サイドチャネル攻撃標準評価ボード(SASEBO)を使った AES 暗号の実装攻撃実験

南崎　大作†　岩井　啓輔†　黒川　恭一†
防衛大学校情報工学科†

1　はじめに

情報関連産業や関連技術が顕著な成長を見せ、インターネットや携帯電話の普及に伴い、通信の安全な利用に対する要求が高まり、通信セキュリティに対する研究はその重要性を増している。

サイドチャネル攻撃に関する研究が盛んに行われている昨今、実験に関する統一評価手法の確立を目的として、標準評価プラットフォーム仕様 INSTAC-8 及び INSTAC-32 が策定され、それらの準拠ボードが開発された。[1][2]

本稿では、それらの準拠ボードを用いた暗号モジュールへの攻撃実験から得られた知見を生かし、産業技術総合研究所及び東北大学が新たに開発したサイドチャネル攻撃標準評価ボード(SASEBO : Side-Channe Attack Standard Evaluation Board)に対して共通鍵ブロック暗号を実装し、サイドチャネル攻撃に関する検証を行った結果を示す。

2　サイドチャネル攻撃

2.1 概　要

サイドチャネル攻撃は、暗号化を行う際に暗号デバイスの内部動作に応じて変化する電流、電圧、電磁波処理時間等を漏洩情報として利用し、秘密情報を解析しようとするものである。

サイドチャネル攻撃には、消費電力を利用する電力解析攻撃、暗号デバイスから放射される電磁波を利用する電磁波解析攻撃、計算機が動作中に発するノイズを利用する音響解析攻撃などがある。

本研究では Kocher らによって提案された単純電力解析(SPA : Simple Power Analysis)[3]を AES 暗号に適用して SASEBO ボードの性能を検証する。

2.2ＳＰＡ(Simple Power Analysis)

サイドチャネル攻撃の一種であり、漏洩情報として電力消費量を用いて、秘密情報を推定する。秘密情報の推定の際に、統計的手法を用いずに、電力消費量の波形を直接観測することにより、秘密情報を推定する。

SPA experiments of AES circuit on SASEBO
†Daisaku MINAMIZAKI, Keisuke IWAI, and Takakazu KUROKAWA
†Department of Computer Science, National Defence Academy

3　SASEBO

3.1 SASEBO の概要

SASEBO は PowerPC プロセッサコアを内蔵した Xilinx 社の FPGA(XC2VP7,XC2VP30)を搭載したサイドチャネル攻撃評価用標準プラットフォームであり、FPGA 上に共通鍵暗号をハードウェア実装し、データの暗号化及び復号を行うマルチチップ組み込み型の暗号ハードウェアモジュールである。また、AES 回路とのデータの入出力については RS232C によるシリアルインタフェースを通して行う。

図 1 に SASEBO-FPGA ボードのブロック図を示す。

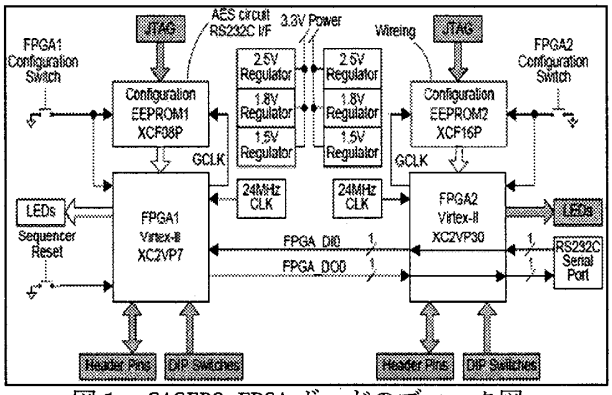

図 1　SASEBO-FPGA ボードのブロック図

3.2 解析システムの概要

本研究では、図 2 に示すような電力解析のための環境を整えた。

システムの構成は、暗号処理を行う SASEBO ボード、消費電力データを測定するデジタルオシロスコープ、電源及びデータ解析用の PC である。

SASEBO による暗号処理時の消費電力データは、デジタルオシロスコープで測定記録され、解析用 PC に転送し、Excel により解析する。また、FPGA のコンフィギュレーションにもこの PC を使用した。

3.3 暗号回路の実装

実装する暗号は共通鍵ブロック暗号 AES(Advanced Encryption Standard)として Verilog-HDL で記述し、ボード上の FPGA への論理合成及び配置配線には Xilinx ISE9.1i を用いた。なお、本研究で実装した AES 暗号は産業技術総合研究所及び東北大学から提供されたコードである。[1]

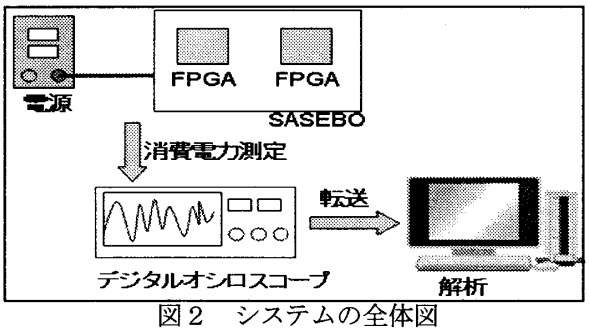

図２　システムの全体図

4　測　定

4.1 測定方法

今回の測定では、まず我々に配布された２つの SASEBO に AES 暗号を実装し SPA 実験し、ロットの違いを検証してみた。

AES 暗号では、128 ビットの秘密鍵を設定し、平文を暗号化する際の最終ラウンドの消費電力を測定・解析する。消費電力の波形については、SASEBO-FPGA のグランド側に挿入された抵抗における電圧変動をプローブを使用して測定した。また、Verilog-HDL によるプログラムを実装する際、デジタルオシロスコープ用のトリガとなりうる信号を出力するようにしてある。

4.2 測定結果

図３及び図４にロットの違う２つの SASEBO(G01241,G01242)の測定波形(最終ラウンド)を示す。図３及び図４から、２つの測定波形を比較すると、最終ラウンドにおける電圧は、どちらのボードにおいても約 18mV という測定結果を得ることができた。

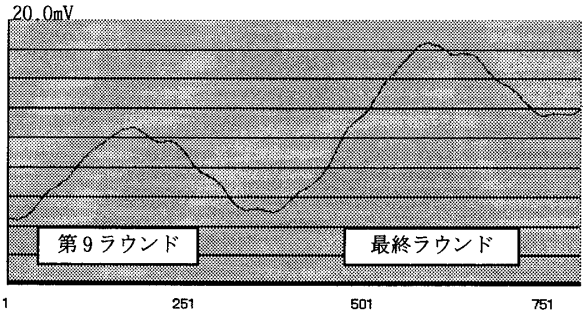

図３　SASEBO(G01241)

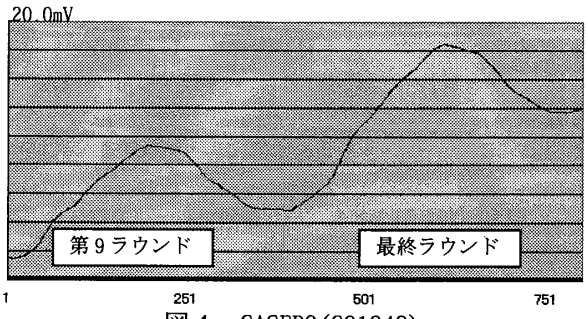

図４　SASEBO(G01242)

また、その他の比較対照として、我々の所有している SCAPE ドーターボード B(XC2VP70)にも同様に AES 暗号を実装し SPA 実験を行い、SASEBO との消費電力の比較を実施した。SCAPE ドーターボード B では、Vccint 側を測定ポイントとし、core 電圧は 1.5V である。図５に SCAPE ドーターボード B の測定波形を示す。

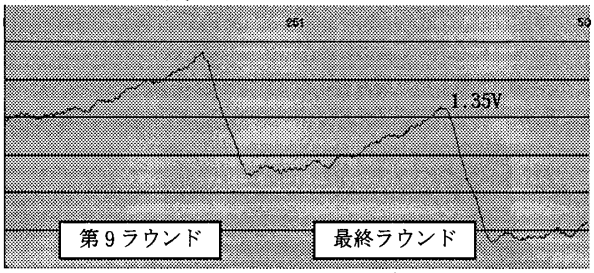

図５　SCAPE ドーターボード B

暗号化が始まるとラウンドが進むにつれて徐々に電圧が降下し、最終ラウンド時には約 150mV の降下が確認できた。

5　まとめ

今回の測定の結果、SASEBO のロットの違いによる SPA の測定波形については、若干の差異は認められたものの、どちらもほぼ同じ測定波形を得ることが出来たことからロットの違いによる波形の違いは認められなかった。

また、SASEBO の最終ラウンドにおける初期状態からの電圧変化は約 18.0mV であるのに対して、SCAPE ドーターボード B は約 150mV あったということで、２種のボードにおける電圧変化には非常に大きな差があることが確認できた。

本稿では、我々が所有している SASEBO 及び SCAPE ドーターボード B に AES 暗号を実装し、SPA を行い測定波形の特徴を確認したが、今後は DPA(Differential Power Analysis)を拡張した手法である CPA(Correlation Power Analysis)を同ボードに対して適用し、解析・評価する予定である。

参考文献

[1]東北大学・産業技術総合研究所 暗号ハードウエア開発プロジェクト"SASEBO-AES 暗号 FPGA ボード 仕様書,"

[2]菅原健,本間尚文,青木孝文,佐藤証, "サイドチャネル攻撃標準評価 FPGA ボードを用いた暗号ハードウェアに対する電力解析攻撃," マルチメディア，分散，協調とモバイルシンポジウム，No.7D-5，pp.1415-1420，July 2007.

[3]P. Kocher, J. Jaffe, B. Jun,: Differential Power Analysis," CRYPTO 1999,LNCS,Vol.1666, pp.388-397,August 1999.