異なる実装方法による暗号モジュールに対する離散フーリエ変換を用いたCPAの適用

CPA using DFT for the encryption module by the different implementation methods

櫻井　敦規†　　岩井　啓輔†　　黒川　恭一†

Atsunori Sakurai, Keisuke Iwai, and Takakazu Kurokawa

1．はじめに

情報通信技術の発達と普及により，通信の安全性を高めるため，暗号技術が使われている．暗号の安全性は，暗号文及び平文から秘密鍵を算出するための処理に要する時間が膨大になることを利用しており，現在使用されている暗号は現実的な時間内に解読が困難とされている．しかしながら，近年，消費電力や電磁波などのサイドチャネル情報を利用した攻撃が注目され，現実的な脅威となりつつある．電力解析には，Brier らによって提案された CPA (Correlation Power Analysis) [1]がある．ここでは，実装方法の異なる AES 暗号モジュールに対して離散フーリエ変換を用いた周波数領域での CPA を行い，デバイスの実装方法や動作周波数，シャント抵抗の影響について検証を行った結果を示す．

2．周波数領域での CPA

CPA のアルゴリズムでは，取得した波形の計測タイミングが正確であることが想定しているが，実際の攻撃においては，タイミングを完全に一致させることは困難である．そこで，文献[2]では，周波数領域で CPA を行う手法が提案されている．この手法では，取得した波形の計測データに対し離散フーリエ変換を行い，振幅スペクトラムに変換し，得られた振幅スペクトラムと予想鍵を用いて予測した消費電力との相関を計算するものである．この手法により，振幅スペクトラムは時間領域の位置ずれによらず一定の値となるため，タイミングの問題を解消することができる．

3．実験

3．1　実験環境

評価基板には，産業技術総合研究所及び東北大学で開発されたサイドチャネル攻撃用標準評価基板 SASEBO-G 及び SASEBO-R を用いた[3]．AES 回路は，合成体による S-box を用いた AES 回路とし，SASEBO-R には FPGA と同様のノードを持つネットリストとなるように制約を与えて論理合成された AES-S を用いた．

オシロスコープには IWATSU DS-4354ML，電源には KIKUSUI PMM18-2.5DU を用いた．クロックには NFCK1615 から 12MHz から 24MHz まで 4MHz ごとの異なるクロックを供給した．測定は xc2vp7 または ASIC の core 側の GND の測定ポイントを用いて，シャント抵抗が 1Ω，2Ω，4Ω の3通りで行い，AES の 10 ラウンド開始から 1μ秒を測定した．この区間に対して離散フーリエ変換を行った．CPA には，サイドチャネル攻撃評価用自動測定ソフトウェア[4] を用いた．

3．2　SASEBO-R の実験結果

SASEBO-R の動作周波数及びシャント抵抗値を変化させた場合の離散フーリエ変換を用いた CPA の結果の例として，動作周波数を 12MHz，24MHz とした結果を図1に示す．CPA は，200MHz までの帯域は 50MHz ごとに，それ以降は 100MHz ごとに実施した．全般に 0－50MHz 及び 50－100MHz の周波数帯に相関が取れることが確認できた．また，シャント抵抗値が2Ωで動作周波数が低いほど結果が良好になっていることが確認できる．

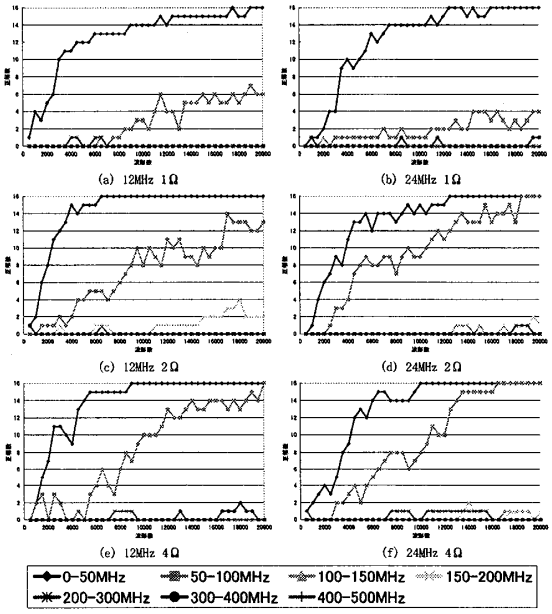

図1　SASEBO-R の離散フーリエ変換を用いた CPA

次に，取得波形 20000 個を用いて，0－100MHz における正解鍵の相関値を比較する．図2はシャント抵抗を 1Ωに固定し，動作周波数を変化させた場合を示し，図3は動作周波数を 16MHz に固定し，シャント抵抗を変化させた場合を示している．

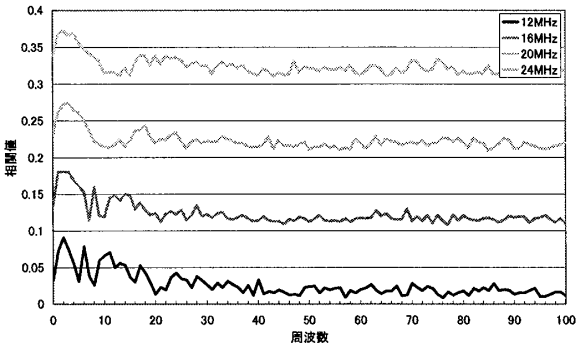

図2　SASEBO-R　正解鍵の相関値　1Ω

† 防衛大学校　情報工学科
Department of Computer Science, National Defense Academy

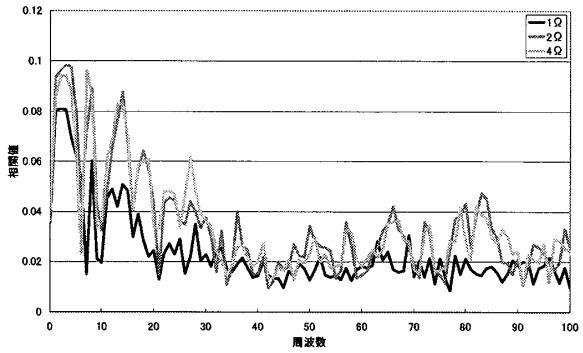

図３　SASEBO-R　正解鍵の相関値　16MHz

シャント抵抗値が大きくなるにつれ，ピーク値の周波数が低くなり，動作周波数が高くなるにつれ，相関値のピーク値が現れる周波数が高くなる傾向が確認できた．

３．３　SASEBO-G の実験結果

SASEBO-G の動作周波数及びシャント抵抗値を変化させた場合の離散フーリエ変換を用いた CPA の結果の例として図４に示す．全般に 0－50MHz の周波数帯に相関が取れることが確認できた．また，シャント抵抗値が 1Ω で動作周波数が低いほど結果が良好になっていることが確認できる．

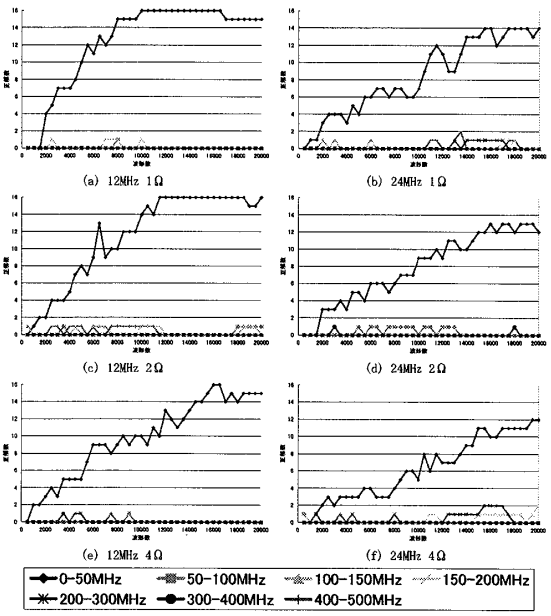

図４　SASEBO-G の離散フーリエ変換を用いた CPA

次に，取得波形 20000 個を用いて，0－100MHz における正解鍵の相関値を比較する．図５はシャント抵抗を 2Ω に固定し，動作周波数を変化させた場合を示し，図６は動作周波数を 12MHz に固定し，シャント抵抗を変化させた場合を示している．

シャント抵抗値が大きくなるにつれ，ピーク値の周波数が低くなり，動作周波数が高くなるにつれ，相関値のピーク値が現れる周波数が高くなる傾向が確認できた．

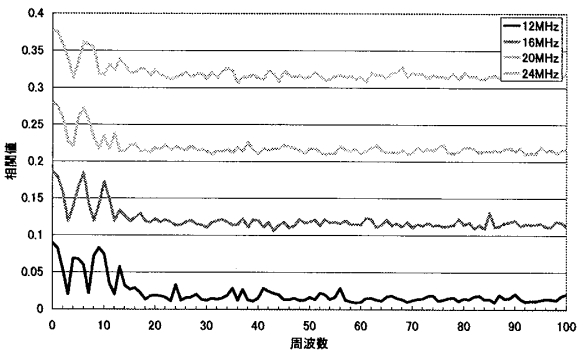

図５　SASEBO-G　正解鍵の相関値　2Ω

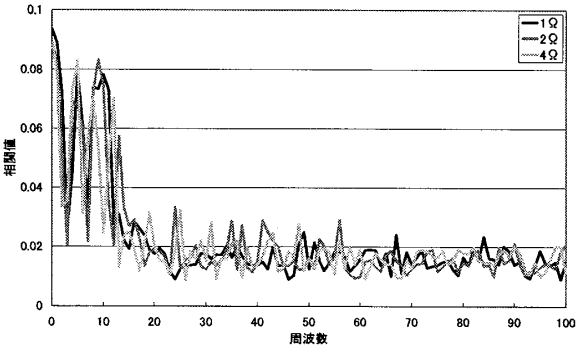

図６　SASEBO-G　正解鍵の相関値　12MHz

４．まとめ

SASEBO-R，SASEBO-G ともに，動作周波数及びシャント抵抗の違いによる相関値のピーク周波数の変動傾向は同様であることが確認できた．しかしながら，SASEBO-R，及び SASEBO-G は同じ回路構成の AES で CPA を行ったにもかかわらず，相関のとれる周波数帯は大きく異なっていることから，回路構成が同じでも，使用するデバイスごとに対策が必要となる周波数帯が異なることが考えられる．

今後の課題として，周波数変化の原因の特定とデバイスに適した対策の手法について研究を行う必要があると考える．

参考文献

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

[2]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，“ 周波数領域での暗号モジュールの電力解析，” 情報科学技術フォーラム，Vol. FIT2009 講演論文集 4 分冊，pp. 135-138, 2009.

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

[4]岩井啓輔，南崎大作，黒川恭一，“サイドチャネル攻撃評価用自動測定ソフトウェアの開発，” 電子情報通信学会技術研究報告，Vol. 108, No. 38, ISEC2008 1-15, pp. 9-14, 2008.