．以降では，これらの波形を電力波形として参照する．電力波形の例と，対応する振幅スペクトラムを図 4, 5 にそれぞれ示す．図 4 において，およそ 140ns の位置において暗号化が開始し，11 サイクル(458 ns=11×1/24MHz)後に完了する．図より，暗号化が行われている区間において，計測値が増大する様子が観察できる．一方，図 5 に示す振幅スペクトラムは，図 4 の時間波形に DFT を適用することで計算したものである．なお横軸は，オシロスコープのサンプリング周波数 4.0GSa/s に対応する有効な周波数 2.0GHz までを表示している．

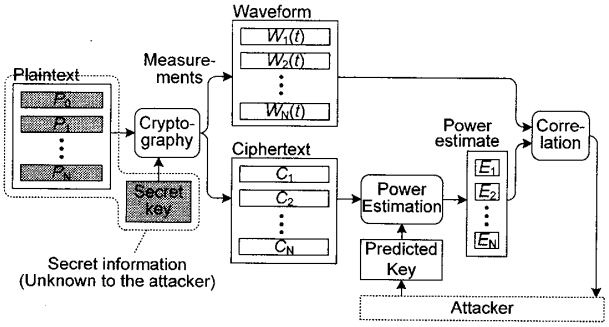

図 1 攻撃の流れ

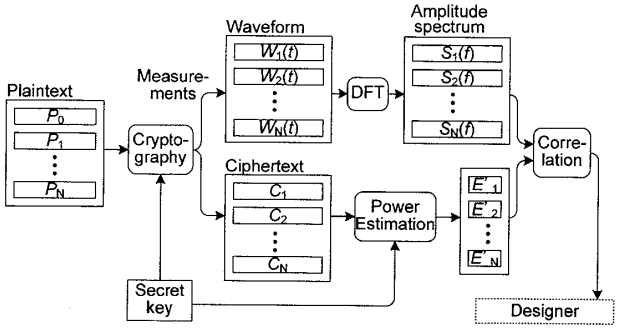

図 2 有意な情報を含む周波数帯を同定する流れ

4.2. 有効な帯域の同定

第 3 節で述べた既知鍵評価および，提案手法（周波数領域での既知鍵評価）の結果を，図 6, 7 にそれぞれ示す．なお，予測電力値は，AES の最終ラウンドを対象とし，電力モデルとしてハミングディスタンスモデルを仮定して計算した．比較のため，誤った予測電力値として，上述の正しい予測電力値をランダムにシャッフルしたものを計算した．図 6, 7 において，正しい予測電力値による相関値を黒，誤った予測電力値による相関値を灰色で示してある．

図 6 において，正しい予測電力値では相関の最大値 0.35 が得られた．これに対し，誤った予測電力値による相関値はほぼゼロである．図 6 の時間—相関のグラフは，550ns 付近で上昇を始め，振動しながらゼロへ収束していく．相関が現れるタイミングは，AES の最終ラウンドが始まる時間と一致する．一方，図 7 に示す周波数領域の結果では，最大の相関値は 0.22 と，図 6 による結果 0.35 と比較して小さかった．これは，DFT を波形全体(0<t<1000ns, 4000 点)に対して適用したため，図 6 において相関を持たない 0<t<550ns の領域がスペクトラムに混入し，相関値を下げたものと考えられる．より短い時間窓で DFT を適用することで結果を改善することも可能であるが，相関を持つ周波数帯を探すという目的のためには，図 7 の結果で十分である．図より，0-50MHz に強い相関があり，比較的小さい相関が 50-500MHz の領域に存在することが分かる．提案手法では，このように相関を有する周波数帯が，暗号処理と相関する情報を有すると同定する．

4.3. 帯域制限した波形への DPA

本節では，前節で有意な情報を含むと判定された周波数帯を制限することで，DPA が困難になることを実証する．前節の結果は，計測波形は 0-50MHz で強い相関を，50-500MHz で弱い相関を有することを示していた．この周波数帯を除去するため，ローパスフィルタ(LPF)およびハイパスフィルタ(HPF)を設計し，計測波形へ適用した．このために，遮断周波数 f_c が 50MHz のもの(LPF1 および HPF1)と，500MHz のもの(LPF2 および HPF2)の合計 4 種類を作成した．それぞれのフィルタの周波数応答を図 8 に示す．これらのフィルタは，計測波形に対して順方向と逆方向の 2 回適用し，ゼロ位相特性に補正した[14].

時間領域での CPA を，5 種類の波形: (i)計測波形，およびフィルタ出力である(ii)LPF1，(iii)HPF1，(iv)LPF2，(v)HPF2 へ適用した．図 9 に，CPA の結果をエラーレートにより表示した．図の縦軸は 16 バイト(=128 ビット)のラウンド鍵全体のうち推定に失敗したバイト数（エラーレート）である．すなわち，値がゼロの時，AES のラウンド鍵全体の解読に成功していることを表す．一方，横軸は，解析に用いた波形数である．少ない波形数で低いエラーレートを示す場合，解析が容易であると言えるため，図より攻撃の難易度を読み取ることが可能である．

(i), (ii)および(iv)は，ほぼ同様のグラフを描いた．これら

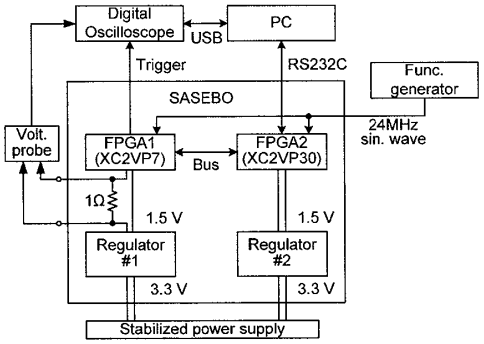

図 3 実験環境のブロック図

表 1 実験条件

	Setup
Oscilloscope	Agilent MSO6104A @ 4.0 GSa/s
Voltage probe	Agilent A1130A with SMA probe head (up to 1.5 GHz)
Operating freq.	24MHz
Num. acquisition	30,000

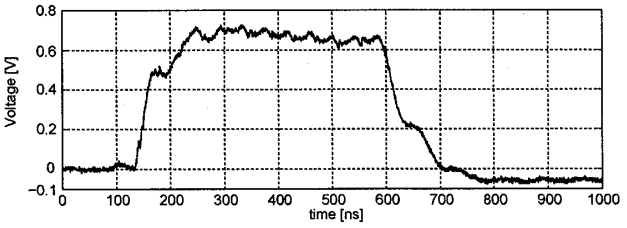

図 4 計測波形の例

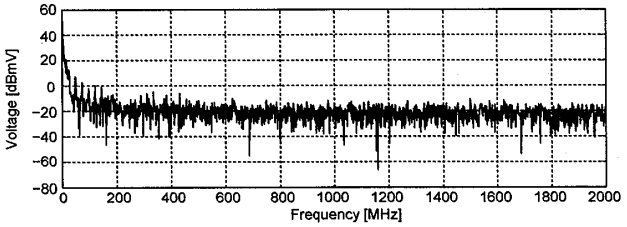

図 5 計測波形の振幅スペクトラムの例

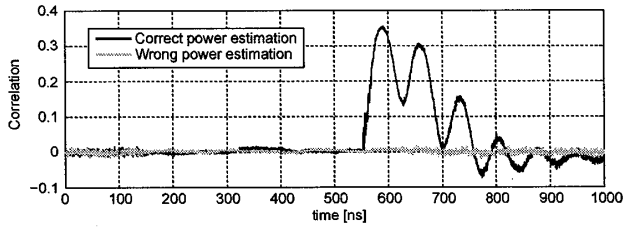

図 6 時間領域での相関値のグラフ

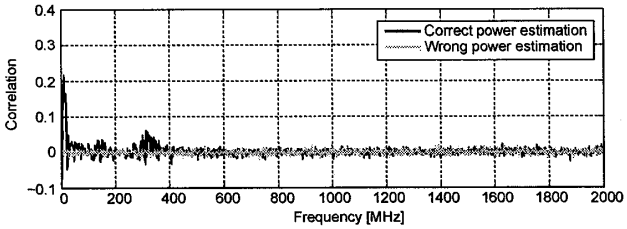

図 7 周波数領域での相関値のグラフ

の結果は，低い帯域(0-50MHz)を共有している．そのため，この領域が CPA の結果を支配したと考えることができる．これは，図 7 において，0-50MHz の帯域が強い相関を持っていたことと合致する．これに対し，(iii)HPF1 を適用すると，この支配的な周波数 0-50MHz が遮断される．これらを比較すると，(iii)による結果は，(i), (ii), (iv)と比較し，解読するのにより多くの波形数を要することが分かる．こ結果，(iii)では，30,000 波形を用いても 16 バイトすべてを解読することはできなかった．これは，図 7 において高い相関を得た周波数帯を遮断することで，CPA による攻撃が困難になったことを示している．

(iii)の結果では，解読は困難にはなったものの，以前として攻撃は成功しており，より多くの波形を用いれば，全体の解読も可能であると予測される．これは，図 7 において弱い相関を得ていた 50-500MHz の帯域による影響によるものと考えられる．これは，0-500MHz の帯域を遮断する(iv)の結果において，鍵の一部さえ取得することができなかったことと合致する．

以上の結果は，提案手法により有意な情報を含む周波数帯の同定が行われたことを示している．また，提案手法により有効な周波数帯域を同定し，その帯域を遮断するような対策を施せば，DPA の対策となることを示すものである．

5. まとめ

本稿では，DPA において有効な周波数帯域を同定する手法を提案した．既知鍵の条件で CPA を実行することで有効な周波数帯を同定した．実験により，同定した周波数帯をフィルタで遮断することで，CPA が困難になることを実証した．本稿の結果より，サイドチャネル情報の漏洩を効率的に遮断するノイズフィルタの設計が可能となる．今後は，様々な実験条件（ほかのデバイスやクロック周波数）において実験を行い，有効な周波数帯域を決定する要因や回路構造の検討を行う予定である．また，PCB へのフィルタの実装方法についても検討する．

参考文献

[1] T. Sudo, H. Sasaki, N. Masuda and J. Drewniak, “Electromagnetic interference (EMI) of system-on-package (SOP),” IEEE Trans. Advanced Packaging, 27(2), pp. 304--314, 2004

[2] C. R. Paul, “Introduction to Electromagnetic Compatibility (Wiley Series in Microwave and Optical Engineering),” Wiley-Interscience, 2006

[3] D. Hockanson, J. Drewniak, T. Hubing, T. Van Doren, F. Sha, and M.Wilhelm, "Investigation of fundamental EMI source mechanisms driving common-mode radiation from printed circuit boards with attached cables," IEEE Trans. Electromagn. Compat., vol. 38, no. 4, pp. 557-566, Nov. 1996.

[4] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” CRYPTO 1999, Lecture Notes in Computer Science, vol.1666, pp.388 – 397, Aug. 1999.

[5] S. Mangard, E. Oswald, T. Popp, “Power Analysis Attacks: Revealing the Secrets of Smart Cards,” Springer-Verlag, 2007.

[6] NIST, "Advanced Encryption Standard (AES) FIPS Publication 197," Nov. 2001.

[7] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model,” CHES 2004, LNCS 3156, pp. 16-29, 2004.

[8] N. Homma, S. Nagashima, Y. Imai, T. Aoki, and A. Satoh, "High-resolution Side-Channel Attack Using Phase-Based Waveform Matching," CHES2006, LNCS4249, pp. 187-200, 2006.

[9] H.C. Gebotys, S. Ho, and C.C. Tiu, “EM analysis of Rijndael and ECC on a Wireless Java-based PDA,” CHES 2005, LNCS, vol.3659, pp.250 – 264, Aug. 2005.

[10] 渡部，高橋，松本, "暗号モジュールへの信号ラインからのサイドチャネル攻撃 (2) - 詳細実験結果 -," コンピュータセキュリティシンポジウム 2008 (CSS2008), Oct. 2008.

[11] F. -X. Standaert, S. B. Őrs, and B. Preneel, "Power Analysis of an FPGA Implementation of Rijndael: Is Pipelining a DPA Countermeasure?," CHES 2004, LNCS3156, pp. 30-44, Aug. 2004.

[12] Research Center for Information Security, AIST, ”Side-channel Attack Standard Evaluation Board (SASEBO),” http://www.rcis.aist.go.jp/special/ SASEBO/index-en.html

[13] “Cryptographic Hardware Project,” Computer Structures Laboratory, Graduate School of Information Sciences, Tohoku University, http://www.aoki.ecei.tohoku.ac.jp/crypto/.

[14] Oppenheim, A.V., and R.W. Schafer, “Problem 5.39,” in Discrete-Time Signal Processing, Prentice-Hall, 1989.

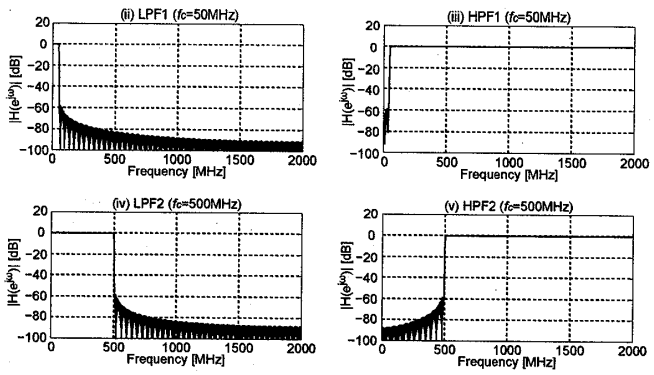

図 8 設計したフィルタの周波数応答

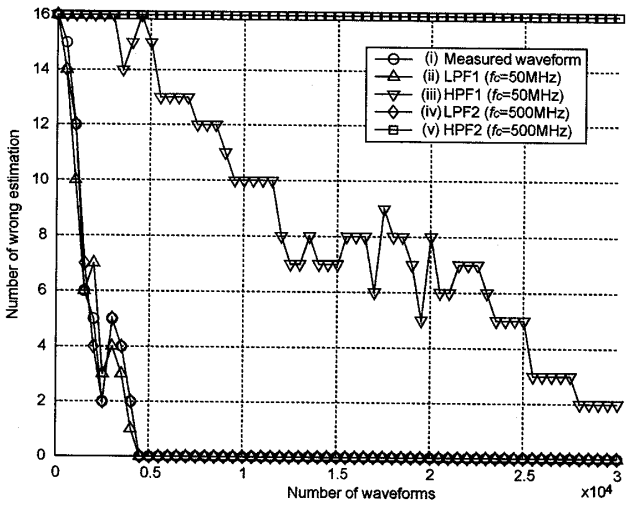

図 9 CPA の結果（エラーレート）