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

SRAM アクセスのサイドチャネル情報
Side-Channel Information associated with SRAM access

佐伯 稔* Minoru SAEKI　鈴木 大輔* Daisuke SUZUKI　菅原 健* Takeshi SUGAWARA

汐崎 充† Mitsuru SHIOZAKI　藤野 毅‡ Takeshi FUJINO

あらまし SoC のサイドチャネルセキュリティを向上するためには，秘密情報に関る各構成要素が高いサイドチャネルセキュリティを備える必要がある．代表的な IP コアの１つである SRAM は，SoC の構成要素として広く利用される．そこで本稿では TEG チップに搭載された SRAM のサイドチャネル評価を行い，SRAM のサイドチャネルセキュリティについてケーススタディした．高帯域の磁界プローブを用いた評価の結果，SRAM アクセス時のアドレスやデータとサイドチャネル情報の間に有意な相関が確認された．特に，アドレスについては，アドレスの値と線形な興味深い依存性を確認した．総消費電力を均一化して電力解析攻撃に対する対策を施したメモリであっても，空間分解能の高い電磁波解析攻撃に対しては，アドレスに依存した情報リークが発生する危険性が高い．

キーワード サイドチャネル攻撃，SoC，CMOS，SRAM，CPU

1 はじめに

SoC(Systems-on-a-Chip)はシステムに必要な機能を１チップに集積したシステム LSI であり，CPU，各種メモリ，暗号コプロセッサなど，さまざまな構成要素から成る．SoC のサイドチャネルセキュリティを向上するためには，暗号コプロセッサはもちろん，秘密情報に関る各構成要素が高いサイドチャネルセキュリティを備えることが求められる．このため，秘密要素に関る構成要素として既存 IP コアを利用する場合は，事前にその IP コアの安全性を確認する必要がある．該当する IP コアのうち CPU については，例えば，文献[1]でオープンソース CPU のサイドチャネルセキュリティを体系的にケーススタディした結果が報告されている．SoC におけるもう１つの代表的な IP コアは SRAM である．もしも SRAM アクセス時のサイドチャネル情報と秘密情報の間に有意な相関が存在すると，高いサイドチャネルセキュリティを備えた特別な SRAM を新たに開発するか，または CPU や暗号コプロセッサの SRAM 利用方法に特別な考慮が必要となる可能性がある．

SRAM は極めて一般的なコンポーネントであることから，これまでにいくつかの研究が知られている[2,3]．また，SRAM へのアクセスによる電力消費の差が，組み合わせ回路と比較して少ないと信じられていることや[4]，実装制約の大きい CPU での対策を目的として，SRAM のテーブル参照を元にした対策手法が多く提案されている[4,5,6]．これらの研究の多くでは，SRAM 自身のリークは無いものと前提を置くか，もしくは入出力であるアドレスやデータのハミング重みモデルやハミング距離モデルによる抽象化を行っている．それに対し，

* 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 Mitsubishi Electric Corporation, Information Technology R & D Center, 5-1-1 Ofuna Kamakura, Kanagawa, 247-8501, Japan.
† 立命館大学総合理工学研究機構 〒525-8577 滋賀県草津市野路東 1-1-1 Research Organization of Science & Engineering, Ritsumeikan University, 1-1-1, Nojihigashi, Kusatsu, Shiga, 525-8577, Japan.
‡ 立命館大学大学院理工学研究科 〒525-8577, 滋賀県草津市野路東 1-1-1 Graduate School of Science and Technology, Ritsumeikan University, 1-1-1, Nojihigashi, Kusatsu, Shiga, 525-8577, Japan.

SRAM の内部構造にまで踏み込んだ解析を行っているものは，文献[2]しか存在しない．また，文献[2]についても，攻撃者の視点でどこまで情報が取りうるのかという解析はなされていない．もし，対策が要求する前提条件が成立しなくなるのであれば，その対策は無効化される可能性がある．そのため，SRAM 単体としてのリークの挙動を調べることは重要である．

そこで本稿では TEG チップを用いて，SRAM アクセスに付随するサイドチャネル評価を行い，標準的な SRAM のサイドチャネルセキュリティについてケーススタディする．高帯域の磁界プローブを用いた評価の結果，既存研究で想定されていたアドレス・データのハミング重み・距離に応じたリークに加え，行アドレスと列アドレスそれぞれの値と線形な，従来知られていないリークが存在することを確認した．そのような未知のリークは，前述の通り既存研究の前提条件を成立しなくさせる危険性を持つものである．その具体例として，Dual-Rail RSL メモリ方式[7]を適用した AES 暗号回路に対して，このアドレス依存性を利用した電磁波解析攻撃実験を行ない，総消費電力を均一化して電力解析攻撃に対する対策を行ったメモリであっても，空間分解能の高い電磁波解析攻撃に対しては，アドレスに依存した情報リークが発生する危険性が高いことを示す．

以下，まず 2 章では基礎実験として，標準的な SRAM のサイドチャネル情報のアドレス依存性とデータ依存性を評価する．続く 3 章ではこれらの依存性に基いた SPA 的手法による攻撃可能性を評価する．また，4 章では Dual-Rail RSL メモリ方式を適用した AES 暗号回路に対する攻撃結果を示す．最後に 5 章でまとめと今後の課題について述べる．

2　アドレス/データ依存性の評価

SRAM アクセス時のアドレスやデータがサイドチャネル情報と高い相関を持つと，サイドチャネル情報を解析することで秘密情報またはその一部が漏洩する可能性がある．単純な例では，鍵データなどの秘密情報の読み書きや，Sbox などのテーブル参照が該当する．さらに，アドレスやデータそのものが特定されなくても，異なる SRAM アクセスでそれらのコリジョンが検出可能であれば，例えば，公開鍵暗号のべき乗剰余演算処理にとって脅威になり得る[8]．そこで，本節では SRAM のサイドチャネル情報のアドレス/データ依存性を評価する．

なお，SRAM アクセスの有無やアクセスの種類（リード/ライト）を識別されることが脆弱性につながるようなシステムもあり得るかも知れないが，これらについては本稿では扱わない．

2.1　SRAM 概要

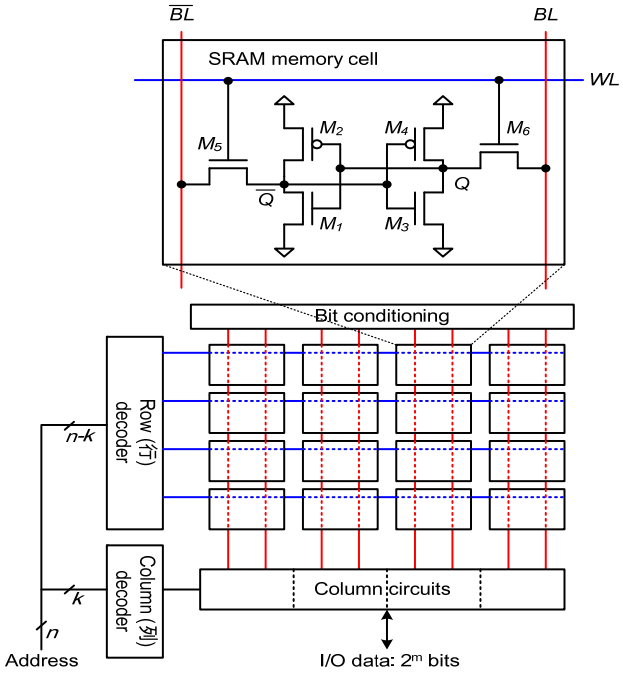

図 1: 一般的な SRAM のメモリセル(上)と SRAM ブロックの基本構成(下)

図 1 (上)に一般的な SRAM のメモリセル（1 ビット）を示す．メモリセルは，データを保持するための 4 個のトランジスタ（M_1–M_4）とデータのリード・ライトのための 2 個のトランジスタ（トランスファーゲート）で構成する．ワード線（WL）によってセルが選択され，ビット線（BL, $\overline{BL}$）を通じてデータのリード・ライトが行なわれる．SRAM ブロックは図 1(下)のように，このメモリセルが 2 次元のマトリックス上に配列されたメモリアレイと，セルの選択を制御するアドレスデコーダ，入出力制御回路などが含まれる．

SRAM へのアクセスは次のように行う．外部から入力したアドレスは，行アドレスと列アドレスに分割される．その後，行アドレスは行デコーダに，列アドレスは列デコーダに入力される．行デコードの結果，ワードラインのうち 1 本のみが有効化されて行が選択される．リード時は，選択された行のデータが並列で読み出され，最後に列デコードの結果によって 1 つの列が選択される．列アドレスで選択された列のデータが SRAM ブロックの出力データになる．ライト時には，列アドレスで選択された列にデータが駆動され，行アドレスで選択された行に書き込まれる．このように，行と列が一致したメモリセルがリード・ライトの対象となる．

メモリアレイは非常に規則正しい構造であり，ワード線やビット線は基本的に等間隔の並びとなっている．どのようなアドレスでも行と列が各 1 つずつ選択されるが，この規則性のため，選択される行や列によって電流経路なども規則的に変わり，何らかの形でサイドチャネル情報に反映する可能性がある．

2.2　実験環境

TEG チップの外観を図 2 に示す．このチップは各種スタンダードセル単体のサイドチャネル評価を可能とするためにローム 0.18 μm プロセスを用いて開発したもので，サイズは 2.5mm 角である．本稿で評価する SRAM ブロックは図右下の矩形領域に配置されている．TEG チップに搭載されている SRAM ブロックはリード・ライトのためのアドレスやデータのポートを 2 組備え，クロック同期で動作する 2 ポート SRAM であるが，基本的な構造は図 1 と変わらない．この SRAM は 16 ビット×512 ワードの構成で，リード・ライトなどの制御信号と，アドレス（9 ビット），入力データ（16 ビット），出力データ（16 ビット）のポートを持つ．アドレスの上位 6 ビットが行アドレス，下位 3 ビットが列アドレスである．TEG チップでは，SRAM にアクセスしないクロックサイクルは，SRAM の入力データとアドレスを全て 0 にプリチャージしている．

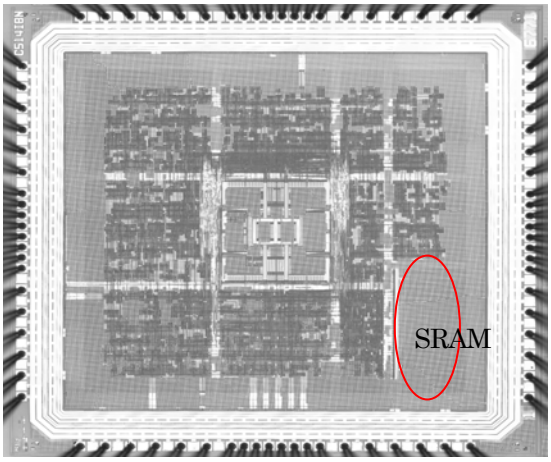

図 2: TEG チップ外観

表 1: 計測器

Instrument	Specification
Oscilloscope	Bandwidth 12.5 GHz, Sampling rate 25 GSa/s
M-field probe	φ 500 μm, 2 MHz--6 GHz.
XYZ stage	50 to 100 μm resolution

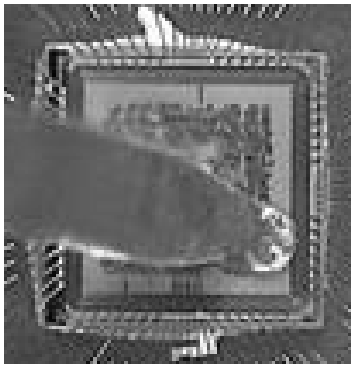

図 3: 測定時のプローブ位置

実験に用い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．計測は，開封したチップの近傍に設置した磁界プローブを用いて行った．　計測器の詳細を表 1 に示す．オシロスコープのサンプリング周波数は 25 GSa/s，TEG チップのクロック周波数は 24 MHz とした．図 3 に示すように，測定時のプローブ位置は図 2 の SRAM のほぼ真上とし，プローブの先端にあるコイルを，チップの絶縁膜に触れるまで降ろして行った．

SRAM アクセス時のリークは，データとアドレスのリークが複合したものとなるため，実験ではそれらの影響を分離できるようなテストベクタを適当に選択した．また，テストベクタ当たり 1,000 波形ずつ測定を行い，その平均波形を用いて評価を行った．

2.3　データ依存性

以降の解析では，波形のうち，特定の時刻(POI: Point of Interest)のデータを抽出して解析するということを行う．POI は，全て基本的に SRAM アクセス中のグループ毎の平均波形間のばらつきが最大となる時刻とした[9]．図 4 に，例として，リードのデータ依存性の POI と，POI 付近の波形を示す．図 4(中)はグループ毎の平均波形の重ね合せ，図 4(下)は各グループの平均波形と全波形の平均波形の差分の重ね合せである．

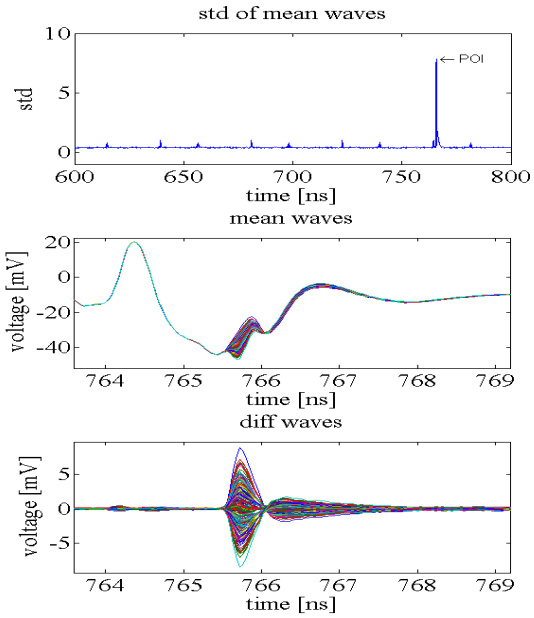

図 4: 平均波形間の標準偏差(上)，および POI 付近の平均波形の重ね合せ（中)と差分波形の重ね合せ(下)

まず，リードとライトのデータ依存性を調べる．結果を図 5,6 にそれぞれ示す．これらは，横軸に読み出した（または書き込んだ）データの整数値，縦軸に対応する平均電圧値をプロットしたものである．これは，Collision Power Analysis において相関を求める対象と

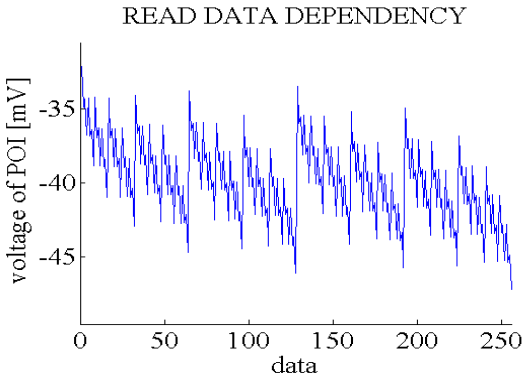

図 5: データ依存性（リード）

図 6: データ依存性（ライト）

なるデータに等しい．また，これは，実測に基づいて電力モデルを推定した結果と解釈することもできる．図は横軸がグループ分けしたデータで，縦軸は POI における各グループの平均電圧値である．極性は逆になっているが，リード・ライトともに類似したパターンの繰り返しが現れている．このような形はハミングウェイトモデルが強く成立することを示唆する．図 7,8 は横軸を各グループのデータのハミング重みとして，図 5, 6 をプロットしなおしたものである．この図から，SRAM のサイドチャネル情報のデータ依存性は主にデータのハミング重みによることがわかる．従って，サイドチャネル情報のデータ依存性 L_{data} は，(1)式のようにモデル化できることが確認できた．

$$L_{data} = k * \mathrm{HW}(data) + bias \quad \cdots (1)$$

ここで，k は比例係数，$data$ はリード・ライトのデータ，HW(X)は X のハミング重みである．これは，既存の結果と同様のものである．

2.4 アドレス依存性

次に，リードとライトのアドレス依存性を調査する．結果を図 9,10 にそれぞれ示す．これは，図 5，6 と同様の図を，データではなくアドレスで行ったものである．図は横軸がグループ分けしたアドレスで，縦軸は POI における各グループの平均電圧値である．ただし，アドレスは 9 ビットあるため，0 から 511 まで表示している．リード・ライトともに全体的には大きく右下がりになっ

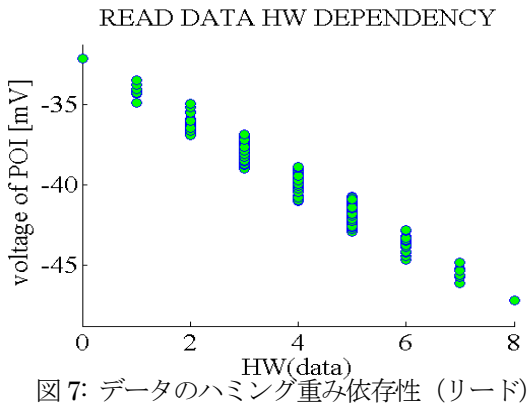

図 7: データのハミング重み依存性（リード）

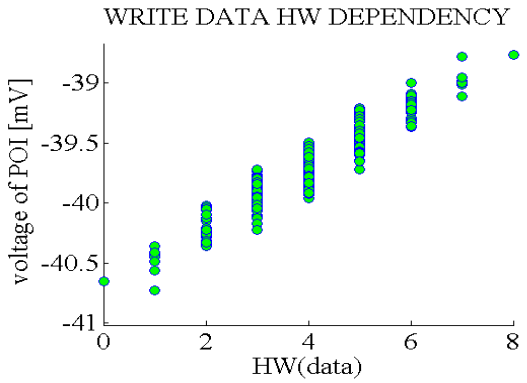

図 8: データのハミング重み依存性（ライト）

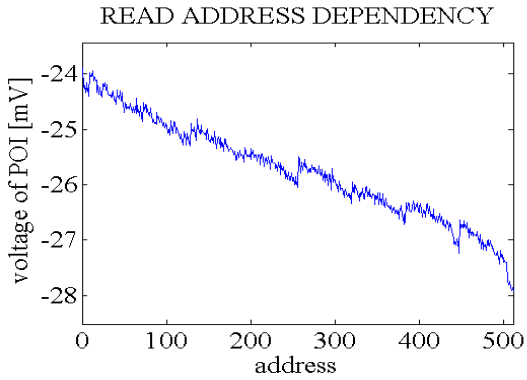

図 9: アドレス依存性（リード）

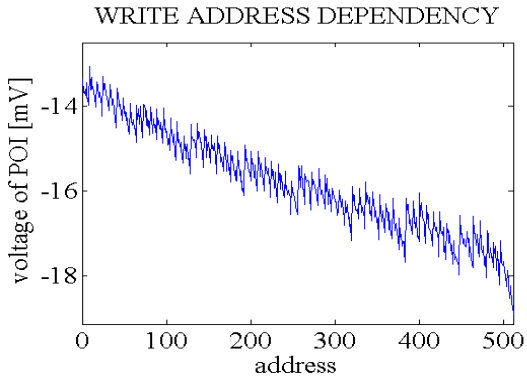

図 10: アドレス依存性（ライト）

ている．この結果は，図 5, 6 のデータ依存性の実験結果と大きく異なっており，アドレスでは，ハミング重みと異なるモデルが成立することを示唆している．図 9, 10

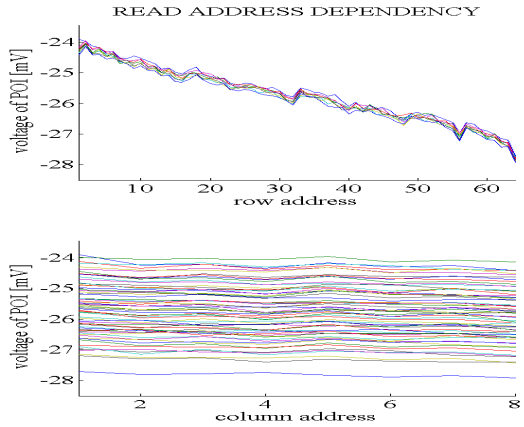

図 11: 行／列アドレス依存性（リード）

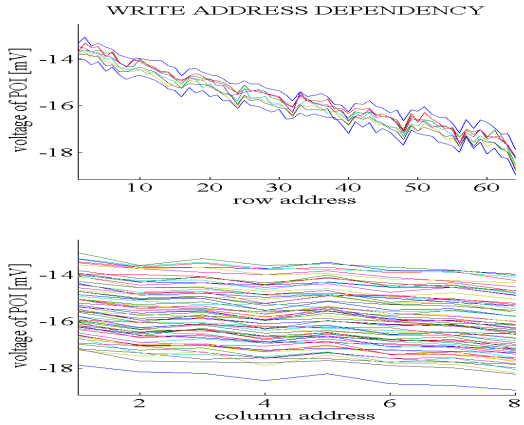

図 12: 行／列アドレス依存性（ライト）

をさらに詳しく観察すると，64 回分の細かい繰り返しパターンが現れていることが分かる．これは，2.1 節で述べた行アドレスが 6 ビットでアドレスの総数 2^6=64 と一致する．そこで，行アドレスと列アドレスについて個別にプロットしなおした（図 11,12）．この結果から，サイドチャネル情報は行アドレスと列アドレスそれぞれとの依存性を持つことが分かる．図 9,10 は両依存性が複合したもので，64 個の細かい繰り返しパターンは，行アドレス依存性が現れたものである．一方，行アドレス依存性の図には，列アドレスに依存しない 8 つの繰り返しパターンが確認できる．これは，行アドレスの上から 3 ビット目の関与が特に強いためと考えられるが，現時点ではその理由は不明である．

アドレス依存性の図に現れた傾向は，アドレスの「整数値」とサイドチャネル情報の間に，線形に見える関係があることを表している．これは，行アドレスと列アドレスのそれぞれについても言える．また，アドレス依存性には，データ依存性ほど顕著ではないが，ハミング重み依存性も含まれることが図から確認できる．従って，サイドチャネル情報のアドレス依存性 L_{adr} は次の式(2)でモデル化できる．

$$L_{adr} = k_0 * \mathrm{int}(R\_adr) + k_1 * \mathrm{HW}(R\_adr) + k_2 * \mathrm{int}(C\_adr) + k_3 * \mathrm{HW}(C\_adr) + bias \quad \cdots (2)$$

ここで，k_n は比例係数，R_adr，C_adr data はそれぞ

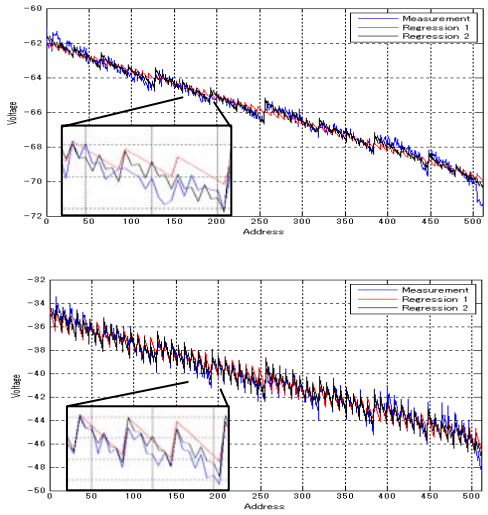

図 13: アドレス依存性のモデル化（上:リード，下:ライト）

れ行アドレスと列アドレス，HW(X)はハミング重み，int(X)は整数値を表す．本モデルの妥当性を検証するために，図 9, 10 のグラフに，(2)式をフィッティングする．具体的には，計測データを元に，(2)式の比例係数 k_0-k_3 と bias を，重回帰分析で求めるということを行った．図 9,10 に合わせてフィッティングして L_{adr} をプロットした結果を図 13 に示す．図の青線は実チップの結果，黒線が(2)式によるフィッティング結果，赤線は(2)式からハミング重みの項を除いてフィッティングした結果である．図には一部の拡大図も示したが，線形の項のみを用いた赤線も実チップの結果を良く近似している．さらに，ハミング重みを加味することでより実チップの結果と一致することがわかる．攻撃者の視点からは，以上の結果より，式(2)を電力モデルとして使用することで，電力モデルを使用する攻撃(CPA や MIA)を高精度化できる可能性がある．その場合，プロファイリングにより k_0-k_3 を求めることもできるし，プロファイリング無しで，k_0=1, k_1=k_2=k_3=$bias$=0 と近似する場合でも，ハミングウェイトモデルよりもよく当てはまる可能性がある．

サイドチャネル情報とアドレスの値の間に線形な関係が現れる原因は判明していないが，等間隔に並んだワード線やビット線の距離関係が何らかの関与をしている可能性がある．線形性に関するもう 1 つの興味深い結果を図 14 に示す．この図は磁界プローブ位置を 0.1mm ずらして測定を行い，同じ POI での行／列アドレス依存性（ライト）を図 12 と同様に表示したものであるが，行アドレス依存性の傾きが図 12 と逆になっている．この結果は，特定の信号ラインを流れる電流が，アドレス依存性と深く関っていることを示唆している．

3 Collision Power Analysis

前節の冒頭で述べた通り，異なる SRAM アクセスでアドレスやデータのコリジョンが検出されると脅威にな

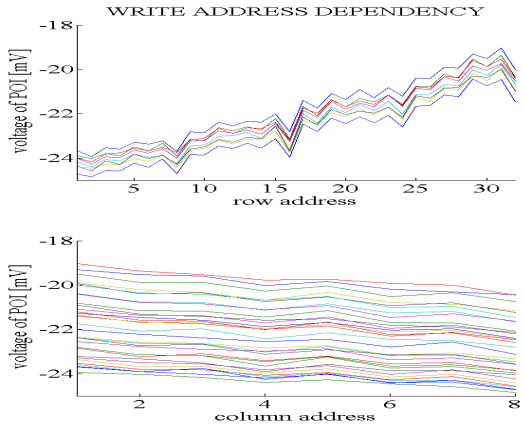

図 13: 異なるプローブ位置での行／列アドレス依存性（ライト）

り得る．本節では前節で示したサイドチャネル情報のアドレス依存性やデータ依存性を利用したコリジョン検出可能性に関する基礎実験結果を示す．実験環境は前節のものと同一である．

3.1　アドレスコリジョン

アドレスコリジョンの基礎実験として，列アドレスの最上位ビットを 1 に固定した 256 ワード分の各アドレスに 0 と 255 のデータを読み書きする 2 つの波形セット（アドレス毎に 1,000 波形分の平均波形）を用意し，波形セット間の SRAM アクセスタイミングの波形形状の相関をアドレス毎に評価した．具体的には，POI を含む同じ時間区間の 2 つの波形データ同士の相関係数を計算し，アドレスの組別にその値の分布を調査した．POI における平均電圧値のみを用いなかったのは，時間軸上の 1 点だけでは，ノイズなどの影響により，コリジョン検出が極めて困難であったためである．図 14 にライト同士のアドレスコリジョン評価結果を示す．図 14(上)は，横方向が対象アドレス（0 のデータをライト），縦方向が候補アドレス（255 のデータをライト）で，波形セット間の波形形状の相関係数を表したものである．高い相関係数ほど濃い暖色で表現している．図の左上から右下への対角線上に濃い暖色が集中するほど，2 つのアドレスが等しい，または近いことが識別し易くなる．また，図 14(下)は相関係数の確率分布を示すもので，横軸は相関係数，縦軸は確率密度である．青線は，アドレスが一致する 256 通りの組合せの相関係数の分布，赤線はアドレスが一致しない 65280 通りの組合せの分布である．どちらからも，アドレス一致時の相関係数は高い値に集中しており，ライト同士のアドレスコリジョン検出が現実的な脅威になり得る可能性がある．これは，前節で示したアドレス値とサイドチャネル情報間の線形な相関が大きく関係している．

紙面の都合により省略するが，リード同士のアドレス

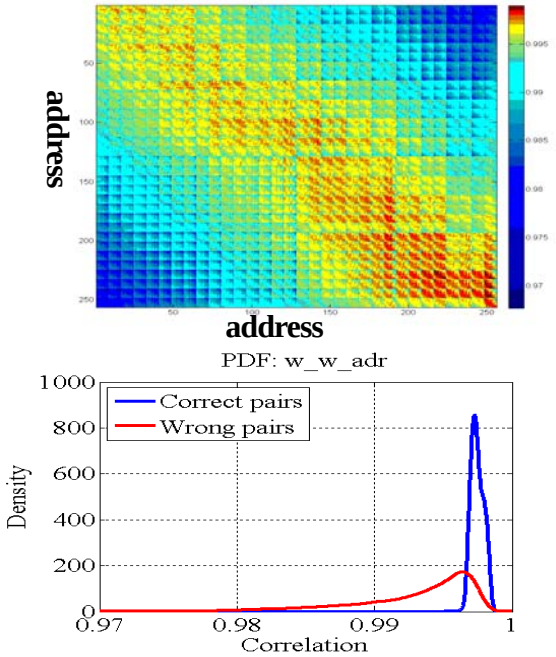

図 14: ライト同士のアドレスコリジョン評価結果(上:相関係数マトリックス，下:相関係数の確率密度)

コリジョンも上記とほぼ同様の結果であった．また，リード・ライト間については，TEG チップはリードとライトで波形形状や POI における平均電圧値が大きく異なっていたため，今回の方法では，コリジョン検出はほぼ不可能であった．

3.2　データコリジョン

データコリジョンについてもアドレスコリジョンとほぼ同様の基礎実験を行なった．アドレス空間の先頭と末尾に，0 から 255 の各データを読み書きする 2 つの波形セット（アドレス毎に 1,000 波形分の平均波形）を用意し，波形セット間の SRAM アクセスタイミングの波形形状の相関をデータ毎に評価した．図 15 にライト同士のアドレスコリジョン評価結果を示す．

図 15 の見方は，図 14 と同様である．前節で示したように，サイドチャネル情報のデータ依存性は，主にデータのハミング重みとの相関であるため，ハミング重みが近いデータ同士の区別が非常に困難であることが図から分かる．ライト同士のデータコリジョンもほぼ同様の結果であった．また，リード・ライト間はアドレスコリジョンと同様に，今回の方法では，コリジョン検出はほぼ不可能であった．

4　Dual-Rail RSL メモリ方式を適用した AES 暗号回路に対する攻撃

文献[7]で提案された AES 暗号回路は，AES の Sbox を Dual Rail RSL メモリとしてとして実装している．Dual Rail RSL メモリは，アドレスやデータに依存したリークを防ぐことを目的として，入力アドレスのランダ

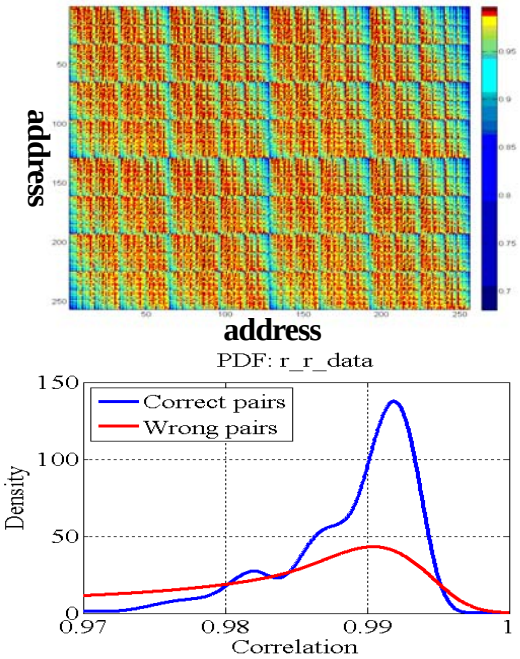

図 15: リード同士のデータコリジョン評価結果(上:相関係数マトリックス，下:相関係数の確率密度)

ムマスク，及び ROM 内の 2 線化により，DPA 耐性の向上を図ったものである．なお，SRAM ではなく ROM であるが，図 1 に示したような，行・列構造を有する．本節では，我々が設計・試作を行った文献[7]のチップを用い，SRAM のアドレス依存性評価と AES の鍵探索を行なった結果を報告する．このチップの Dual Rail RSL メモリの行アドレスは 6 ビット，列アドレスは 2 ビットである．評価対象の AES 暗号回路は，16 個の Sbox に対応する 16 個の Dual Rail RSL メモリを有する．計測器は 2.2 節で示したものと同じである．

4.1　アドレス依存性

まず，Dual Rail RSL メモリのアドレス依存性を検証する． 計測した 20,000 枚の計測波形に対し，これまでと同様の方法で POI を定めた．その後，POI における電圧値を，（鍵が既知の条件の下で）SubBytes 入力でグループ分けして平均値を求めた．それは，SubBytes 入力が Dual Rail RSL メモリのアドレスに入力されるためである．

図 16 に，16 個ある Dual Rail RSL メモリのうち 1 つに関するアドレス依存性評価結果を示す． 4 つのノコギリ上の大きな繰り返しパターンが確認でき，その周期は 64 である．このようなパターンは，アドレスの上位 2 ビットによって引き起こされており，それは前述の通り列アドレスに対応する．一方，下位 6 ビットについては，（ハミング重みではなく）整数表現した値と線形であることが分かる．この結果は，列アドレス依存性は無いものの，2.4 節の結果と良く整合する（これまでの結果とのグラフの見えの違いは，行アドレスと列アドレスのい

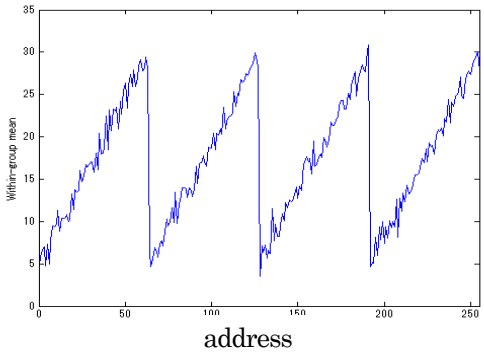

図 16: 1 つの Sbox のアドレス依存性

ずれが最上位ビット側かのエンコードの違いによる）．行アドレスの整数表現は，選択されたワード線の物理位置となっており，電磁波解析によって活性化されたワード線の情報がリークしていると判断できる．また，列アドレス依存性が無いのは列アドレスでは，ビット線上に並列に読みだされたデータを局所的なコラムデコーダで選択しているだけで，メモリアレイの動作は列アドレスに依存していないためであると考えている．

2.4 節の通常の SRAM の実験結果で列アドレス依存性があったのは通常の SRAM ではアドレス線の充放電依存性があるためであると考えられる．一方 Dual Rail RSL メモリでは入力アドレスには乱数マスク，メモリ内のデコーダ回路では， 2 線相補動作が行われ電力の均一化が行われているため，電磁波解析によって，メモリアレイの動作だけを理想的に抽出できたのではないかと考えられる．

以上は，ある 1 つの Sbox の結果であるが，多くの Sbox で同様の傾向が確認できている．ただし，別の Sbox では，図 17 に示すように極性が逆転する．これは，2.4 節の最後で示した現象と極めて類似しており，磁界プローブのコイルと Sbox の位置関係によるものと考えられる．

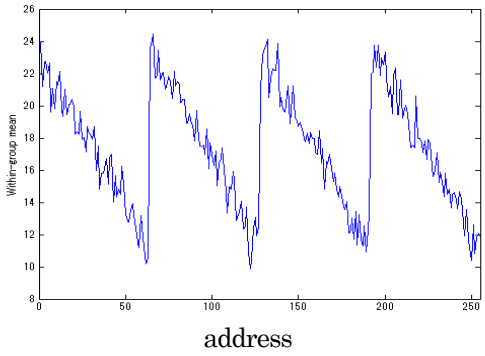

図 17: 別の 1 つの Sbox のアドレス依存性

4.2　鍵探索結果

鍵が未知の条件で CPA を適用し，鍵抽出を行った．その際，プロファイリングは不可能だが SRAM の構造について事前知識を持つ攻撃者を想定し，従来とは異な

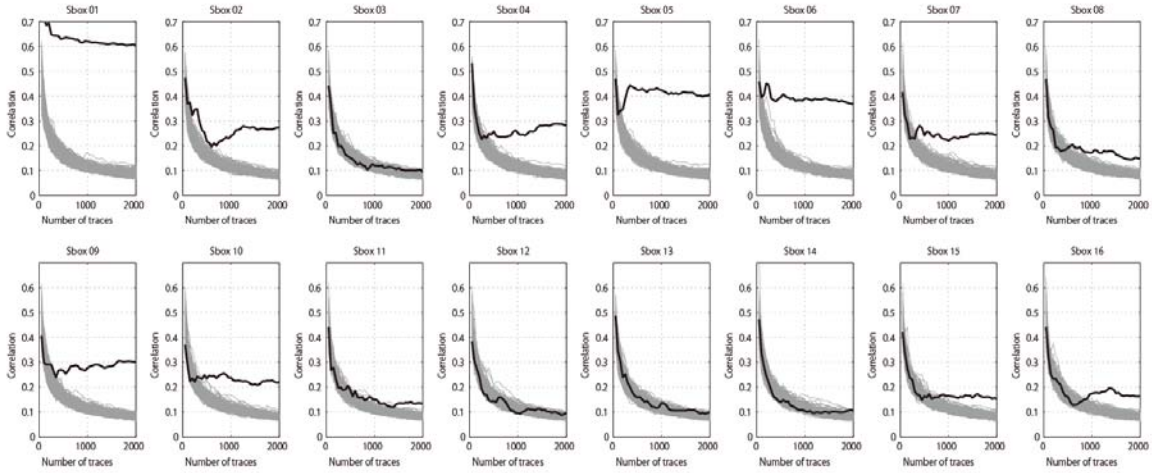

図 17: 10 ラウンド目の解析における，波形数と相関値の遷移．黒線：正解鍵，灰線：その他

る電力モデルを使用した. すなわち, (2)式において, k_0=1, k_1=k_2=k_3=*bias*=0 とするモデルにより予測電力値を算出した．10 ラウンド目の鍵探索を行なった結果を図 17 に示す．図は，16 個の Sbox に対応する MTD グラフである．灰色が誤った予測，黒色が正しい予測における相関値である．横軸は波形数であり，その変化に応じた相関値の遷移を表現している. 図より, 攻撃が成功しており, 正しい候補が，ほかの候補から識別できている様子が読み取れる．また，極めて高い相関を得ており，およそ 1,000 波形で全体の半数のバイトが識別できている．Sbox によって難易度が大きく変化する挙動については, 磁界プローブと Sbox の相対位置関係によるものと考えられる.

攻撃が成功したのは，4.1 節で示した Dual Rail RSL メモリのアドレス依存性による. ROM による Dual Rail RSL メモリでも，2.4 節の SRAM と同様の結果が得られたことから，このアドレス依存性が，行・列によるメモリ構造に起因するものと考えられる.

5　まとめ

本稿では，SoC で広く利用される IP コアの 1 つである SRAM のサイドチャネル評価を行った. 評価の結果, SRAM のサイドチャネル情報はアドレスやデータと特徴的な相関を示し，特に，アドレスについては，行アドレスと列アドレスそれぞれの値と線形な，従来知られていない依存性が存在することを確認した．これは，メモリマクロの規則正しい行列構造に起因するものと考えている．システムによってはこの点に注意をした設計が必要である．今回発見したリークの，既存対策法への影響も検討する必要がある.

今後は今回用いた SRAM 以外の SRAM の評価や，攻撃に使える波形数と攻撃成功確率の関連などを調査していく予定である.

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] 佐伯,鈴木,菅原 “オープンソース CPU のサイドチャネル評価,” 2009 年暗号と情報セキュリティシンポジウム, SCIS2009

[2] E. Konur, Y. Özelçi, E. Arikan, and U. Eksi, “Power analysis resistant SRAM” , WAC 2006.

[3] S. Shah, R. Velegalati, J.P. Kaps, D. Hwang, “Investigation of DPA Resistance of Block RAMs in Cryptographic Implementations on FPGAs”, ReConFig 2010.

[4] E. Prouff, M. Rivain, “A generic Method for Secure SBox Implementation”, WISA 2007.

[5] H. Maghreb, E. Prouff, S. Guilley, and J.-L. Danger, “A First-Order Leak-Free Masking Countermeasure”, CT-RSA 2012.

[6] M. L. Akkar, C. Giraud, “An Implementation of DES and AES Secure against Some Attacks”, CHES 2001.

[7] 橋本,岩井,汐崎,淺川,鵜飼,藤野, “Dual-Rail RSL メモリ方式を適用した AES 暗号回路の設計および DPA 耐性評価,” 2012 年暗号と情報セキュリティシンポジウム, SCIS2012

[8] N. Hanley, H. Kim, and M. Tunstall, “Exploiting Collisions in Addition Chain-based Exponentiation Algorithms”, Cryptology ePrint Archive, Report 2012/485, 2012-08-22

[9] A. Moradi, O. Mischke, and T. Eisenbarth. Correlation-Enhanced Power Analysis Collision Attack. In CHES 2010, volume 6225 of LNCS, pages 125–139. Springer,2010.