M_051

MRSLによるS-BOXへのDPA対策効果の検証

Verification of effectiveness of Modified RSL against DPA for S-BOX

佐々木 稔† 岩井 啓輔† 黒川 恭一†
Minoru Sasaki Keisuke Iwai Takakazu Kurokawa

1 はじめに

電力差分解析 (Differential Power Analysis, DPA)[1] とは暗号回路における内部変数の遷移確率に着目し、測定した消費電力を統計的に処理することで、秘密鍵を推定するサイドチャネル攻撃の一種である。

DPA 対策として、CMOS ゲートの遷移確率に着目した RSL(Random Switching Logic)[2] が提案されているが、RSL の実装には許可信号 (Enable signal) の生成及び詳細なタイミングの管理を行う回路が必要になる。

本発表では、許可信号を用いずに伝播遅延に伴うスパイクの発生を防止できる方式として MRSL(Modified RSL) を提案する。RSL と比較して、許可信号を必要としないため、MRSL の実装は容易となり、実装後の回路規模も削減できる。これらの事実を確認するため、MRSL を FPGA 上に実装し、DPA 対策としての有効性と回路規模の検証を行った結果を示す。

2 共通鍵暗号における DPA 対策

共通鍵暗号（ブロック方式）で用いられる S-BOX は非線形関数である。CMOS 回路における消費電力は単位時間当たりの信号遷移確率に比例するので、S-BOX のような非線形関数では、その出力値と消費電力の間に相関が生じる。内部情報が消費電力に漏洩しないように消費電力を均一化する方法が主要な DPA 対策である。

2.1 ランダムマスク方式による DPA 対策

共通鍵暗号の DPA 対策の一つとしてランダムマスク方式がある。この方法は非線形関数の入出力を乱数と XOR することで、遷移確率を乱数の確率に帰着させるものである。Messerges[3],Trichina[4], 清水 [5] らによってそれぞれのマスク方式が提案されてきたが、これらの方式は信号が遅延しないことを前提に設計されているため、伝播遅延によってスパイクが顕著に現れる。しかも、スパイクの確率が均一化されていないため、結果的に消費電力に差が生じ DPA が可能になる。

2.2 RSL による DPA 対策

伝播遅延を考慮したランダムマスク方式として、鈴木らによって RSL が提案された [2]。図 1 及び表 1 に示すように入力信号 (a,b) 及びマスク乱数値 (r) が到達してから十分後に許可信号 (en) を入力することで、伝播遅延に起因するスパイクを防止することができる。

しかし、RSL を多段構成する場合、複数の許可信号を生成、管理しなければならない。細粒度パイプラインを用いて高速性を追求する場合、非同期設計等により

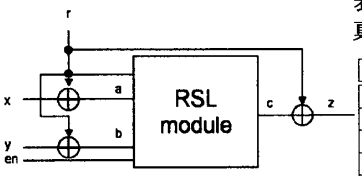

図 1: RSL モジュール図

表 1: RSL-NAND の真理値表 (en = 1 のとき)

x	y	r	a	b	c	z
0	0	0	0	0	1	1
0	0	1	1	1	0	1
0	1	0	0	1	1	1
0	1	1	1	0	0	1
1	0	0	1	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	0	0	1	0

許可信号のタイミングを厳密に管理する必要が生じる。また通常の粗粒度パイプラインで構成する場合、RSL の段数だけクロックサイクルが必要になるので、レイテンシによってスループットが悪化することが考えられる。このように RSL の実装には許可信号のタイミングの管理と、許可信号を生成・制御するハードウェア回路が必要になる。

3 MRSL

3.1 基本 MRSL ゲート

本研究では RSL の改良版として、許可信号を必要としない MRSL(Modified RSL) を提案する。許可信号による遅延制御の代わりに、ゲートに入力値と乱数値を与える前に必ず初期化させることで、スパイクを生じさせない方法である。初期値から任意の値へ遷移する過程では、MRSL の静的ハザードを防止することができる。表 1 の 2 入力 1 出力 RSL-NAND の真理値表をそのまま MRSL の真理値表とした場合、図 2 に示すように初期値 (a,b,r)=(0,0,0) または (1,1,1) から任意の値への遷移においてスパイクは生じない。

また 4 入力 1 出力の LUT 形式の FPGA に実装する場合、RSL の許可信号の代わりに入力を追加すれば、図 3 に示すような 3 入力 1 出力 MRSL-NAND ゲートを構成することができる。LUT に実装する場合、2 入力 RSL よりも 3 入力 MRSL を用いた方が、ハードウェア量を削減することができる。

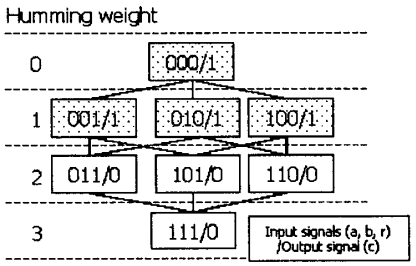

図 2: 2 入力 MRSL-NAND ゲートの遷移図

† 防衛大学校 情報工学科

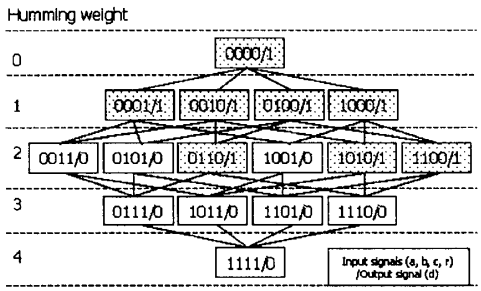

図 3: 3入力 MRSL-NAND ゲートの遷移図

3.2 多入力 MRSL ゲート

1 LUT におさまらない多入力 MRSL-AND(NAND) の構成方法を説明する。図4 (a) のように、多入力 MRSL-AND は、MRSL-AND のみで多段構成できる。一方多入力 MRSL-NAND は、図中 (b) のように最終段のみ MRSL-NAND として、それ以前の段は MRSL-AND で構成できる。両者共、全段の MRSL に同じ乱数値を使用できる。しかも乱数値が各基本 MRSL に任意のタイミングで到達しても、初期値から開始されればスパイクは発生しない。

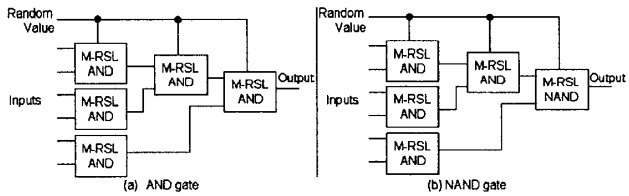

図 4: 多入力 MRSL-AND(NAND) ゲート

3.3 積和回路

前述の多入力 MRSL-NAND を用いた図5のような NAND の2段構成によって、多入力1出力の積和回路を構成することができる。1段目の多入力 MRSL-NAND 群と2段目の多入力 MRSL-NAND の初期値を (入力の初期値, 乱数の初期値)=(Xn, r1) 及び (Yn, r2) とする。Xn を全て 0 で初期化するとき、r1 も 0 にしなければならない。このとき1段目の NAND の出力である Yn は全て1となるため、r2 を1とすることによって初期化できる。逆に (Xn,r1) を全て1とした場合、r2 を 0 とすることで初期化できる。1段目と2段目の乱数値の初期値が異なっても、初期値から遷移を始める条件に反さない限りスパイクは生じない。初期化後は、両段ともに同一のマスク乱数値を使用して積和演算ができる。

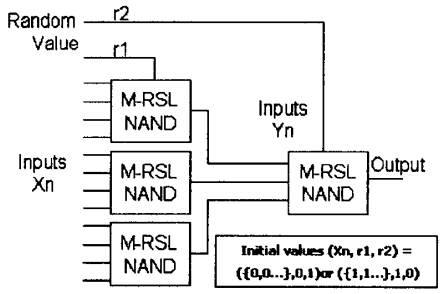

図 5: MRSL-NAND による積和回路

4 実験結果

本研究では MRSL-NAND を用いた積和回路で構成した DES の S-BOX1 を FPGA 上に実装し、8 万回の消費電力を計測して平均を求め、DPA 対策の効果を評価、検証した。三菱電機が開発したサイドチャネルアタック評価用プラットホーム (SCAPE) を用い、対象回路は SCAPE に搭載されている Xilinx の FPGA(Virtex1000) に実装した。SCAPE の電源は外部電源 5V のみ使用した。回路の設計等は Xilinx の ISE8.1i を使用し、測定には IWATSU のデジタルオシロスコープ DS-4354ML を使用した。

図6に DPA の結果を示す。上から順に無対策回路、粗粒度パイプラインで実装した RSL、3．1節で示した2入力基本 MRSL のみでの実装、及び3入力 MRSL での実装の測定結果である。無対策回路では DPA のピークが確認できるのに対して、MRSL は RSL と同等の DPA 耐性を持つ。また許可信号の制御回路の削減と3入力 MRSL の適用により、RSL と比較してハードウェア量が大幅に削減できた。

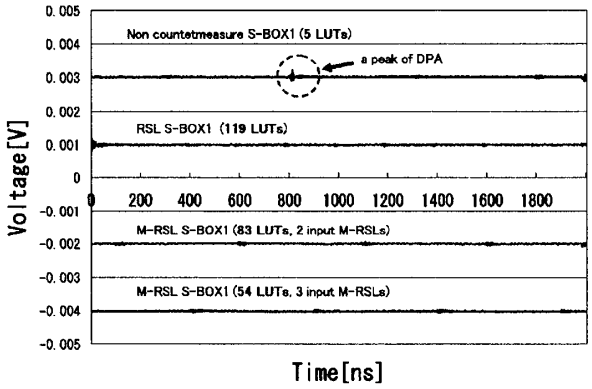

図 6: DPA 波形の比較結果

5 まとめ

本研究では伝播遅延によるスパイクを防止するために初期化をする MRSL という方法を提案した。ブロック暗号は処理に数クロックを用いるため、S-BOX 内の MRSL の初期化を安易に行うことが可能である。今回の実験結果によって、RSL と同等の DPA 耐性と RSL よりハードウェア量を節減できることを確認できた。

今後の課題として、1st order DPA だけではなく高次 DPA や標準偏差 DPA などの耐性を検証することがあげられる。

参考文献

[1] P.Kocher, J.Jaffe, B.Jun, “Differential power analysis”, Advances in Cryptology - CRYPTO ’99, vol.1666 of Lecture Notes in Computer Science, pp.388-397, Springer-Verlag, 1999.

[2] 鈴木 大輔, 佐伯 稔, 市川 哲也：遷移確率を考慮したＤＰＡ対策手法の提案, 電子情報通信学会技術研究報告, ISEC2004, Vol.104, No.200, pp.127-134, 2004.7.

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

[4] E.Trichina, “Combinational logic design for AES subbyte transformation on masked data,” ePrint2003/236, 2003.

[5] 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.