SCIS 2013 The 30th Symposium on Cryptography and Information Security
Kyoto, Japan, Jan. 22- 25, 2013
The Institute of Electronics, Information and Communication Engineers

スタンダードセルからの微小な EM リーク
Measurable Subtle EM Leak from Standard Cells

菅原健* 鈴木大輔* 佐伯稔* 汐崎充† 藤野毅‡
Takeshi Sugawara Daisuke Suzuki Minoru Saeki Mitsuru Shiozaki Takeshi Fujino

あらまし ASIC セミカスタム設計における最小単位であるスタンダードセル内部のリークが，電磁界解析において計測可能であることを示す．専用に設計・試作した TEG チップを用い，スタンダードセル単独で動作させた際に生じる磁界の変化を，チップのごく近傍に設置した磁界プローブにより計測する．実験の結果より，(i) これまで理論的な検討のみされていた，オンになる PMOS, NMOS の個数に応じたリークが計測可能であることを実証する．また，(ii) 新たなリーク要因として内部非線形ゲートによるモデルを示し，それに基づいて XOR ゲートがリークすることを実証する．加えて，実験結果が，既存の対策手法へ与える影響について論じる．

キーワード サイドチャネル攻撃，電磁界解析，ASIC セミカスタム設計，ゲートレベル対策技術

1 はじめに

2012 年に高橋によって，スタンダードセル内のリークに注目し，RSL (Random Switching Logic[1])を攻撃する手法が提案された[2]．それは，後述するように，単一セル内の PMOS（もしくは NMOS）のうち，オンになるトランジスタ数により配線容量の充放電電流（およびそれによって生じる信号遅延）が変調されることに基づくものである．ただし，提案法は理論的な検討とシミュレーションに留まっており，そのような微小な差が計測可能か否かは未解決である．そもそも RSL は，RSL セルに安全境界を置いて設計されている[3]．換言すれば，攻撃者はセル内を観察する能力を持たないことを想定している．そのような前提は，論理ゲートを最小単位とする（すなわちトランジスタレベルを考慮しない）他の多くの対策(WDDL, MDPL など[4])でも共有されていると言える．そのため，問われているのは，対策を設計する際に採用する前提の妥当性である．その問題の解決には，攻撃者は実際にどこまで計測可能なのかを検証することが不可欠である．

一方，攻撃者の計測能力は，時間とともに向上すると考えるべきである．近年では，特に電磁波解析[5, 6]の進展がめざましい．電磁波解析は，提案当時より，地理的な局所性を利用できる点が有利であると言われてきた．それに加え，近年では，消費電力の計測では観測できなかった「向き」に関する情報が取得できることが実証された[7, 8]．しかし，電磁界解析の研究は暗号アルゴリズムを実装する回路システムを対象とするのが一般的であり，スタンダードセル 1 個について何が計測しうるかという基礎的な研究は，著者らの知る限りでは存在しない．

以上の背景より，スタンダードセル内の挙動を，電磁界プローブにより計測する研究を実施した．本論文の主な貢献は以下の通りである．(i) 高橋によるセル内のチャネル数に応じたリーク[2]は，チップ近傍からの磁界計測により検出可能であることを実証する．(ii) さらに別のセル内のリーク要因として内部非線形ゲートによるものを示し，それに基づき XOR ゲートがリークすることを実証する．

本論文は，次のように構成する．まず，スタンダードセル内外でのリークについて，リークモデルの観点から論じる．その後，単一のスタンダードセルを計測するために設計・試作した専用の TEG (Test Element Group) チップについて述べる．実験では，チップ内で単一のスタンダードセルを動作させ，その際の電磁界をチップの近傍に設置した磁界プローブにより計測する．NAND ゲートと XOR ゲートを対象とした実験結果より，セル内部に起因するリークが計測可能であることを示す．最後に，実験の結果が，既存の対策法へ与える影響について考察する．

本論文の結果によれば，比較的性能の良い計測器を持つ攻撃者は，スタンダードセル内のリークを計測可能で

* 三菱電機株式会社 情報技術総合研究所
Sugawara.Takeshi@bp.mitsubishielectric.co.jp
† 立命館大学 総合理工学研究機構
‡ 立命館大学 大学院理工学研究科

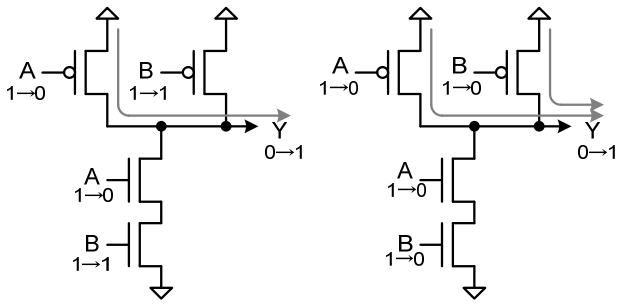

図１　NAND ゲートの出力が 0->1 と遷移する際にオンになる PMOS の違いと，その際の電流経路

ある．それは，レイアウトレベル・トランジスタレベルでの対策の必要性を示唆するものである．

2　リークモデル

本論文がテーマとするセル内外のリークについて，リークモデルの観点から述べる．リークモデルは，攻撃用と対策用のものに大別できる．

攻撃側では，中間値から電力の予測値を求めるのにリークモデルを用いる．有名なものとして，ハミングウェイトモデルや Zero-value モデルなどがある[4]．攻撃者にとっては，最小限の事前情報・仮定の元で攻撃成功することが望ましい．そのような観点で，これまでに様々な手法が提案されてきた[4, 9]．

防御側では，攻撃者の計測能力を抽象化するためにリークモデルを用いる．すなわち，あるモデルに従ったリークが観測可能であったとしても，攻撃が困難となるように対策法が設計される．そのようなモデルを明示的に扱った文献としては，ゲートの信号遷移に基づくモデル[3]を提案したものが存在する．想定するリークモデルが成立しなくなった場合，その対策は無効化される可能性がある．例として，信号遷移を均一化する対策であっても，グリッチ[10]やアーリープロパゲーション効果[3]により，対策が破られることが知られている．

これまで知られているゲートレベル対策手法では，前述の信号遷移モデルが採用されることが多い．すなわち，ゲート（もしくはスタンダードセル）はブラックボックスとして扱い，その入出力に関する信号遷移を均一化するという設計方針を採用する．本稿では，スタンダードセル内部のリークを扱い，以上の前提が妥当なものであるかどうか検証する．以降では，そのようなリークとして，(i) 電流経路リークと (ii) 内部非線形ゲートリークについて述べる．

2.1　電流経路リーク

本モデルは，RSL を攻撃するために，高橋によって提案された[2]．以下では，原論文よりも小さな例として，

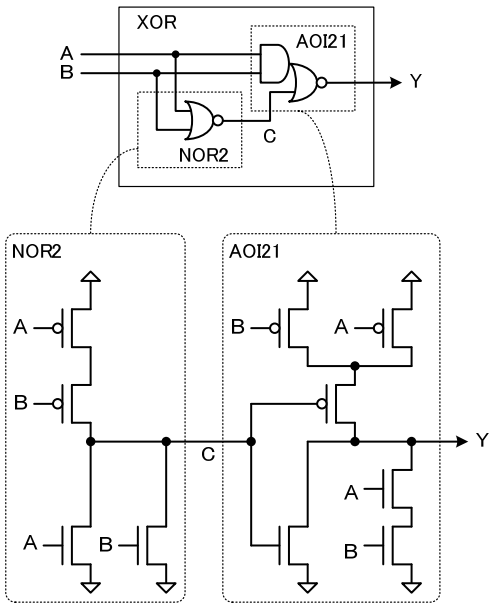

図２　XOR ゲートのトランジスタレベルの実装

NAND ゲートを対象にその機序を述べる．

図１に，典型的な NAND ゲートと，その出力が 0 から 1 へ変化する際の電流経路を示す．NAND ゲートの V_{DD} 側には 2 つの PMOS が接続されており，いずれか，もしくは両方がオンになることで電源電圧から信号線 Y への経路が成立し，過渡電流が生じる．過渡電流はいずれ配線の負荷容量を充電し，結果として信号線 Y の電圧値の遷移が生じる．そのような遷移には 2 通りのパターンが存在する．2 つの PMOS のうち片方だけオンになる場合と，両方ともオンになる場合である（図１の左と右）．それぞれは，電流のドライブ能力が異なる．すなわち，2 つの PMOS のオン抵抗が同じと仮定した場合，電源—信号線間の抵抗が 1 つだけオンになる場合と 2 つともオンになる場合では 2 倍異なる．そのため，2 つともオンの場合は，より大きい過渡電流を生じる．また，電流量の違いが負荷容量の充電時間の違いとなり，最終的には信号遷移時間に差が現れる．攻撃者の視点では，表１に示すように，入力値に応じた波形を，信号遷移モデルと比較して細かく区別することが可能となる．その結果，「あるグループ内の遷移は区別できない」という前提に基づく対策手法を攻撃できるようになる可能性がある．

表１　NAND ゲートの入力が 前状態$(11)_2$ から遷移する際，各モデルの攻撃者が識別できるグループ

	信号遷移	電流経路
Group #1	$(11)_2 \rightarrow (11)_2$	$(11)_2 \rightarrow (11)_2$
Group #2	$(11)_2 \rightarrow (01)_2$ $(11)_2 \rightarrow (10)_2$ $(11)_2 \rightarrow (00)_2$	$(11)_2 \rightarrow (01)_2$ $(11)_2 \rightarrow (10)_2$
Group #3		$(11)_2 \rightarrow (00)_2$

以上は PMOS 側についてのみ述べたが，　NOR ゲー

	A	B	A'	B'	C	C'	Y	Y'	Sum (Y⊕Y')	Sum (C⊕C')
	0	0	0	0	1	1	0	0	2	3
(a)	0	1	0	0	0	1	1	0		
(b)	1	0	0	0	0	1	1	0		
	1	1	0	0	0	1	0	0		
	0	0	0	1	1	0	0	1	2	1
	0	1	0	1	0	0	1	1		
	1	0	0	1	0	0	1	1		
	1	1	0	1	0	0	0	1		
	0	0	1	0	1	0	0	1	2	1
	0	1	1	0	0	0	1	1		
	1	0	1	0	0	0	1	1		
	1	1	1	0	0	0	0	1		
	0	0	1	1	1	0	0	0	2	1
(c)	0	1	1	1	0	0	1	0		
(d)	1	0	1	1	0	0	1	0		
	1	1	1	1	0	0	0	0		

図 3　　NAND ゲートの出力が 0->1 と遷移する際のONとなるPチャネルトランジスタの個数の違い

トでも NMOS 側で同じことが起こる．また，3 入力以上の NAND，NOR ゲートでも同じことが起きる．

文献[2]では，以上の機序による差が存在することを，LTSpice シミュレーションによって検証している．しかし，シミュレーションは電源電圧 5V の MOS と 3 pF の負荷容量を用いたものであり，スタンダードセルではなくディスクリート素子のスケールのものである．また，シミュレーションはノイズ無しで行われるため，本モデルが実測に計測可能かどうかは未解決であった．

2.2　内部非線形ゲートリーク

セル内の挙動が外部より計測できるという立場であれば，電流経路リークとは機序の異なるリーク要因を考えることができる．図 2 に， XOR ゲートのトランジスタレベル実装の 1 つを示す．本実装では，NOR と AOI (AND-OR-Inverter)ゲートを連結して 1 つのセルに納めることで XOR スタンダードセルを実現する．これは XOR ゲートをトランジスタで構成する一般的な方法の 1 つであり，文献[11]の XOR ゲートもこの方法で実装されている．従来，線形である XOR ゲートは，信号遷移確率が等しくなるため解析対象にはならなかった．しかし，セル内が観測可能という立場であれば，XOR ゲートを構成する非線形ゲート(NOR, AOI)の性質が顕在化し，結果として遷移確率がアンバランスすることが考えられる．

図 3 に，図 2 の XOR ゲートの信号遷移表を示す．信号名は図 2 と対応している．ただし信号 A, B, C, Y は遷移前，A', B', C', Y'は遷移後の値を表すものとする．NOR ゲートの出力信号 C に注目した場合，その遷移確率は（NOR の遷移確率と同じであり）偏ることが分かる．そのため，セル内の中間信号 C を観測できる攻撃者であれば，XOR の入力として$(00)_2$と$(11)_2$を区別することができる．

そのような機序によるリークを，以降では内部非線形ゲートリークと呼ぶことにする．

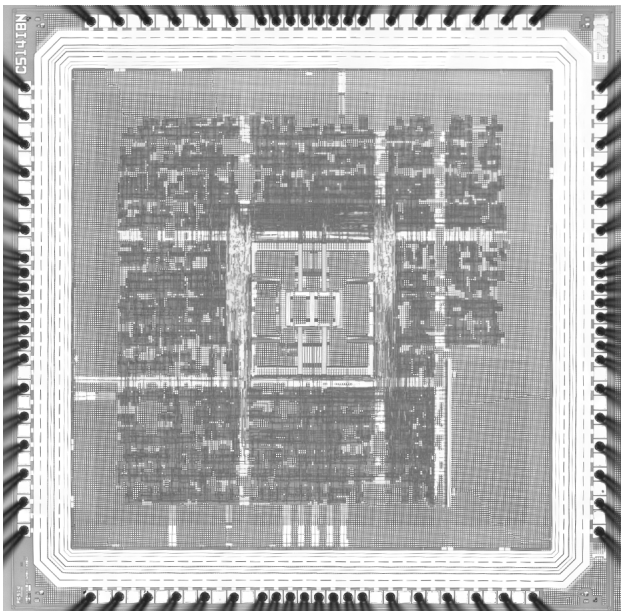

図 4　　計測用 TEG チップの写真
(Rohm 180 nm 2.5mm*2.5mm)

3　計測用 TEG チップ

スタンダードセル単体の計測を行うために，専用の TEG チップ（図 4）を開発した．プロセスはローム 180 nm，サイズは 2.5mm 角である．

図 5 に，TEG チップに含まれる回路のデータパスとタイミングダイアグラムを示す．TEG チップには，図 5 に示すような回路が，スタンダードセルの種類ごとに 64 個搭載されている．

図 5 に示すように， 1 つの TEG は，イネーブル付きレジスタ（MUX と DFF で構成する）で計測対象(DUT: Device Under Test)を挟み込んだ構成を持つ．DUT のデータパス幅は 16 ビットであり，1 つの DUT につきスタンダードセルが 4 つずつ接続されている．それら 4 つは全て同種のスタンダードセルであるが，出力のレジスタの個数が異なる．それにより，ファンアウトの違いに基づく差を計測することも可能である．なお，スタンダードセルの入力数に応じて，2 入力用の Type A, 3 入力用の Type B など，複数のタイプが存在する．なお，TEG への 16 ビットの入力(data_in)は，外部バスから供給される．そのため，書き込む値に応じて，動作するセルの個数を選択できる．

ゲートの遷移とレジスタによるリークを区別するために，順序回路によりシーケンスが構成される．TEG は次のように動作する．まず，外部バスから TEG の入力を書き込むと，それは data_in にセットされる．その時点で DUT はまだ動作しない．その後，外部バスから（図 5 には表示されていない）コントロールレジスタに特定の値を書き込むと，DUT を動作させるシーケンスが開始する．シーケンスが開始すると，まず波形取得用のトリガ信号がチップ外へ出力される（clk=0）．その後，

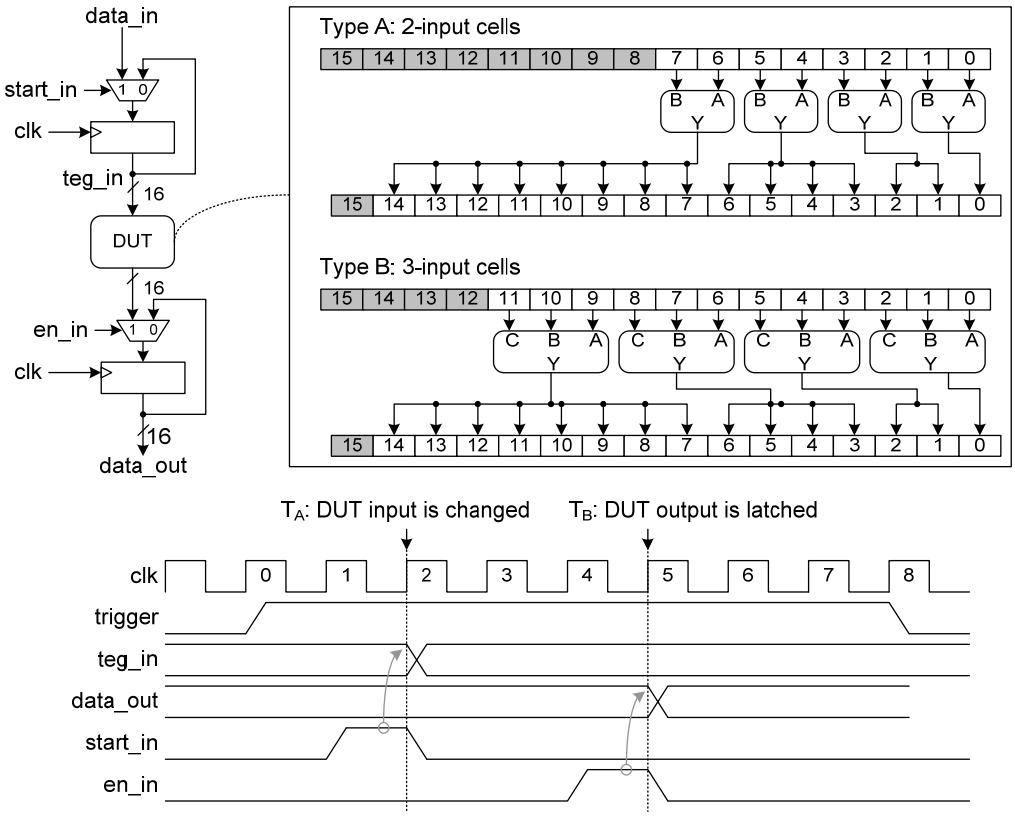

図 5　　計測用 TEG の回路構成とタイムチャート

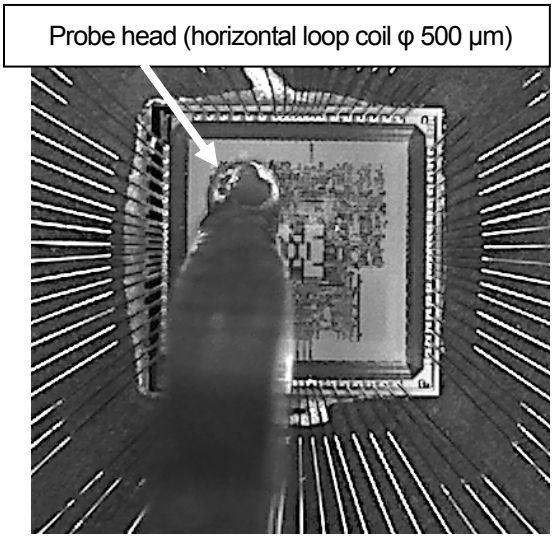

図 6　　チップに磁界プローブを設置した様子
（チップの向きは図 4 と同じ）

start_in 信号がアサートされると，続く立上りエッジ(T_A)において DUT の入力が遷移する．DUT の動作によるリークは，このタイミングで計測される．さらに数サイクル後，時刻 T_B において，DUT の出力値がレジスタに取り込まれる．このタイミングでは，レジスタの遷移に関するリークが計測される．なお，出力レジスタの出力(data_out)は比較的大きい論理ゲート（TEG 選択用 64:1 セレクタ）に接続されている．

4　実験

4.1　実験環境

前述の TEG チップの計測を行った．評価プラットフォームは SASEBO-W とその上にマウントされた SASEBO-R2 である．SASEBO-R2 上のソケットに，前述の TEG チップを搭載して実験を行った．計測は，開封したチップの表面に，磁界プローブを設置して行った．計測器の詳細は表 2 に示す通りである．

表 2　　計測機器

Instrument	Specification
Oscilloscope	Bandwidth 12.5 GHz, sampling rate 25.0 GSa/s
M-field probe	Horizontal magnetic probe, 500 μm diameter, bandwidth 2.0 MHz – 6.0 GHz, with built-in amplifier
XYZ stage	50 to 100 μm resolution

図 6 に，プローブを設置した様子を示す．プローブの座標は，TEG チップのレイアウト情報(GDSII)を用い，図 5 に示した TEG 回路全体がコイルのループ内に納まるように定めた．プローブの高さについては，プローブの先端がチップの絶縁膜に接触するまで降下させた．

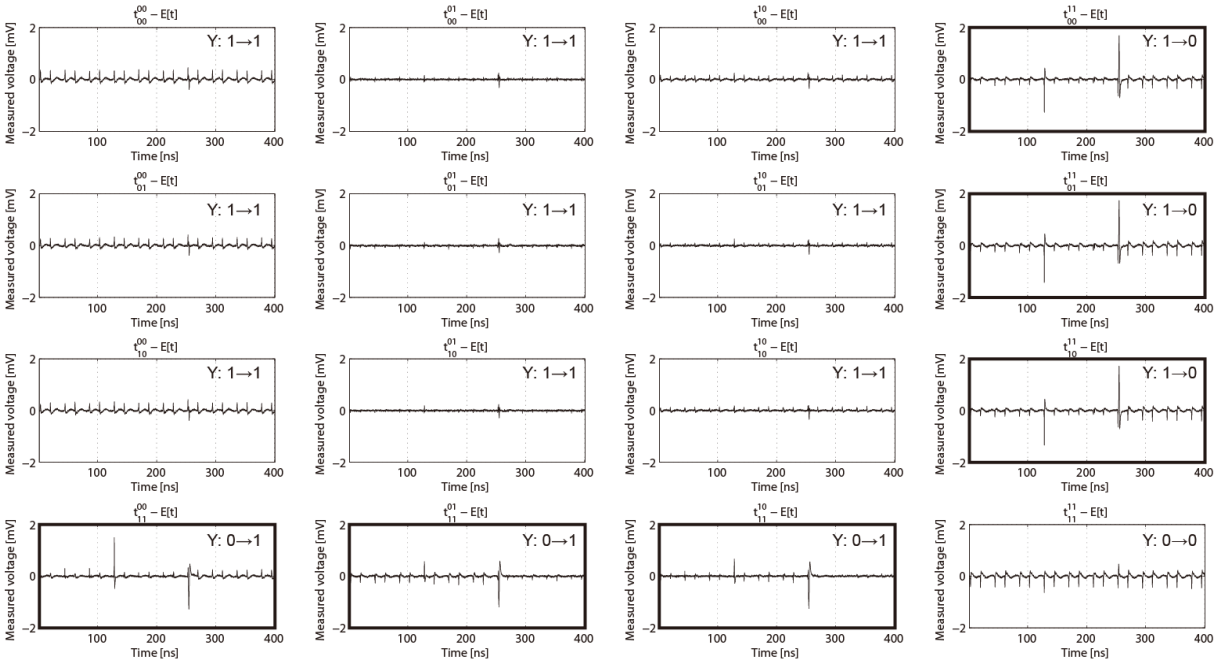

図 7　2 入力 NAND ゲートの 16 通りの遷移に対応する差分波形.
各グラフの右肩に，出力信号 Y の遷移を合わせて示す

いずれの実験でも，DUT に含まれる 4 つのスタンダードセル（図 5 を参照）のうち，ファンアウトが 4 のものを単独で動作させた.

計測では，擬似的な相関を排除するために，入力を乱数により選択した．その後，記録しておいた入力パターンを元に，信号遷移に応じてグループ分けを行った．たとえば 2 入力ゲートであれば，遷移のパターンは前状態 2^2×後状態 2^2=16 種類である．計測回数は，各グループの波形数の期待値が 10,000 個になるように決めた．すなわち，2 入力ゲートであれば 160,000 波形，3 入力ゲートであれば 640,000 波形（$2^3 \times 2^3$=64 グループ）を計測した．　最後に，各グループごとの平均波形を求めた.

<u>波形の記法</u>

以降では，1 つの遷移パターンに対応する平均波形を，次のように表記する：

$$t_{before}^{after}.$$

なお，*before* と *after* は 2 進数表記とする.

（例 1）2 入力ゲートで，入力が $(00)_2$ から $(01)_2$ へ遷移する際の平均波形を，t_{00}^{01} と表記する.

（例 2）3 入力ゲートで，入力が $(101)_2$ から $(111)_2$ へ遷移する際の平均波形を，t_{101}^{111} と表記する.

また，計測波形全体の平均を E[t] と表記することにする.

4.2　2 入力 NAND

単独のセルによるリークの計測可能性，および電流経路リーク（2.1 節）を検証するために，2 入力 NAND ゲートを計測した.

まず，ゲート 1 個の遷移による差が観測できることを検証する．そのために，16 種類の遷移パターンに応じた 16 枚の平均波形（$t_{00}^{00} \cdots t_{11}^{11}$）を求め，全体の平均 E[t] からの差をプロットした(図 7)．図 7 において，NAND ゲート出力が変化する 6 ケースを太枠で表示した．図より，太枠のケースについて，スパイクが 2 本ずつ確認できる．それらは，図 5 におけるタイミング T_A と T_B に対応する．T_A のタイミングでのスパイクの存在は，単独のセルが生じる信号変化が計測可能であることを表している.

続いて，電流経路リークの計測可能性を検証する．そのために，PMOS が 2 つともオンになる t_{11}^{00} と，1 つだけオンになる t_{11}^{01}，t_{11}^{10} を比較する（図 1 を参照）．なお，図 7 からは，時刻 T_A・T_B 以外でも細かなスパイクが複数存在する様子が確認できる．それは，直前に入力した値のハミングウェイトに応じて強さが変化する．そのため，これはセルそのものではなく，入力に応じた擬似的なものと考えられる．その補正のため，後状態を共通とするグループごとの差分を求めた．例として t_{11}^{00} では，後状態が$(00)_2$ と共通である波形を差し引いた $t_{11}^{00} - (t_{00}^{00} + t_{01}^{00} + t_{10}^{00})/3$ を求めた．このような補正は，以降の実験でも採用する．図 8 に，t_{11}^{00}，t_{11}^{01}，t_{11}^{10} の 3 通りについて重ねて表示した結果を示す. なお, 図 8 は, 時刻 T_A と T_B のスパイクをそれぞれ拡大して表示したものである．結果より，時刻 T_A のスパイクにおいて t_{11}^{00} が他 2 つと分離している様子が観察できる．これは，2.2 節で述べた電流経路リークであると考えられる．一方，時刻 T_B のスパイクについては, 3 通り全てでよく一致し

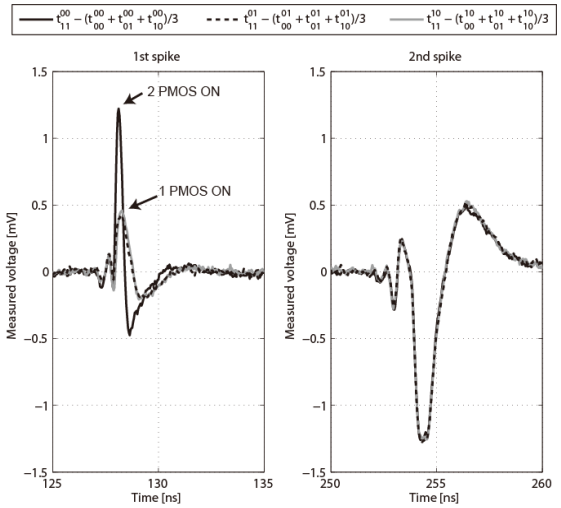

図８　2 入力 NAND ゲートの計測結果 : 出力が 0 から 1 へ遷移する 3 通りに関する差分波形．（左）時刻 T_A でのスパイク，(右)時刻 T_B でのスパイク

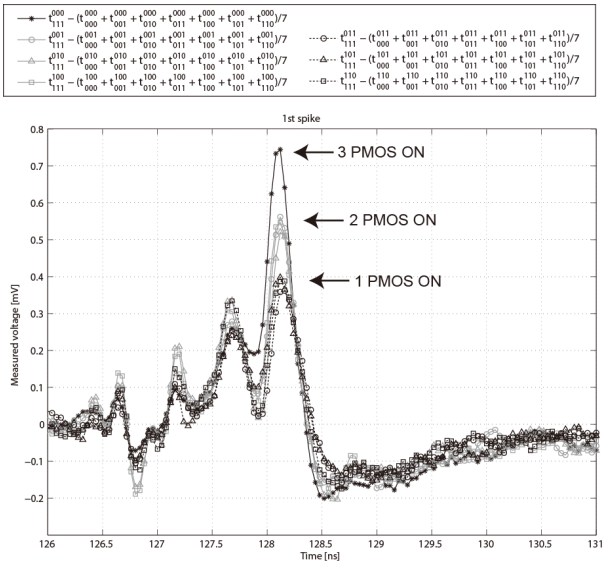

図９　3 入力 NAND ゲートの 7 通りの遷移パターンに対応する差分波形，時刻 T_A でのスパイクを拡大して表示したもの

ている. それは, 出力レジスタに取り込まれた後は, t_{11}^{00}, t_{11}^{01}, t_{11}^{10} に区別が無いためである．また，図より，T_A と T_B の波形でスパイクの幅に顕著な差があることが分かる．T_B のスパイクは 1--2 ns 程度であるが，T_A のスパイクの幅は 1ns 未満である.

4.3　3 入力 NAND

4.2 節の実験を，3 入力 NAND ゲートを対象として繰り返した．ゲートへの入力数が増加するため，遷移パターンは前述したように 64 通りになる. その場合, NAND 出力が 0 から 1 に遷移するのは 7 ケースある．それぞれと，その際の PMOS のオンになる個数の関係は表 3 のようになる.

表３　3 入力 NAND の出力が 0 から 1 に遷移する 7 ケースを，ON になる PMOS 個数で分類したもの

# PMOS ON	Trace
3	t_{111}^{000}
2	t_{111}^{001}, t_{111}^{010}, t_{111}^{100}
1	t_{111}^{011}, t_{111}^{101}, t_{111}^{110}

以上 7 通りの場合について，図 8 と対応するプロットを作成した．結果を図 9 に示す．図 9 は，時刻 T_A のスパイクのみを示している．図の見やすさのために省略するが，時刻 T_B のスパイクは，図 8 と同様に 7 ケース全てでよく一致した．結果より，スパイクのピーク付近において，値が 3 群に分離する様子が確認できる．その 3 群は，表 3 の場合分けと一致する．この結果は，電流経路リークが計測可能であることをさらに補強するものである.

4.4　2 入力 XOR

内部非線形ゲートリークの計測可能性を検証するため, これまでと同様の実験を，2 入力 XOR ゲートを対象として繰り返した．なお，計測対象の XOR スタンダードセルは, 図 2 に示す NOR と AOI の組み合わせで実現されているものである．XOR ゲート出力 Y による影響と中間信号 C による影響を区別するため，出力が 1 から 0 に遷移する場合についてのみ解析する．そのような場合は, 図 3 における(a) t_{01}^{00}, (b) t_{10}^{00}, (c) t_{01}^{11}, および(d) t_{10}^{11} の 4 ケースが存在する．図 3 から読み取れるように，(a) t_{01}^{00}, (b) t_{10}^{00} の場合のみ，中間信号 C の遷移が生じる．そのため，内部非線形ゲートリークが存在するならば, (a), (b)の組と(c), (d)の組は識別できるはずである．そこで，(a)—(d)の 4 ケースについて，図 8 と同様の図を作成した．結果を図 10 に示す．結果より，時刻 T_A のスパイクにおいて，(t_{01}^{00}, t_{10}^{00})の組と(t_{01}^{11}, t_{10}^{11})の組に波形が分離する様子が観察できる．一方，図 8（右）より，ゲート出力については，いずれの場合でもよく合っていることが分かる．以上の結果は，内部非線形ゲートリークも計測可能であることを示している.

5　考察

以降では，これまでに示した実験結果が，既存の対策手法へ与える影響について述べる.

5.1　電流経路リークを利用した攻撃

<u>RSL [1, 3] と MDPL [4]</u>

RSL への影響は，文献[2]にある通りである．また，

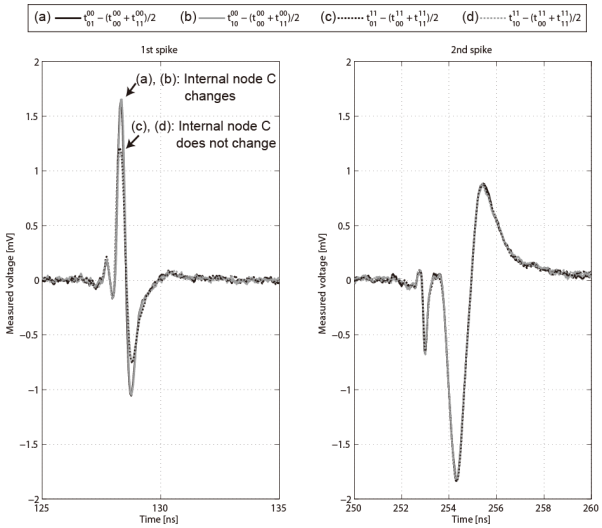

図 10　3 入力 XOR ゲートの計測結果：出力が 1 から 0 へ遷移する 4 通りに関する差分波形．(左) 時刻 T_A でのスパイク，(右)時刻 T_B でのスパイク

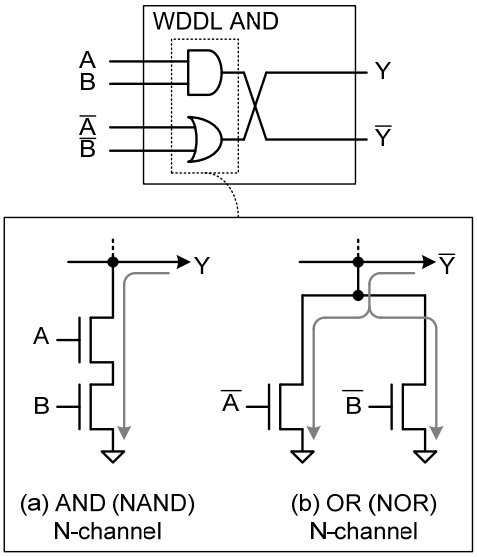

図 11　WDDL NAND を構成する NAND/NOR ゲートの N チャネルと，立下り時の電流経路

RSL とほぼ同様の回路構造をとる多数決論理ゲート(MAJ ゲート)を利用する MDPL も同様である．

WDDL [4]

これまでに知られているように，相補対がバランスしていない場合，WDDL は攻撃可能であることが知られている．また，たとえ相補対がバランスしていても，WDDL ゲートへの入力信号の到来時間に差があった場合，アーリープロパゲーション効果により攻撃可能となる[3]．それに対し，たとえ WDDL の相補対のアンバランスとアーリープロパゲーション効果が解決できたとしても，電流経路リークが計測できる攻撃者であれば攻撃可能である．

WDDL NAND ゲートは，AND, OR ゲートの組で構成する[4]．AND，OR ゲートは，NAND，NOR ゲートと NOT の組み合わせで構成するのが一般的である．動作する際は，まずプリチャージフェーズで出力が $(00)_2$ に初期化される．すなわち，AND ゲートと OR ゲートの両方の出力が 0 になる．NAND, NOR ゲートに注目して考えれば，出力が $(11)_2$ にプリチャージされる．評価フェーズでは，NAND と NOR ゲートの出力のいずれか一方が 1 から 0 に遷移する．その際の電流パスを図 11 に示す．図 11 では，出力が 1→0 と遷移する際に考慮される N チャネルのみ示している．WDDL の安全性は，NAND と NOR のいずれの遷移であるか区別できないことによる．しかし，NAND と NOR では NMOS の電流経路が異なるため，両者を区別できる攻撃者であれば，相補対のいずれがスイッチしたのかを知ることができる．

5.2　内部非線形ゲートリークを利用した攻撃

2.3 節に示した，XOR ゲートのリークを利用した攻撃について考察する．図 12 に対象となる回路構造を示す．それは，乱数マスクのアンマスキングを想定している．図 12 の回路構造は一般的なものであり，ほぼ全ての 1st order masking で使用される．XOR ゲート出力 x は攻撃者にとって既知，入力 r は攻撃者にとって未知の乱数とする．攻撃は，内部非線形ゲートリークを用いて，乱数 r の分布にバイアスをかけることに基づく．乱数がバイアスされたサブセットが得られた場合，1st order attack が適用可能となる[12]．本節で述べる攻撃の，従来法[12]に対する優位は，たとえ乱数 r を生成する乱数生成器が SPA リークを生じなかったとしても適用可能である点にある．なぜなら，XOR 自身のリークをバイアスに利用するためである．

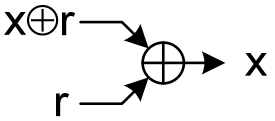

図 12　対象となる回路構造

バイアスは次のように行う．まず，攻撃者は，従来のサイドチャネル攻撃と同様に，大量の波形と出力の組を収集する．その後，既知の出力が x=0 となる半数のみを選別する．残留したセットのうち，ありうる XOR の入力ペアは(x⊕r=0, r=0)か(x⊕r=1, r=1)のいずれかである．乱数が完全であれば，

$$P(x\oplus r=0, r=0) = P(x\oplus r=1, r=1)$$

である．内部非線形ゲートリークにより，XOR の入力が $(00)_2$ であるか $(11)_2$ であるか識別できる攻撃者は，波形

を用いて P(x⊕r=0, r=0) > P(x⊕r=1, r=1)となるように，サブセットを選択することができる．具体的な選別方法は両ケースの分布によるが，図 10 の場合であれば，電圧値に適当な閾値を設け，閾値を超えた（もしくは超えない）サブセットを選別するだけでよい（2 つの分布の平均値に差があるため）．結果として P(x⊕r=0, r=0) > P(x⊕r=1, r=1) なるバイアスが達成できた場合，それは P(r=0) > P(r=1)なるバイアスを達成したことに他ならない．以降は文献[12]と同様である．

6 まとめ

本論文では，スタンダードセル内部のリークの計測可能性を検証した．そのために専用の TEG チップを試作し，その表面に設置した磁界プローブにより電磁界を計測した．その結果，電流経路リーク・内部非線形ゲートリークと呼ぶセル内部に起因するリークが計測可能であることを実証した．今回検出できたリークを利用した場合，多くの対策法が無効化できる．

本稿の結果は，少なくとも実験室環境ではセル内のリークが計測可能であることを示している．そのため，我々は対策を考える上で，セルの外側に安全境界を置くことに対して慎重になる必要がある．セルやゲートを安全境界として対策を設計する際は，少なくとも，抽象化するセルやゲートへの要件を明確にすべきである．

本稿の結果は，トランジスタ・レイアウトレベルでの対策法の必要性を示唆するものである．ただし，セル内部に起因するリークを電流経路リーク・内部非線形ゲートリークの 2 つで尽くしたとは考えていない．特に，製造ばらつきやレイアウトの非対称性を考慮した場合，いずれの PMOS がオンになったのかまで識別可能になる可能性は残されている．そのような現象が計測可能かどうかは未解決である．また，半導体が物質である以上，完全にリークしないゲートの設計はおそらく困難である．そのため，対策を設計する際に前提とするモデルの妥協点と，セルのリークを許容する上位レイヤの対策法に研究の余地がある．

その他にも，複数の課題が残されている．今回は，基礎的な検討を目的として，単独セルの計測を行った．暗号アルゴリズムを実装した回路システムを計測した場合，電流経路リーク・内部非線形ゲートリークがどの程度の深刻度を持つかは未解決である．今回実験に用いたのは，比較的古い 180 nm プロセスである．先端プロセスを用いた際の計測難易度の変化は検証する必要がある．

謝辞

本研究の一部は，JST CREST「ディペンダブル VLSI システムの基盤技術」の一環として実施した．また，本研究に用いたチップの試作は、VDEC ならびにローム株式会社の支援により行われたものである。

参考文献

[1] D. Suzuki, M. Saeki, T. Ichikawa “Random Switching Logic: A Countermeasure against DPA based on Transition Probability”, IACR Cryptology ePrint Archive 2004: 346 (2004)

[2] 高橋芳夫，暗号モジュールの電力解析攻撃耐性の評価法に関する研究，博士論文，2012.

[3] D. Suzuki, M. Saeki, T. Ichikawa “DPA Leakage Models for CMOS Logic Circuits”, CHES 2005: 366-382

[4] S. Mangard, E. Oswald, T. Popp, “Power Analysis Attacks: Revealing the Secrets of Smart Cards,” Springer-Verlag, 2007.

[5] K. Grandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results", CHES 2001.

[6] S. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM Side Channel(s)", CHES 2002.

[7] E. Peeters, F. -X. Standaert, and J. -J. Quisquater, “Power and electromagnetic analysis: Improved model, consequences and comparisons,” Integration, the VLSI Journal, Vol. 40 Issue 1 (January 2007), pp. 52 - 60.

[8] 菅原健，鳥塚英樹，本間尚文，佐藤証，青木孝文，山口正洋，” 最近傍から計測した磁界を用いた差分電磁波解析，” 2009 年暗号と情報セキュリティシンポジウム，3A1-5, January 2009.

[9] C. Whitnall, E. Oswald, F-X. Standaert, "The myth of generic DPA and the magic of learning", http://eprint.iacr.org/2012/256.pdf

[10] S. Mangard, K. Schramm, “Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations”, CHES 2006

[11] Silicon zoo, Megamos chip XOR gate, http://www.siliconzoo.org/megamos.html

[12] K. Tiri , P. Schaumont, "Changing the Odds against Masked Logic", SAC2006.