L-040

ハードウェア実装されたXOR演算に対するDPA手法

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

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].

ストリーム暗号の keysetup 時等の暗号デバイスに多く用いられている XOR 演算についても,DPA 手法がいくつか提案されている [3][4][5]．しかしこれらの手法は，CPU 処理を前提としたターゲットに実装された XOR 演算に対する DPA 手法である．著者らは，ハードウェア実装された XOR 演算に適応することは難しいことを確認した [6]．一方，ハードウェア実装された暗号デバイスに対しての現在までに提案されている DPA 手法は，信号遷移時における遷移確率の偏りを利用したものである．XOR 演算は線形演算であり遷移確率に偏りがないため，これまでの手法は適応できない．

本稿では，CMOS 素子構造におけるスイッチング特性に着目した XOR 演算に対する DPA 手法を提案する．

2　CMOS 素子の消費電力

近年におけるデジタルデバイスは，そのほとんどが CMOS 素子で構成されている．図 1 に CMOS 素子のインバータ構成を示す．信号遷移が起こる際に，nMOS と pMOS ではスイッチの on/off が相補的に動く．消費電力は信号の遷移の際に出力の信号値を保持する負荷容量の充放電に加えて，貫通電流及び漏れ電流を考慮することで次式で評価できる [7].

$$P = \underbrace{p_t \cdot C_L \cdot V_{dd}^2}_{a} + \underbrace{p_t \cdot I_{sc} \cdot V_{dd} \cdot f_{clk}}_{b} + \underbrace{I_{leakage} \cdot V_{dd}}_{c} \quad (1)$$

p_t:信号の遷移確率　C_L:負荷容量　V_{dd}:電源電圧
I_{sc}:貫通電流　f_{clk}:動作周波数　$I_{leakage}$:漏れ電流

ここで a は，負荷容量の電力を充放電するために生じる消費電力であり，b は信号遷移時に nMOS と pMOS がどちらも導通することで発生する電力であり，a,b 共に信号の遷移に依存している．c は漏れ電流によるものである．

3　CMOS 素子のスイッチング特性

pMOS と nMOS の電子移動度は異なり，nMOS が pMOS の 2〜3 倍であると言われている．MOS 素子のドレイン電流はゲート幅 W と長さ L の比に比例する．通常の CMOS 回路では，pMOS 素子の W/L ゲート比

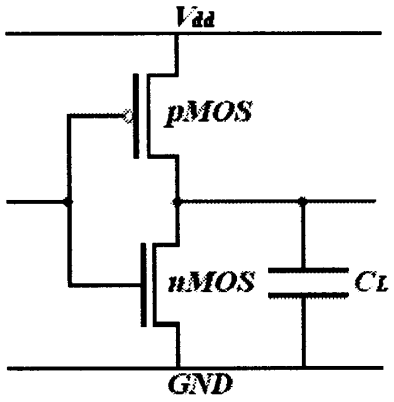

図 1: CMOS 素子によるインバータ

を約 2.5:1 とすることでスイッチ速度を均等にするような設計になっている．速度の問題を無視する場合や MOS トランジスタの占有面積を最小化したい場合には，ゲート比を同一にする場合もある [8].

前者のスイッチ速度を均等にした場合，pMOS においてゲートの幅が大きくなり上方遷移と下方遷移では貫通電流量に差が生じる可能性がある．また後者のゲート比を同一にした場合ではスイッチ速度に差が生じる．そのため CMOS 素子の場合，上方遷移と下方遷移の際に観測される消費電力を基にした DPA によって，有意なリークが発生する可能性がある．

4　提案する DPA 手法

ここでは，ターゲットデバイスの CMOS 素子における遷移時のスイッチ速度が均等であり，演算時に観測される消費電力において上方遷移の方が下方遷移より大きいことを前提とする．

式 (2) は n ビットの XOR 演算に対する DPA 攻撃モデルである．IV は公開データであり外部から制御可能とする．K は秘密データで固定値とする．X は IV と K の演算結果であり外部から観測不可能とする．

$$X = f(K, IV) \quad (2)$$

1. 波形計測

   IV を変えて演算 $f(K, IV)$ を行い，その際の電位差 V を計測する．

2. 波形の分類

   n ビットの K のうち特定目標ビット i を定め K_i とする．K_i と IV_i による演算 $X_i = f(K_i, IV_i)$ において，遷移が起こる事象を $X_{i,(T)}$ とする．さらに入力 IV_i の値により 2 パターンに分類する．

   (a) $X_{i,(IV_i=0)}$ ：IV_i が $0_{(low)}$ の集合
   (b) $X_{i,(IV_i=1)}$ ：IV_i が $1_{(high)}$ の集合

† 防衛大学校　情報工学科

3. 平均電圧波形の算出

計測した電圧波形 V をグループ分けにしたがって分類し，平均電圧波形を求める．$\#X_{i,(IV_i=0)}$ 及び $\#X_{i,(IV_i=1)}$ はそれぞれの事象の総和である．

$$V^{average}_{X_{i,(IV_i=0)}} = \frac{1}{\#X_{i,(IV_i=0)}} \sum_{X_{i,(IV_i=0)} \in X_{i,(T)}} V \quad (3a)$$

$$V^{average}_{X_{i,(IV_i=1)}} = \frac{1}{\#X_{i,(IV_i=1)}} \sum_{X_{i,(IV_i=1)} \in X_{i,(T)}} V \quad (3b)$$

4. 差分結果による判定

演算が実行された時間 t における平均電圧の差分を算出する．

$$\Delta V_i(t) = V^{average}_{X_{i,(IV_i=1)}}(t) - V^{average}_{X_{i,(IV_i=0)}}(t) \quad (4)$$

最初に述べた前提条件により，差分結果 $\Delta V(t)$ をグラフ化した際に正のスパイクが表れれば K_i=$0_{(low)}$ と特定できる．逆に負のスパイクが表れたならば，K_i=$1_{(high)}$ と特定できる．

5 DPA 手法の評価実験

5.1 実験環境

DPA 実験検証には，日本規格協会情報技術標準化研究センター (INSTAC) が策定した INSTAC-32 準拠ボードを使用した．

- FPGA: XC2V1000-5FG456
  (INSTAC-32 FPGA-BOARD)
- 回路記述言語: Verilog-HDL
- オシロスコープ: IWATU DS-4354ML
  500Msample/s

5.2 4bit XOR に対する DPA 実験方法

FPGA 上に 4bit XOR 回路を実装して，提案した DPA 手法を用いて検証を行った．なお，XOR 演算出力部の信号を保持する負荷容量を増大させる目的で，XOR 演算出力部のファンアウト数を 512 にした．電圧の測定は FPGA の GND 部にある抵抗の両端で行った．

秘密情報 K を $0101_{(2)}$ として，これを特定することを目標とした．IV を変えて演算 $f(K, IV)$ を行い，電圧波形 V を必要数取得した．ビット毎に $X_{i,(IV_i=0)}$ と $X_{i,(IV_i=1)}$ の集合に分類した．分類にしたがって平均電圧波形の差分を算出し ΔV_0〜ΔV_3 としてグラフ化した．

5.3 実験結果と考察

10 万サンプルの電圧波形を測定し，その差分結果は図 2 のようになった．どれも約 $0.2mV$ のスパイクが観測できた．K のビット値が 0 であるものでは，差分結果に正のスパイクを観測できた．一方，K のビット値が 1 であるものでは，負のスパイクが観測された．これにより，差分波形に観測されたスパイクの正負で，K の各ビット値を全て特定することができた．

本実験では，実装デバイスに FPGA(XC2V1000-5FG456) を用い，その結果 **4** で示した前提条件を基にした結論と同じ結果となった．そのため，今回用いた FPGA では，CMOS 素子のスイッチング特性上，上方遷移時において下方遷移時よりも大きな消費電力となる．

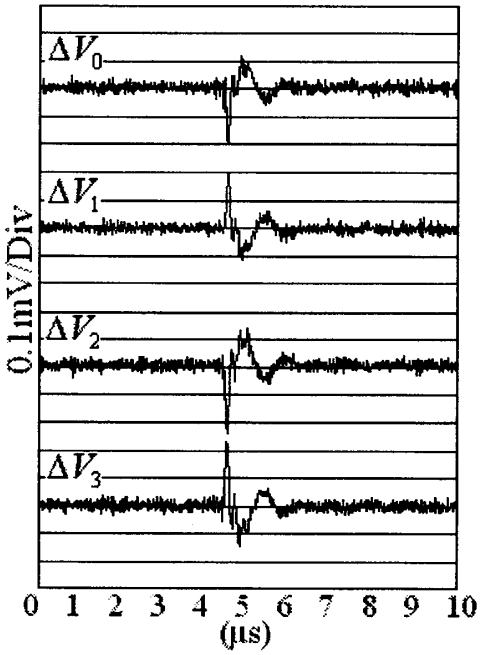

図 2: 4bit XOR に対する DPA 評価結果

6 まとめ

本稿では，ハードウェア実装された XOR 演算に対する DPA 手法を提案し，評価実験によりその有効性を確認した．冒頭でも述べたが，現在主流となっているハードウェアデバイスは CMOS 素子が大半を占めている．この素子構造の特性を利用すれば，線形演算である XOR 演算に対する DPA が可能である．

今回の評価実験は，少ないサンプル数で明確なスパイクを観測できるように，XOR 演算出力のファンアウトを増加させていた．今後はファンアウトの増加処置を行わない実装における検証及び，XOR 演算部を含む暗号デバイス全体を含めた実装検証を行い，本 DPA 手法を確立する必要がある．

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] Kerstin Lemke, Kai Schramm, Christof Paar, "DPA on n-Bit Sized Boolean and Arithmetic Operations and Its Application to IDEA, RC6, and the HMAC-Construction",CHES2004,pp.205-219.

[4] 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.

[5] 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,SCIS2006.

[6] 辻洋平, 岩井啓輔, 黒川恭一,XOR 演算を対象にしたサイドチャネル攻撃手法の検証, 情報処理学会第 69 回全国大会,2006.

[7] 佐伯稔, 鈴木大輔, 市川哲也 : CMOS 論理回路の電力解析モデル,SCIS2005.

[8] 菅野卓雄, 桜井貴康,MOS LSI 設計入門,1984.