社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2004－ＣＳＥＣ－26 (47)
2004／7／21

遷移確率を考慮したDPA対策手法の提案

鈴木 大輔† 佐伯 稔† 市川 哲也‡

† 三菱電機株式会社 情報技術総合研究所 〒247-8501 神奈川県鎌倉市大船 5-1-1
‡ 三菱電機エンジニアリング株式会社 鎌倉事業所 〒247-8501 神奈川県鎌倉市大船 5-1-1
E-mail: † {dice, rebecca}@iss.isl.melco.co.jp, ‡ ichikawa@kam.mee.co.jp

あらまし 本稿では，従来のロジックレベルにおけるDPA対策手法である2線式対策手法の問題点を指摘し，1線式による新たなDPA対策手法を提案する．提案する対策手法はCMOS回路で実現可能であり，ゲート毎の信号遷移を均等化し，過渡遷移の伝搬を抑えることで，予測可能なデータに依存しない電力消費を実現することが可能である．また，提案する対策手法の効果を確認するためにFPGAを用いてモデル化を行い，実装評価及びDPAにおけるリークに対する評価を行った．その結果，従来の対策手法と比較して安全性，実装効率，実現性の面で優れた結果が得られた．

キーワード DPA，対策，遷移確率，CMOS回路，ASIC，FPGA

Countermeasure against DPA Considering Transition Probabilities

Daisuke SUZUKI† Minoru SAEKI† and Tetsuya ICHIKAWA‡

† Mitsubishi Electric Corporation, Information Technology R&D Center,
5-1-1 Ofuna Kamakura, Kanagawa, 247-8501, Japan
‡ Mitsubishi Electric Engineering Company Limited, Kamakura Office,
5-1-1 Ofuna, Kamakura, Kanagawa, 247-8501, Japan
E-mail: † {dice, rebecca}@iss.isl.melco.co.jp, ‡ ichikawa@kam.mee.co.jp

Abstract In this paper, we point out the problem of the countermeasure against DPA using dual-rail circuit, and propose a new countermeasure on single-rail circuit. Our countermeasure can be constructed using CMOS circuit and achieve the power consumption that doesn't depend on predictable data equalizing the transition of each gate and suppressing dynamic hazards. Moreover, by modeling that uses FPGA, we show that the proposed method can efficiently achieve security against DPA compared with a past method.

Keyword DPA, Countermeasure, Transition Probability, CMOS Circuit, ASIC, FPGA

1. はじめに

1999年にKocherらによって提案されたSPA(Single Power Analysis),DPA(Differential Power Analysis)は，スマートカード等の暗号化デバイスに格納されている秘密情報を，その消費電力から推定する強力な攻撃法である[8][9]．この提案をきっかけに，それまで差分解読法や線形解読法等の暗号アルゴリズム自体の強度評価に加えて，いわゆるサイドチャネル攻撃と呼ばれる，暗号デバイスの処理中に発生する二次的な情報からの秘密情報のリークに対する評価が注目されている．

一方，サイドチャネル攻撃への対策手法も盛んに研究されており，特にDPAに対しては，様々な対策手法が提案されている．これらの対策手法は以下の2つに大別できる．

i) アルゴリズムの改良による対策
ii) 演算器や演算素子の改良による対策

例えば，公開鍵暗号系の処理に対する様々な対策手法[16][17][18]や，乱数によるデータマスクを用いた共通鍵暗号系の対策手法[5][11][15]はi)に類する．また，文献[5]のデータマスクを組み合わせ回路で実現した方式[4]や，DCVSL(Differential Cascode Voltage Switch Logic)を応用したSABL(Sense Amplifier Based Logic)[1][2]及び，CMOS回路で同一機能を実現したSDDL(Simple Dynamic Differential Logic)，WDDL(Wave Dynamic Differential Logic)[3]はii)に類別される．

ii)に類別される対策は，DPAにおけるリークを発生源から絶つことができるため，汎用性が高く，効率のよい対策が実現可能であると考えられる．

ここで注意すべき点は，各対策手法の安全性は，ある実装上の条件を満たすときのみに保証されることである．例えば，乱数によるデータマスクはその安全性が乱数値や乱数性に依存することが知られている[5]．

また，著者らは文献[26]で，データマスクを組み合わせ回路で実現した対策は，ある特定のタイミング条件を満たすときにのみ，リークレスな回路が実現されることを示している．つまり，対策手法はその方式に加え，実装上の条件とその実現性を明確にする必要がある．

本稿では，DPA におけるリークの発生が演算素子の遷移確率の偏りに起因することから[25]，これを根本的に絶つべく，演算素子のレベルでの対策手法を提案する．提案する対策手法は，従来の ii)に類別される手法と比較して，実装上の条件が緩和でき実現性が高い．また，演算素子のレベルでリークの発生を防ぐため，どのような暗号アルゴリズムに対しても適応可能である．

以下，まず 2 章ではこれまでに提案されている演算器や演算素子のレベルでの DPA 対策手法について紹介する．3 章では，DPA におけるリークモデルを示し，そのモデルから導かれる従来手法の実装上の条件と，その実現性について述べる．続けて 4 章では，本稿で提案する DPA 対策手法である Random Switching Logic(RSL)とその実装上の条件及び，RSL を用いた暗号回路全体の設計方式について述べる．5 章では，FPGA を用いた RSL のモデリングによる実装結果，及び DPA 評価結果を示し，最後に 6 章でまとめを行う．

2. 関連研究

著者らの知る限り，演算器や演算素子に DPA 対策を行うアプローチには 2 通りの方法がある．1 つは，アルゴリズムの改良による対策を，CMOS ゲートの組み合わせ回路まで落とし込む手法であり，文献[4]の対策手法がこれにあたる．もう 1 つは，独自の演算素子を構成し，それ自体に対策効果を盛り込む手法であり，例として文献[1][2]の SABL や文献[3]の SDDL,WDDL 等の手法が挙げられる．

マイクロプロセッサや暗号コプロセッサの多くは CMOS プロセスで製造されている．よって CMOS 回路の基本演算素子への DPA 対策は，消費電力に係わる最小単位での対策となるため，安全性，汎用性の面で他の手法に勝ると考えられる．よって本稿では，CMOS ゲートの改良を行うことで．DPA 対策を行うアプローチを採る．

Tiri らは DPA 対策として DCVSL を応用した SABL を提案している[1]．図 1 に SABL による AND-NAND ゲートの基本構造を示す．このゲートは，スタティック型 CMOS ゲートにはない，以下のような特徴をもつ．

① 相補的な出力が存在する．
② (0,0)を出力する休止相と(0,1)もしくは(1,0)を出力する稼動相をプリチャージにより制御できるため，2 線 2 相式回路の実装に応用できる．
③ 各状態遷移に対して消費電力が一定になる
④ 入力信号の遅延に依存せずに，1 回だけ状態遷移が発生する．

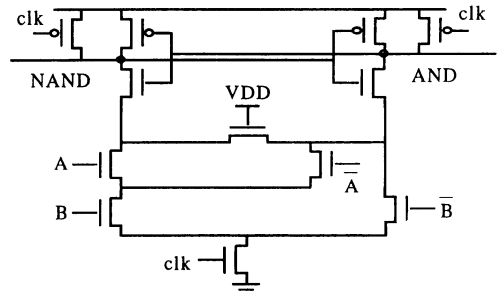


図1 SABLによるAND-NANDゲート

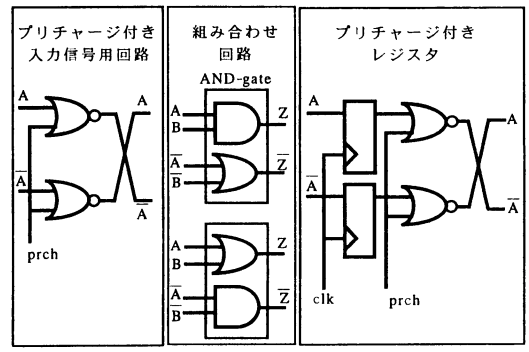


図 2 WDDL の基本演算素子

③及び④からわかるように，SABL は信号値に依存せず一定の消費電力となるため，DPA 対策として有効である．一方で，SABL は一般的なスタティック型 CMOS ライブラリには存在しない回路であるため，既存の設計環境に適合しないという問題点があった．そこで，Tiri らは，スタティック型 CMOS を用いた SABL と同機能をもつ SDDL，及びプリチャージ機能を最適化した WDDL を提案している[3]．図 2 に WDDL の基本構成図を示す．WDDL はプリチャージを組み合わせ回路の初段で行い，かつ使用するゲートを AND, OR, NOT に限定して回路を構成することで，①から④までの機能を実現している．また，FPGA 上で WDDL を実装する方式についても提案されている[3]．

これらの 2 線式回路を用いた DPA 対策は，その安全性を保証するためには以下のような条件が必要となる．

- 相補的な動作をするゲートは同じタイミングで動作する．
- 相補的な入出力間における配線容量が同じになる．

これらの条件は，回路の配置配線時に最適化が必要であることを意味し，一般的なレイアウトツールを用いた場合，通常は対応できない．以下本稿では，状態

遷移に基づいたリークモデルから，これらの条件の正当性を導き，相補動作を必要としない新たな DPA 対策手法を提案する．

3. DPA におけるリークモデル

本章では，著者らが文献[25]で提案した CMOS 回路における状態遷移に基づく DPA のリークモデルについて紹介する．

3.1. リークモデル

CMOS 回路の消費電力は,一般に式(1)で評価できる[20][21][22][27].

$$P_{total} = p_t(1/2 \cdot C_L \cdot {V_{dd}}^2 \cdot f_{clk} + I_{sc} \cdot V_{dd} \cdot f_{clk}) + I_{leakage} \cdot V_{dd} \quad (1)$$

ここで，C_Lは負荷容量,f_{clk}は周波数,V_{dd}は電源電圧，p_t は信号の遷移率,I_{sc} は貫通電流,$I_{leakage}$ は漏れ電流である．式(1)からわかるように，DPA で観測される"データに依存した消費電力差"は p_t が要因となり発生する[25].

ここで，DPA 攻撃者が入力データの場合分けに用いる,ある 1bit の信号 x に関連する回路について考える．この回路が，1 サイクルの間に信号遷移が発生する可能性のある,全ての事象の集合を E とする．このとき，x の値に依存する総遷移回数の期待値 N は，以下の式で表される[25].

$$N_{x=0} = \sum_{e \in E} \sum_{i=1}^{m} \sum_{j=1}^{n_i} (p_{0(i,j)}(e) \cdot (\sum_{j=k}^{n_i} \prod_{l=j}^{k} \beta_{(i,l)}(e))) \quad (2)$$

$$N_{x=1} = \sum_{e \in E} \sum_{i=1}^{m} \sum_{j=1}^{n_i} (p_{1(i,j)}(e) \cdot (\sum_{j=k}^{n_i} \prod_{l=j}^{k} \beta_{(i,l)}(e))) \quad (3)$$

ここで，m は x に関するレジスタ間の経路数，n_i は i 番目の経路におけるゲート段数，$p_{0(i,j)}$, $p_{1(i,j)}$,は x の値に応じた経路 i の j 段目における遷移回数の期待値，$\beta_{(i,j)}$ は $p_{0(i,j)}$と $p_{1(i,j)}$の遷移に対する伝搬係数,$N_{x=0}$,$N_{x=1}$ はそれぞれ x の値による回路全体における総遷移回数の期待値である．$p_{0(i,j)}$, $p_{1(i,j)}$, $\beta_{(i,j)}$,は事象 e と無関係であれば 0 で，そうなでければ何らかの値を持つことになる．式(2),(3)から，x の値に依存した総遷移回数の期待値の差は

$$N_{diff} = N_{x=1} - N_{x=0} \quad (4)$$

となり，$N_{diff} \neq 0$であれば，(1)式からデータ x の値によって消費電力差が発生することになり，DPA で解析される可能性があると言える．

3.2. 2 線式対策法の安全性

本節では，3.1 節で示したリークモデルを基に SABL,SDDL,WDDL に代表される 2 線式対策法の安全性について議論する．これらの対策手法で提案されている回路では，その構成上，過渡遷移が発生しない[1][2][3]．よって，(2),(3)の $\beta_{(i,l)}$ は $l = j$ のとき 1 で，それ以外では全て 0 として評価できる．従って，x の値に依存する総遷移回数の期待値は，

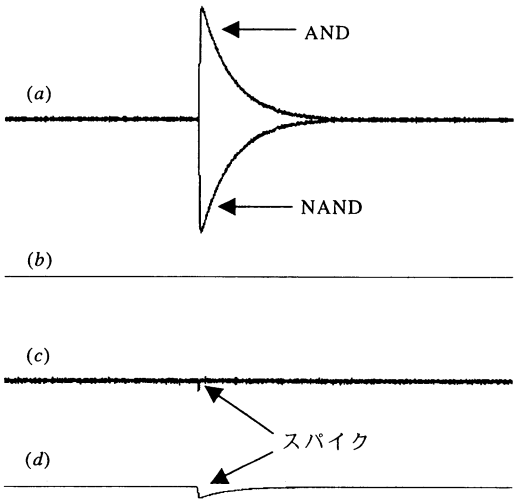


図 3　2 線式対策手法のリークモデル
(a)は 2AND ゲート(上図),2NAND ゲート(下図)のリーク(実測値)．(b),(c),(d)はそれぞれ，(a)から予測される,(b)2 つの波形の位相と大きさが等しい場合,(c)位相にずれがある場合,(d)配線容量が異なる場合 のリークモデル．

$$N_{x=0} = \sum_{e \in E} \sum_{i=1}^{m} \sum_{j=1}^{n_i} p_{0(i,j)}(e) \quad (5)$$

$$N_{x=1} = \sum_{e \in E} \sum_{i=1}^{m} \sum_{j=1}^{n_i} p_{1(i,j)}(e) \quad (6)$$

となる．つまりこれは，x に関する論理関数が持つ，各ゲートの過渡遷移に依存しない遷移回数の期待値のみで，回路全体の信号遷移回数を評価できることを意味する．ここで，2 線式対策手法における AND(または OR)ゲートは，全て相補的な動作を行う回路を合わせ持つ．よって，2 線式対策手法による 2 入力 AND ゲートにおける遷移回数の期待値の差 n_{diff}^{2AND} は，

$$\begin{aligned} n_{x=0}^{2AND} &= p_{0(AND)}(e_{AND}) + p_{0(NAND)}(e_{NAND}) \\ &= p_{0(NAND)}(e_{NAND}) \\ &= 1(e_{NAND}) \\ n_{x=1}^{2AND} &= p_{1(AND)}(e_{AND}) + p_{1(NAND)}(e_{NAND}) \\ &= 1/2(e_{AND}) + 1/2(e_{NAND}) \\ n_{diff}^{2AND} &= n_{x=1}^{2AND} - n_{x=0}^{2AND} = 1/2(e_{AND}) - 1/2(e_{NAND}) \end{aligned}$$

となる．これより，e_{AND} と e_{NAND} が同じタイミングで発生すれば，$n_{diff}^{2AND} = 0$となるが，タイミングが異なる場合，図 3(c)に示すような，e_{AND} による電力波形と e_{NAND} による電力波形に対して位相をずらした電力差

分波形に類似したスパイクが発生すると考えられる．また，AND と NAND に関する配線容量が異なれば，遷移回数の期待値が等しくても式(1)における p_i の係数項が異なることになるので，図 3(*d*)のような電力差分波形が現れる可能性もある．但し，SABL や SDDL に関しては，プリチャージのタイミングを制御することで，位相差の問題は解決できる．しかしながら，配線容量の問題，及び WDDL における位相差の問題は，レイアウトの最適化により解決する必要がある．

4. 提案する DPA 対策方式

既存の対策手法で配線等が問題となるのは，相補動作により信号遷移回数を均等化していることに起因する．ここでは，相補動作を必要としない新しい DPA 対策手法を提案する．

4.1. Random Switching Logic

まず，3 章で述べたリークモデルから，CMOS による 1 線式回路が DPA に対して安全であるための条件を示する．

補題 1 DPA に対して安全な 1 線式 CMOS 回路

秘密情報が含まれる，予測可能な中間値全体の集合を X する．そして，$^{\forall}x \in X$ に関連する回路について，1 サイクルの間に信号遷移が発生する可能性がある，事象全体を E_x とする．

このとき x に関連する 1 線式回路は，

「$^{\forall}e_x \in E_x$ の観測に対し，各ゲートの遷移回数の期待値 $p_{(i,j)}$ が x の値に依存せず，一定となる」

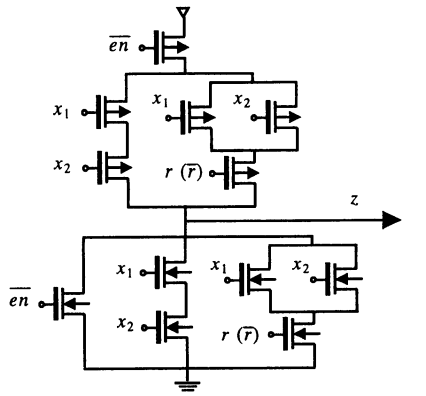
とき DPA に対して安全である．

x の値に依存せず，$p_{(i,j)}$ が一定であれば，(2),(3)式から明らかに $N_{diff} = 0$ を満たす．また，1 線式であれば位相差や配線容量差の問題は発生しない．よって DPA に対して安全となり，補題 1 が成立する．しかし，一般に NAND, NOR に代表される CMOS の基本ゲートは，補題 1 を満たさない[25]．そこで，図 4 に示すような乱数成分をゲート内で同時に処理する Random Switching Logic(RSL)を提案する．図 4(*a*)は RSL による 2 入力 NAND(NOR)ゲートであり図 4(*b*)は 2 入力 XOR 回路である．RSL は以下 2 つの性質を持つ．

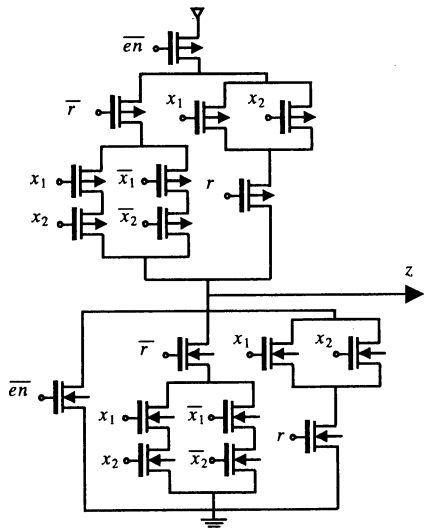
性質 1　全ての入出力に同一の乱数を用いたマスク処理を行う．

性質 2　許可信号(*en*)が 1 の時に処理を実行し，0 の時は常に 0 を出力する．

性質 1 は定常的な信号遷移回数の期待値を乱数の変化率に帰着させる．図 5 に示すように，許可信号(*en*)



(*a*)



(*b*)

図 4(*a*) RSL-NAND(NOR)ゲート
(*b*) RSL-XOR ゲート

RST-NAND: $z = \left(\overline{(x_1 \oplus r)\cdot(x_2 \oplus r)} \oplus r\right)\cdot en$

RST-NOR: $z = \left(\overline{(x_1 \oplus r)+(x_2 \oplus r)} \oplus r\right)\cdot en$

RST-XOR: $z = (x_1 \oplus x_2 \oplus r)\cdot en$

が論理 1 のとき，x_1,x_2,r の信号が同時に変化すると過程すると，攻撃者や予測可能な信号(a,b)の値に依存せず信号遷移回数の期待値は 1/2 となる．しかしながら，乱数によるマスクは過渡遷移において乱数に依存しない遷移が発生する可能性がある[26]．そこで性質 2 を用いて，入力信号(x_1,x_2,r)の変化タイミングより十分遅れて，許可信号(*en*)を論理 1 にすることで過渡遷移の発生を防ぐことが可能となる．これにより補題 1 が満たされるため，RSL では DPA に対して安全な回路を構成することができる．

a_1	a_2	x_1	x_2	r	z
0	0	0	0	0	1
0	0	1	1	1	0
0	1	0	1	0	1
0	1	1	0	1	0
1	0	1	0	0	1
1	0	0	1	1	0
1	1	1	1	0	0
1	1	0	0	1	1

$x_1 = a_1 \oplus r$

$x_2 = a_2 \oplus r$

$p_{a_1=0} = p_{a_1=1}$
$= 1/2 \cdot 1/2 + 1/2 \cdot 1/2$
$= 1/2$

a_1, a_2 は予測可能な中間値．x_1, x_2 は乱数 r によりマスクされた中間値．

図 5　RSL-NAND の真理値表と遷移確率

図 4 の他にも，性質 1，2 を満たすような，様々な機能に対応した複合ゲートを構成することも可能である．また XOR については，奇数入力の場合，入力信号が既にマスクされているならば，許可信号のみを備えた回路で処理できる．

以上のことから，RSL が DPA に対して安全に動作する条件は

- 乱数 r の遷移に偏りがない．
- 許可信号(en)が他の入力信号より遅れて変化する．

となる．

図 6 に RSL を用いた暗号回路全体の構成例を示す．平文(暗号文)もしくは 1 サイクル毎に発生する中間値は，データパスを構成する回路に入力される前に正論理と負論理が 1bit の乱数によりランダムに選択される．この乱数は，サイクル毎に更新するものとし，その更新と前サイクルで使用した乱数に対するアンマスクは同時に行う．その後，図中左から入力される制御信号に合わせて,ドミノ回路[26]のような動作で信号が伝搬していく．このとき，前段の信号遷移にばらつきがあっても，後段で過渡遷移が発生しないように TC_i (Timing Controller)で信号 en_i を制御する．最終的な演算結果は，データパスの最終段で暗号文(平文)を出力するときのみアンマスクを行う．但し，図 6 のような回路構成の場合，2 線 2 相式回路の休止相にあたる制御信号の初期化のためのオーバーヘッドが大きい．これには，細粒度パイプライン手法[24]を適応し，RSL 間にラッチを挿入することで，高速化することが可能である．

4.2. FPGA 上での RSL の実現

ここでは，4.1 節で述べた議論を FPGA に対する実装へ応用することを考える．図 7 は FPGA の LUT(Look Up Table)を用いて RSL による等価回路を実装した例である．以下 RSL を LUT で実現した回路を RSLUT と呼ぶことにする．RSLUT は図 7 に示すように少なくとも演算を行うために 4 本の入力線が必要である．一方，

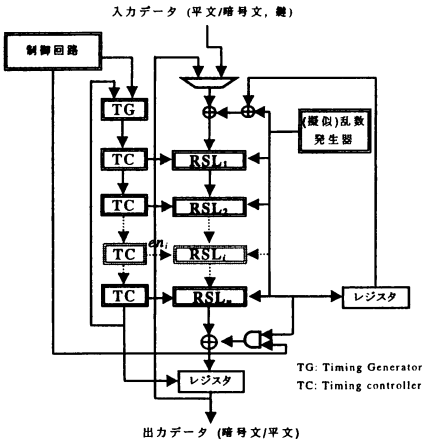


図 6　RSL を用いた暗号回路の全体構成例

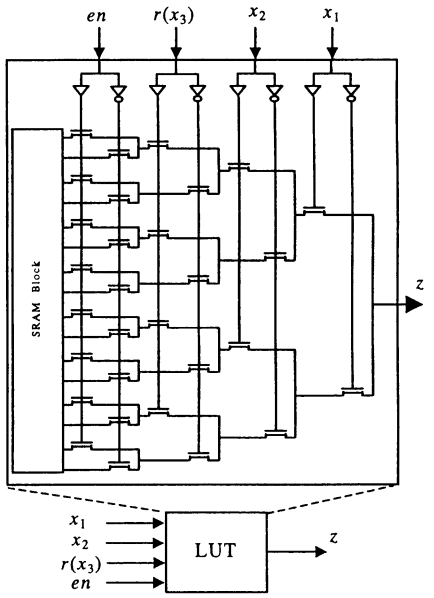


図 7　RSLUT の基本構成図

現在市場に存在する FPGA の多くは，4 入力 1 出力の SRAM ベースの LUT で構成されている．よって著者らの知る限り，ほとんど全ての FPGA で RSLUT は実現可能である．FPGA の消費電力は回路面積の大半を占めるスイッチングマトリクスが支配的となる．つまり，LUT の入出力における遷移確率がデータに依存しなければ，LUT 間をつなぐスイッチングマトリクス内の CMOS インバータの遷移確率も均等化されるため，DPA 対策として有効である．逆にこれは，RSL の実現は LUT 内で閉じて実装しなければならないことを意

味する．このとき，4入力1出力のLUTで実現可能なRSLは2入力NAND(NOR)または3入力XORまでとなる．これは，4.1節で述べたように，XORの場合は奇数入力であれば乱数用の入力線が必要ないためである．

5. 実装結果と考察

FPGAへの実装は，リークモデルの正当性や対策手法の考え方を容易に評価する有効な手段の一つである．以下本章では，AESを実装したFPGAに対する実機による実験結果について示す．評価環境は表1に示すような，一般的なものを用いた．実装ターゲットとしては，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フォーム（SCAPE：Side Channel Attack Platform for Evaluation）を用いて行った．評価に用いたSCAPEボードは，子基盤にXilinx社製のFPGAであるXCV1000-6-BG560Cが搭載されてものを使用した．

表1　評価環境

[設計環境]	
開発言語：	Verilog-HDL
シミュレータ：	Verilog-XL
論理合成：	Synplify version 7.3.4
配置配線と性能評価：	ISE version 6.1.03i
[測定環境]	
実装ターゲット：	SCAPE(XCV1000-6-BG560C)
オシロスコープ：	Tektronix TDS 7104

*電源-FPGA間に挿入した10Ω抵抗の電位差を測定

5.1. S-boxの実験結果

まず我々は，リーク発生の原因となるS-boxについて次の4通りの実装方式で評価を行った．ここで，S-boxの基本アーキテクチャには文献[13]の手法を用いた．

(a) 対策なし
(b) Masked-And[4][26]
(c) WDDL[3]
(d) RSLUT

(a)から(d)は全て自動配置配線によりレイアウトを行った．但し，論理合成については，(b),(c),(d)のそれぞれの提案で，論理合成上の制約があるため，合成ツールのattributeを利用して制御した．

図8は各対策手法に対する電力差分波形の一部である．DPAの選択関数としては，S-boxの設計に合成体を利用した際に必要な，ガロア体上の乗算への入力のある1bitを用いた[26]．図から(a)，(b)は，明らかなスパイクが観測されることがわかる．一方，(c),(d)については一見リークらしきスパイクは発生しない．しかしながら，図8(c)の電力差分波形は3.2節での考察による図3(c)に酷似した波形であることがわかる．つまりこれは，WDDLの場合，自動配置配線では位相差によるリークが発生する可能性があることを意味する．スパイクの位相が(a),(b)と異なる理由は，クロック間

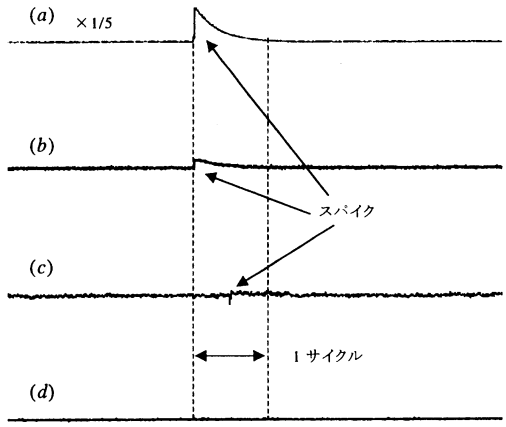


図8　各対策手法のDPA評価結果(AES-Sbox)
(6万サンプル)

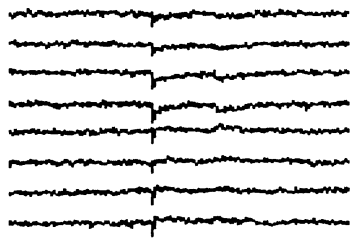


図9　WDDLの電力差分波形(60000サンプル)

の前半は休止相であり，後半でプリチャージ信号が論理0になったタイミングで，ANDやNANDの処理が行われるためである．このスパイクがリークであるもう一つの根拠として，図9のように全てのガロア体上の乗算への入力でも同じタイミングでスパイクが発生していることを挙げる．一方，RSLUTによる対策では，図8(d)からわかるように，スパイクらしき波形は発生しないことがわかる．

5.2. AESの実験結果

次に我々は，RSLUTを用いたAES全体を図6の回路構成をベースに設計を行い，そのDPAのリークを評価した．AES全体の基本アーキテクチャは文献[12]で提案されている構成で設計を行った．またS-boxについては，5.1節で評価した回路と同じ構成とした．

DPAの評価結果を図10に示す．図10は5.1節で述べた選択関数と正解鍵を用いて場合分けした電力差分波形の一例である．乱数値としてはFPGA内部に構成したM系列となるLFSRから，処理開始毎にレジスタ値をサンプリングした値を使用している．図からわかるように，どのビットについてもリークらしきスパイクが存在しない．よって，RSLUTはFPGAでのDPA対策として十分機能していることがわかる．

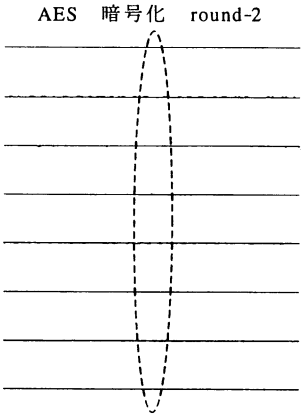


図 10 RSLUT による AES 実装の DPA 評価結果 (20 万サンプル)

5.3. 実装コストの比較

ここでは各対策手法を実現するための実装コストについて，AES の S-box に対する実装結果を元に議論する．

表 2 に各対策手法による回路面積及び最大回路遅延を示す．対策手法の中では，RSLUT が最も回路面積が小さい．Masked-And については AND 処理毎に乱数成分をキャンセルし，かつ新たな乱数でマスクする処理を行う．また，線形変換は乱数に対しても行う必要がある．WDDL については，全ての論理で相補動作を行い，かつ AND，OR，NOT のみで回路を構成する必要があるため，XOR 処理で回路面積が増大する傾向にある．一方，RSLUT は LUT 毎に制御信号を用いて AND 処理を行う必要があるが，回路全体で乱数は 1bit のみであるため，乱数値を制御する回路が不要である．また，XOR 処理も LUT1 つあたり，3 入力 XOR まで可能であるため，面積のオーバーヘッドは小さい．

回路遅延についても，各対策手法の中で RSLUT による対策は最小になるという結果が得られたが，WDDL と RSLUT は休止相にあたる初期化処理が必要であるため，同期的に処理した場合，回路遅延のおよそ 2 倍の処理時間が必要となる．4.1 節で述べたように，この問題は非同期回路設計技術として提案されている細粒度パイプライン手法等により回避可能であるが，その場合，挿入するラッチ分だけ回路面積と遅延が若干増大することになる．

次に，各々の対策手法において DPA の対策効果を保持するための実装条件と必要な機能について考える．Masked-And は，ある遅延時間の範囲内で乱数成分に関する遷移が発生すれば，DPA により解析が困難となることが，著者らの検討から明らかになっている[26]．しかしこの条件は，一般的な設計環境では困難である．

表 2 各対策手法による AES-Sbox の実装結果

対策手法	回路面積 [LUTs]	最大回路遅延 [ns]
対策なし	86	20.68
Masked-And	332	35.39
WDDL	456	46.80
RSLUT	174	30.35

また，1 つの S-box に対して 1 サイクルあたり必要な AND 処理分の乱数(数 10 bit)を必要とする．WDDL については，相補的な動作を行うゲートの配線長をそろえる必要がある．これは，フルカスタムのような手動によるレイアウトが可能な設計環境であれば可能であるが，自動配置配線では一般に保証されない．一方，RSL(RSLUT)は制御信号をデータ信号より遅れて変化させる必要がある．これは，十分な遅延のマージンをとれば，実現は容易であり，自動配置配線も可能である．また，暗号回路全体で必要な乱数は 1 サイクルあたり 1bit のみである．

以上のことから，RSLUT は他の方式と比較して実装効率と実現性に優れている．また，これらの議論は FPGA 上での実装だけに限定されず，RSL を用いた ASIC 実装についても同様の傾向が得られることが予測される．なぜならば，LUT による必要論理量評価はゲート換算でも同等の傾向を示し，また回路遅延についても LUT を通過するために必要な遅延は，ゲート換算でも同等の傾向となるためである．

6. まとめ

本稿では，2 線式対策手法の問題点を指摘し，1 線式による新たな DPA 対策手法を提案した．提案した対策手法は，ゲート毎の信号遷移を均等化し，過渡遷移の伝搬を抑えることで，予測可能なデータに依存しない電力消費を実現することが可能となった．また，他の対策手法ではレイアウトの最適化が必要であるのに対して，本稿で提案した手法は一般的な LSI の設計環境により実現することが可能であることを示した．さらに，提案した対策手法の効果を実証するために，FPGA を用いてモデル化を行い，DPA におけるリークの評価を行った．その結果，十分な効果が確認され，従来の対策手法と比較して実装効率と実現性に優れていることを示した．

参 考 文 献

[1] K.Tiri, M.Akmal, I.Verbauwhede, “A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on SmartCards,” Proc. Of 28th European Solid-State Circuits Conference (2002) 403-406

[2] K.Tiri, I.Verbauwhede, "Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology," CHES 2003, LNCS 2779, p.125-136, 2003

[3] K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,"in Proc. of Design Automation and Test in Europe Conference (DATE 2004), pp. 246-251,2004.

[4] E.Trichina, "Combinational Logic Design for AES SubByte Transformation on Masked Data," Cryptology ePrint Archive, 2003/236, http://eprint.iacr.org/complete/

[5] M.Akkar and C.Giraud, "An implementation of DES and AES, secure against some attacks," CHES 2001, LNCS 2162, pp. 309-318, 2001.

[6] S.Chari, C.S.Jutla, J.R.Rao and P.Rohatgi, "Towards sound approaches to counteract poweranalysis attacks," In Advances in Cryptology - - CRYPTO'99, LNCS 1666, pp. 398-412, 1999.

[7] L.Goubin and J. Patarin, "DES and differential power analysis," CHES'99, LNCS 1717, pp. 158-172, 1999.

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

[9] P. Kocher, J. Jaffe and B. Jun, "Introduction to Differential Power Analysis and Related Attacks," http://www.cryptography.com/dpa/technical/index.html

[10] T.Messerges, "Securing the AES finalists against power analysis attacks," FSE2000, LNCS 1978, pp. 150-165, 2000.

[11] E. Trichina, D. De Seta and L. Germani, "Simplified Adaptive Multiplicative Masking for AES and its secure implementation," CHES 2002, LNCS 2523, pp. 187-197, 2002.

[12] P. Chodowiec and K. Gaj, "Very Compact FPGA Implementation of the AES Algorithm," CHES 2003, LNCS 2779, p.319-333, 2003

[13] A. Satoh, S. Morioka, K. Takano and S. Munetoh, "A compact Rijndael hardware architecture with S-Box optimization," In Advances in Cryptology - ASIACRYPT 2001, LNCS 2248, pp. 239-254, 2001.

[14] T. Messerges, "Using second-order power analysis to attack DPA resistant software," CHES 2000, LNCS 1965, pp. 238–251, 2000.

[15] J.-S. Coron and L. Goubin, "On Boolean and arithmetic masking against differential power analysis," CHES 2000, LNCS 1965, pp. 231–237, 2000.

[16] C. Clavier and M. Joye, "Universal Exponentiation Algorithm – A First Step Towards Provable SPA Resistance," CHES 2001, LNCS 2162, pp. 300–308, 2001.

[17] J.-S. Coron, "Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems," CHES'99, LNCS 1717, pp. 292–302, 1999.

[18] T. Messerges, E. Dabbish, and R. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards," CHES'99, LNCS 1717, pp. 144-157, Springer-Verlag, 1999.

[19] S.B.Ors, E.Oswald and B. Preneel, "Power-Analysis Attacks on an FPGA - First Experimental Results," CHES 2003, LNCS 2779, pp. 35-50, 2003

[20] A.P. Chandrakasan, S. Sheng, and R.W.Brodersen, "Low Power Digital CMOS Design," IEEE Journal of Solid State Circuits, pp. 473-484,1992.

[21] B. Lin and S. Devadas, "Synthesis of Hazard-Free Multilevel Logic Under Multiple-Input Changes from Binary Decision Diagrams," IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, vol. 14, pp. 974-985, 1995.

[22] S. Devadas, K. Keutzer, and J. White, "Estimation of Power Dissipation in CMOS Combinational Circuits Using Boolean Function Manipulation," IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, vol. 11, pp. 373-383, 1992.

[23] Xilinx,Inc, Data sheet "Virtex™ 2.5V Field Programmable Gate Arrays", 2001. (http://www xilinx.co.jp/bvdocs/publications/ds003.pdf)

[24] 小沢,石山,今井,中村,南谷, "細粒度化による非同期式パイプラインの最適化設計," CPSY-99-10, 1999.

[25] 佐伯, 鈴木, 市川, "リークモデルの構築と論理シミュレーションによる DPA 評価," ISEC2004, 2004.7

[26] 市川, 鈴木, 佐伯, "データマスクを利用した DPA 対策に対する攻撃," ISEC2004, 2004.7

[27] 渡辺 誠, "超 LSI 設計," 企画センター,1983.