M_052

DPA対策実験による電力解析評価プラットフォームの検証

Verifcation on power analysis platform by the experiment against DPA

辻 洋平† 岩井 啓輔† 黒川 恭一†
Yohei Tsuji Keisuke Iwai Takakazu Kurukawa

1 はじめに

セキュリティ攻撃のひとつであるサイドチャネルアタックは，消費電力やデータ出力タイミング等の情報を観測し，その情報から統計的手法を用いて秘密情報を推定する．サイドチャネルアタックの中でも有効な攻撃法であるDPA（電力差分解析）やSPA（単純電力解析）への対策及びその評価を行うためには，専用プラットフォームが必要である．[1],[2]

現在サイドチャネルアタック専用プラットフォームとしては，(株) 三菱電機が開発したSCAPE(Side Channel Attak Platform for Evaluation) と財団法人日本規格協会情報技術標準化研究センター (INSTAC) からの委託で (株) 東芝が開発したINSTAC-32などがある．

それぞれのプラットフォームは，SCAPEがマザーボード，ドーターボードA及びドーターボードBで，一方INSTAC-32はマザーボード，CPUボード及びFPGAボードから構成されている．本研究については，これら2つのプラットフォームでDPAを行った際に，期待する成果が得られるかを検証したものである．

2 本研究の概要

本研究においては，SCAPEのドーターボードAとINSTAC-32のFPGAボードを用いた．それぞれの基板にはXilinx社製のFPGAが搭載されている．表1にそれぞれのFPGAの諸元を示す。Virtexシリーズは1個のCLBが2スライスを持ち，1スライスに対して2個の4入力LUT及びFFを含んでいる．コア電源電圧は2.5vである．それに対し，VirtexIIシリーズは1個のCLBが4スライスを持つ．LUT及びFFの数はVirtexシリーズ同様の2個ずつを含んでいる．コア電源電圧も1.5vであり，Virtexシリーズに比べて低電圧で動作する．外部形状もVirtexシリーズに比べて約4分の1程度の大きさになっている．

検証内容については，DPA無対策AND回路及びマスク論理素子を用いてマスク処理を施したAND回路の電力波形を測定して，それぞれのプラットフォームでどのような電力差分波形が導出できるかを検証した．

回路の設計等はXilinxのISE7.1iを使用し，測定はIWATSUのデジタルオシロスコープDS-4354MLを使用した．検証環境の概観を図1に示す．左にあるSCAPEのドーターボードAに電源やオシロスコープをセッティングして測定準備を整えた所である．また，右にINSTAC-32のFPGAボードを並べてある．なお，INSTAC-32にはディップスイッチがない為，別途手動スイッチを作成した．

表1: FPGAの諸元

項目	SCAPE	INSTAC-32
FPGA	Virtex XCV1000	VirtexII XC2V1000
コア電源	2.5v	1.5v
CLB数	64 × 96	40 × 32
SLICE数	12,288	5,120
FF数	24,576	10,240

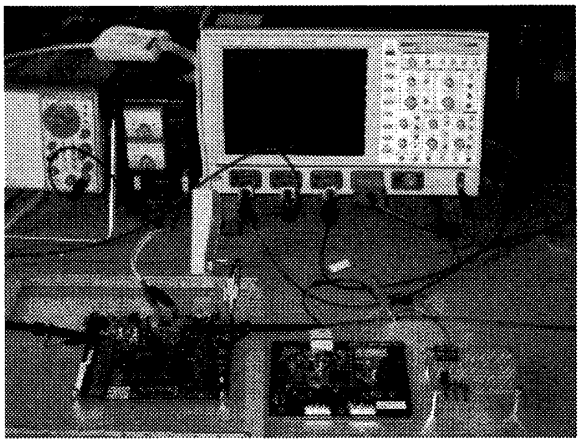

図1: 検証環境

3 DPA無対策AND回路の検証

本章では，マスク処理を施していないAND回路を用いてDPAを行った検証結果を述べる。それぞれのプラットフォームではFPGAの規模が異なるため，それぞれのFPGAが保有するLUTの約1%分のAND回路をFPGA内で均等に設置されるように設計して実施した．

3.1 SCAPEによる検証

SCAPE上のFPGAに搭載されているLUTは約24,000個であるので，240個の2入力AND回路を実装して検証を行った．2つの入力のうち片方を固定して，もう片方の入力についてはLFSRより供給し，逐次AND回路の電力波形を測定した．4000回の電力差

† 防衛大学校 情報工学科

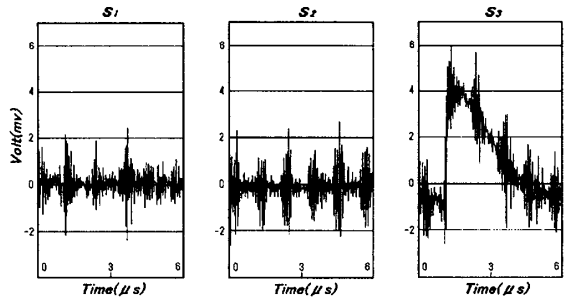

図 2: SCAPE による無対策 AND 回路の検証結果

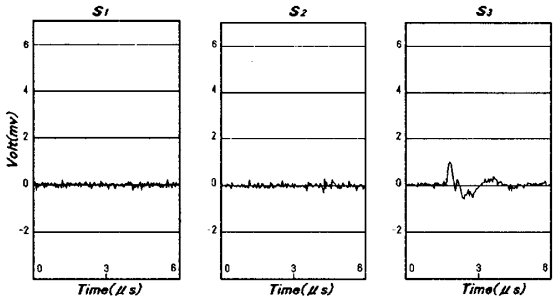

図 3: INSTAC-32 による無対策 AND 回路の検証結果

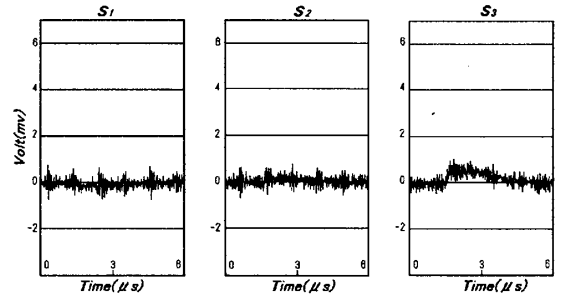

図 4: SCAPE による DPA 対策 AND 回路の検証結果

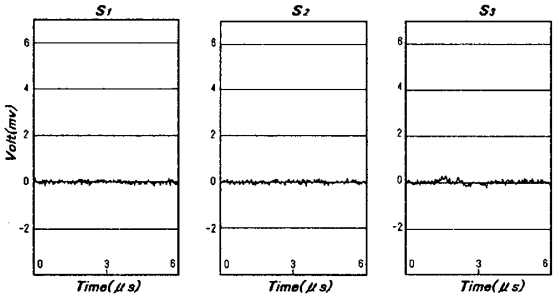

図 5: INSTAC-32 による DPA 対策 AND 回路の検証結果

分の結果を図 2 に示す．左より入力 0 同士の差分，入力 1 同士の差分，及び入力 0 と 1 の差分を取ったものである。図 2 の結果より，入力が異なると差分にパルスを見ることができた．なお，クロックは水晶発振器 4MHz を用いた．一定間隔に現れるノイズは水晶発振器の影響であると考えられる．

3.2 INSTAC-32 による検証

INSTAC-32 上の FPGA に搭載されている LUT は約 10,200 個であるので，LUT 約 1 %分の 102 個の 2 入力 AND 回路を用いて 3.1 と同様の方法で検証を行った．図 3 の結果より，INSTAC-32 についても入力が異なると差分に明らかなパルスを見ることができた．なお，SCAPE よりも全体的なノイズレベルが小さいのは，INSTAC-32 が FPGA ボードに備え付けられている小型水晶発振器 TCO-787RH3 を使用したのが一因と考えている．この水晶発振器によるノイズ等の影響は少ないのが分かる．

4 DPA 対策 AND 回路の検証

ここでは，マスク処理を施した AND ゲートに対して DPA を行った検証結果を述べる．DPA 対策としては，Messerges の提案した AND 回路のマスク方法を採用した．[3]　この方法は不十分であり，消費電力の差分にパルスが出るはずであることが分かっている．[4]

なお回路設計の制約上どちらのプラットフォームにおいても，マスク処理を施した AND 回路 100 個を用いて検証した。

4.1 SCAPE による検証

実験要領は 3.1 と同様である．マスク処理のための入力 2 つには，それぞれ LSFR の出力を使用した．マスク効果が現れて消費電力の差分におけるパルス発生が抑えられているが，図 4 の S3 を見ると明らかなように，まだ明確にパルスを見ることができる．今回のクロックは水晶発振器 1MHz を用いた．3.1 の 4MHz での測定に比べるとノイズ等の影響が少ないのが分かる．

4.2 INSTAC-32 による検証

INSTAC-32 についてもマスク効果は現れているものの，図 5 の S3 の結果のように SCAPE よりその度合いは低いものとなった．

5 結論

本研究は SCAPE と INSTAC-32 という 2 つのプラットフォームに対して，複数個の AND 回路の消費電力差を測定することで，DPA 対策及び評価を行うことができるかどうかを検証したものであった．どちらのプラットフォームに関しても，DPA 無対策の AND 回路に関してはその消費電力差を確認することができた．また，Messerges の提案したマスク方法の不十分な点から，消費電力差においてパルスを確認することもできた．以上の成果により，SCAPE と INSTAC-32 の両プラットフォームは共に成果を得ることができるものであることが分かった．

なお，DPA 及び SPA の実験検証等を行う際には，SCAPE 及び INSTAC-32 に搭載されている FPGA 自体の消費電力にも大きな差があること，また外部の水晶発振器などは測定環境に大きく影響を与えることを十分考慮しなければならない．

参考文献

[1] P.Kocher, "Timing attacks on implementations of Diffe-Hellmann, RSA, DSS, and Other systems", Proc. Advances in Cryptology - Crypto'96, LNCS 1109, pp. 104-113, 1996.

[2] P.Kocher, J. Jaffe, B. Jun, "Differential power analysis", Advances in Cryptology - Crypto'99, LNCS 1666, pp. 388-397, 1999.

[3] T.Messerges, "Securing the AES finalists against power analysis attack," FSE2000, LNCS1978, 150-164, 2001.

[4] 清水 秀雄：マスク論理素子を使ったサイドチャネル攻撃対策，電子情報通信学会技術研究報告，ISEC2004, Vol.104, No.315, pp.15-19, 2004.9.