6W-10

XOR 演算を対象にしたサイドチャネル攻撃手法の検証

辻 洋平 †　　岩井 啓輔 †　　黒川 恭一 †
防 衛 大 学 校 ††

1　はじめに

暗号デバイスに対する攻撃手法として，暗号処理時間や消費電力等の情報を利用して秘密鍵を推定するサイドチャネル攻撃 [1] が注目されている．電力差分解析 (Differential Power Analysis,DPA) はこのサイドチャネル攻撃の 1 つであり，消費電力情報を統計処理することで秘密鍵を推定する強力な攻撃手法である [2].

我々は，ストリーム暗号の keysetup 時や鍵付きハッシュ関数に多く用いられている XOR 演算部が電力差分解析に対する脆弱性 [3][4] について指摘されている点に注目した．本稿では，XOR 演算部を対象にした DPA の実装検証を行った結果を示す.

2　XOR 演算に対する DPA 検証

DPA を行うことで，秘密情報の解析を可能にする情報 (本稿ではリークと呼ぶ) が得られる．CMOS 回路において，このようなリークを得ることができる基本的な要因の一つに，演算素子の遷移確率の偏りがあることが知られている [5][6]．XOR 演算に対する DPA に関しても，演算素子の遷移の有無に起因し，1 ビット単位の DPA[3] 及び Multi-bit DPA[4] などの DPA 手法が提案されている．そこで本研究ではこれらの DPA 手法を検証した.

図 1 のような攻撃対象となる演算モデルを FPGA に実装して検証した．複数ビット長の X（公開可変），Y（秘密固定）を XOR の入力とする．演算結果は Z（入手不可）として出力される．DPA の目標は，公開可変な入力 X を利用して，秘密固定情報 Y を特定することである.

また，XOR 演算部では，毎回の演算実施前に，既定の初期値で初期化されるものとする.

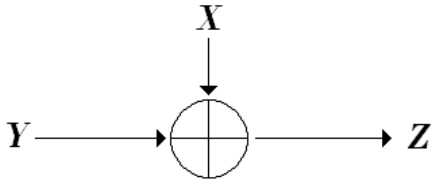


図 1: 攻撃対象の演算モデル

検証では，情報技術標準化研究センター (INSTAC) により設計された INSTAC-32 準拠評価用標準プラットフォームである FPGA ボードを使用した．FPGA ボードには Xilinx 社の FPGA VirtexII が搭載されている．回路の設計は Xilinx 社の ISE8.2i 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．FPGA ボードへの供給電圧は 3.3v，動作周波数は $2MHz$ であり，オシロスコープのサンプリングレートは $1Gsample/Sec$ とした．検証環境の概観を図 2 に示す.

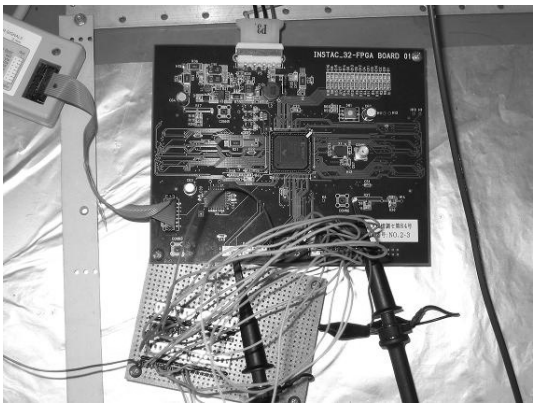


図 2: 検証環境

2.1　1 ビット単位の DPA 検証

まず，特定目標とするビット（ターゲットビット）に対して入力 Y の値を推測する．その推測した入力 Y と入力 X によって計算される Z に対応するビットの値に応じて，出力 Z を 2 つのグループに分類する．それぞれの XOR 演算部での消費電力を計測して，グループ分けし，それぞれの平均消費電力を計算する．この際ターゲットビット以外のビットから定まる電力消費量については，平均化されることで相殺されるため，電力消費量の大小に関しては，ターゲットビットの XOR 演算部における遷移の有無に依存することになる．よってターゲットビットの値を平均消費電力の大小から特定することができる．この作業をターゲットビットを替えて行えば，Y 全てのビットを特定することができる.

4 ビット及び 8 ビット長のデータに対してビットごとの XOR 演算を行う XOR 演算部に対して，1 ビット単位の DPA を実施した結果を図 3 に示す．入力 Y を全て”0”とし，入力 X のターゲットビット以外を LSFR による乱数入力とし，ターゲットビット”1”と”0”との平均消費電力の差分を取った．それぞれサンプル数を 4000 回と 16000 回とし，XOR 演算部後方のファンアウト数を M(=256) の倍数で M，2M，4M と変化させている.

図 3 の結果により，XOR 演算部におけるターゲットビットのみの遷移の有無によるリークが，平均消費電力の差分に表れていることが分かる．また，ファンアウト数を増大させることにより，それにほぼ比例したリークが得られ，サンプル数を増やすことにより，ノイズをより除去できていることが分かる.

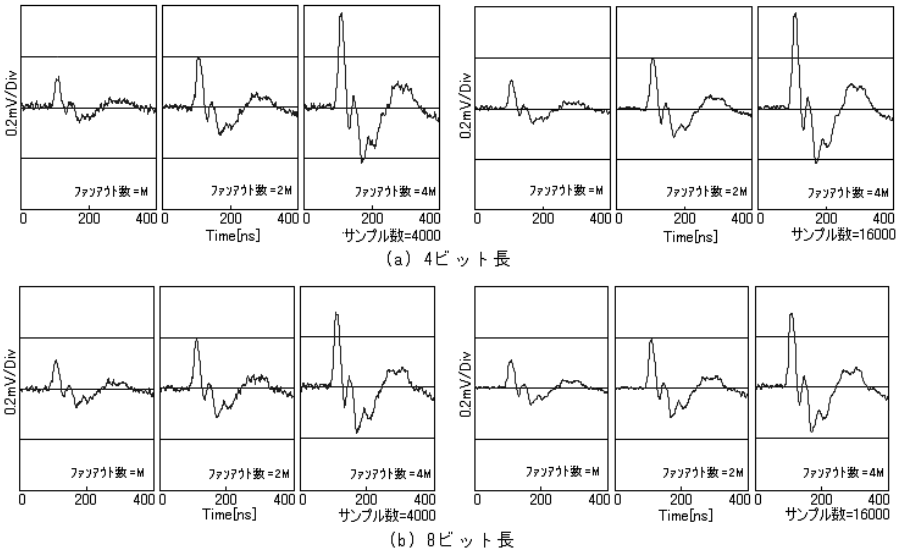
2.2　Multi-bit DPA の検証

XOR 演算は入力と演算結果がビット毎に対応していて，他のビットの影響を受けないという特性を持っている．よって一方の入力に対して，こちらがもう一方の入力を自由に設定できる場合には，各ビット毎の演算結果を意図的に制御できる.

Multi-bit DPA は，この特性を利用して，入力 Y の値を複数ビット同時に解析する手法である．入力 Y に対して，ある入力 X とそのビットを全て反転させた $\bar{X}$ とで XOR 演算させた場合，演算時におけるビット毎の遷移の有無も反転した結果を得られる．このとき入力 Y に対してその全てのビットで遷移が起こるような入力 X とで演算させた場合，演算時における消費電力は最も大きくなる．よって，入力 Y に対する入力 X と

Verification of side channel attacks against XOR operation

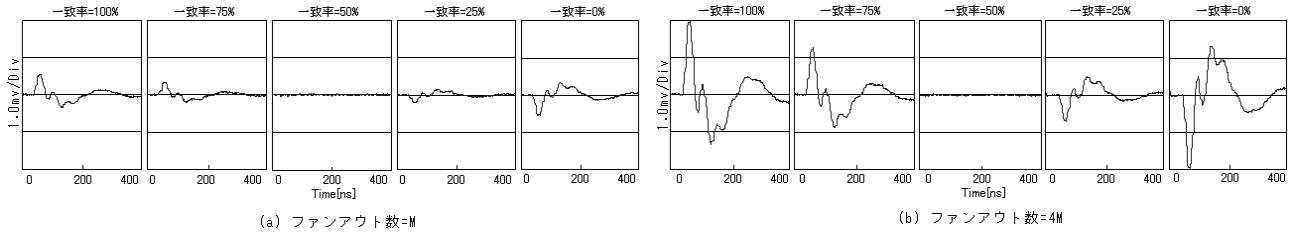
†Yohei Tsuji, Keisuke Iwai, and Takakazu Kurokawa
††National Defense Academy



(a) 4ビット長

(b) 8ビット長

図 3: 1 ビット単位での DPA 検証結果



(a) ファンアウト数=M

(b) ファンアウト数=4M

図 4: 4 ビット長に対する multi-bit DPA 検証結果

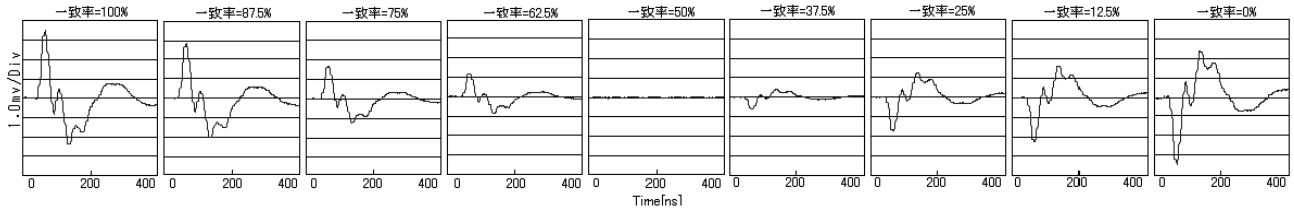


図 5: 8 ビット長に対する multi-bit DPA 検証結果 (ファンアウト数=4M)

入力 $\bar{X}$ の演算時における消費電力の差分が，一番大きくなるような X を求めることができれば，入力 Y を特定することができる．

ここでは入力 Y を全て"0"とし，ビット毎に入力 Y に対する入力 X が遷移する場合を一致するとして，全て一致した場合から全く一致しなかった場合までの 4000 サンプルの平均消費電力の差分を取って検証を行った．図 4，5 はそれぞれ 4 ビット長及び 8 ビット長の XOR 演算部に対して Multi-bit DPA を行った結果である．4 ビット長の結果では，一致率を 100%から 0%まで変化させ，それぞれファンアウト数が M と 4M の 2 通りで行った．8 ビット長の結果では，4 ビット長同様の方法でファンアウト数が 4M のものを表示してある．

図 4 及び図 5 の結果から，推定が正しい場合（一致率=100%）のときに最大の差分が現れた．逆に推定が全てのビットで間違っていた場合（一致率=0%）の場合には負の方向に最大の差分が現れた．また，Multi-bit DPA での平均消費電力の差分は，1 ビット単位での DPA で得られた結果にほぼ比例した．

3 まとめ

本稿では，XOR 演算に関する 2 種類の DPA 手法について，FPGA に実装し検証を行った．結果として様々な回路における XOR 演算部において，演算前の状態が既定の値となっているような実装をおこなっている場合は，これらの手法により DPA が可能であることが検証できた．また Multi-bit DPA を行う際には，1 ビット単位での DPA を行った平均消費電力の差分結果を基にすれば，一致率における平均消費電力の差分の予測が可能であることが判明した．

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] 桶屋勝幸:ハッシュ関数構成法を考慮した HMAC に対するサイドチャネル攻撃, 電子情報通信学会研究報告,ISEC2006-79,pp.53-60,2006.

[4] 久門亨, 角尾幸保, 後藤敏, 池永剛:ストリーム暗号に対する DPA,Symposium on Cryptography and Information Security,SCIS2006.

[5] 佐伯稔, 鈴木大輔, 市川哲也：DPA のリークモデル構築と論理シュミレーションによる評価, 電子情報通信学会研究報告,ISEC2004-57,pp.111-118,2004.

[6] 市川哲也, 鈴木大輔, 佐伯稔：データマスクを利用した DPA 対策に対する攻撃, 電子情報通信学会研究報告,ISEC2004-58,pp.119-126,2004.