第4章

# システムLSI設計におけるDPA対策の指針とAES暗号の対策例

## —— 対策の有効性と回路コストのバランスをじょうずにとる

森岡澄夫

**暗号処理回路は，それ単体で1チップ化されることは少なくなり，今日ではシステムLSIに組み込まれて使われる場合が大半です．システムLSIの実装には，FPGAを使うケースもありますが，通常はスタンダード・セル（セル・ベースIC）を使います．また，暗号の種類について，電力解析の学術論文では旧来のDES（Data Encryption Standard）がよく使われていますが，実務ではAES（Advanced Encryption Standard）などへ移行しています．本稿では，こうした動向を受け，一般のシステムLSI設計における電力解析攻撃への対策方針と，システムLSI上のAES暗号回路の攻撃対策法を紹介します．（著者）**

電力解析攻撃[注1]は，暗号回路実装の研究において，ここ数年ホットな話題です．暗号数理の高度な知識や高価な機器を用いなくても攻撃可能という点で驚くべきテーマであり，暗号研究者以外の人にも比較的知られるようになってきました．

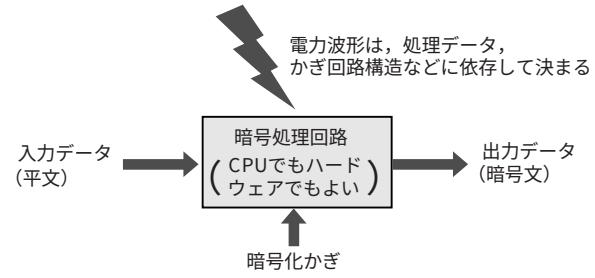
## 1 実設計時の電力解析攻撃と対策

ここで，電力解析攻撃について簡単におさらいします（**図1**）．おおかたの回路では，その動作中の電力波形は，処理するデータの値や回路構造に依存して決まります．この性質を利用し，電力波形の測定結果から，暗号回路にセットされているかぎ（これもデータの一種）を推定するのが，電力解析攻撃です．

### ● 学術論文と通常のLSIには多くのギャップがある

言うまでもなく，学術論文と通常のシステムLSIの間には，設計条件などにかなりのギャップがあります（**表1**）．学会で発表される攻撃対策法（以下，単に対策法）には，コストがかかり過ぎたり，あるいはシステムLSI設計の観点からは非現実的であったりする場合があります．攻撃に過度におびえて回路コストを不必要に跳ね上げる対策法を使うのも，逆に，すっかり無関心になって何も対策しないのも，どちらも好ましくありません．

通常のシステムLSI設計でどう対策に取り組むべきか，確立された方法論はまだありません．本稿では，筆者の私見を記します．あくまで，個人的な見解ですので，みなさんが自分の設計に適用するときは，よく吟味し直してください．




- データ値と電力波形から，かぎを推定
- 波形は電流計で直接測ってもよいし（SPA，DPA），電磁波で間接的に測ることも可能（EMA，DEMA）
- 処理時間の変化から，かぎがわかる場合がある（タイミング・アタック）
- 1回の演算処理波形から，かぎがわかる場合がある（SPA，EMA）
- 多数回の演算処理の平均波形から，かぎがわかる場合がある（DPA，DEMA）

**図1　電力解析攻撃の概要**

**暗号処理回路（CPUでも専用回路でもよい）の電力波形が，入力データやかぎ，回路構造などに依存することを利用して，電力波形からかぎの値を推定する．どのような方法で推定するかは，いろいろバリエーションがある．**

注1：本稿では，SPA（simple power analysis），DPA（differential power analysis），EMA（electromagnetic analysis），DEMA（differential electromagnetic analysis）などを総称して「電力解析攻撃」と呼ぶことにする．

**表1　研究レベルと通常のシステムLSI設計のギャップ**

**電力解析攻撃と対策の研究が盛んだが，学術研究は自由な仮定のもと，さまざまな手法を探るものなので，通常のシステムLSI設計の条件とはギャップがある．一般的なシステムLSIにはとても使えない手法の提案も多いが，LSIの設計ルールも攻撃手法も時代とともに変化するので，「研究は役に立たない」と全部無視してしまうのは危険．なお，現時点において，90nmなどの微細プロセスで製造したシステムLSIを，実際に電力解析攻撃できたという報告は，筆者は聞いたことがない．防御法についても，当然ながら完ぺきなものは存在しない．**

| | 研究レベルの話 | 通常のシステムLSI | 備　考 |
|---|---|---|---|
| 暗号回路のサイズ | チップ全体または大半 | ごく一部 | システムLSIでは，暗号回路の消費電力は，ほかの回路のそれに隠されてしまいがち |
| デバイス | FPGAもしくは旧プロセスで評価（0.5 μm～0.25 μmなど） | 最新のものは90nm～65nmの設計ルールで製造 | 微細化すると，消費電力もチップ上の面積も小さくなるので，攻撃は難しくなる |
| テクノロジ・ライブラリ | 暗号部には専用のセル・ライブラリが使える | 暗号部だけ別ライブラリで設計することは，まず不可 | — |
| 回路の設計抽象度 | どれだけ下位でも可（トランジスタ・レベルなども可） | 通常はRTLが最下位．今後は，ビヘイビア合成の利用も考えられる | — |
| 非同期論理回路 | 使用可能（dual rail方式など） | 原則，使用不可 | — |
| 回路の処理クロック数 | 動的にランダムに変えてよい | 原則，固定したい | システム処理性能が予測不能では困る |
| データ（平文，暗号文）の観測 | 暗号IPの入出力データ値を，外部で観測できる．または外部から制御できる | 暗号IPの入出力は，外部から観測も操作もできない場合が多い | データ値が不明でも攻撃可能な場合がある，との報告が最近あった |
| 暗号のかぎ設定 | 一度セットしたら，ずっと同じ値のままと仮定する | システムによっては，どんどんかぎを切り変えてもよい場合がある | DPA，DEMAにおけるかぎ導出には，同一かぎで，数百回以上の暗号処理が必要 |
| 電力の測定精度 | どのような微小電力，高速変化でも測定可と仮定する | 微小，または高速な変化は，安価な装置では測定不能 | — |

## ● 電力解析攻撃はシステムLSIにとって脅威なのか？

システムLSIといっても多種多様であり，電力解析攻撃が脅威なのかどうか，断定的に“Yes”，“No”を言うことはできません．しかし，少々粗い議論ですが，以下の条件をいくつか満たすならば，今すぐの脅威とはならないでしょう．

- **90nmや65nmといった最近の微細プロセスのスタンダード・セルを使っている**―― 微細プロセスでは，暗号回路の平均消費電力は数百μW～十数mWのオーダになり，しかもリーク電流などの割合が高い．電力解析攻撃に使えるのはゲートのスイッチング動作による消費電力のうち，データ値に依存して変わる電力差であるが，それは数μW～数百μWといった微小なものになる[注2]．
- **暗号処理部が回路全体のごく一部である（図2）**―― 全体の消費電力から暗号処理の分を抽出するためには，多量のデータ・サンプリングが必要になる．
- **暗号演算を専用回路で行っている**―― CPUで行っているならば攻撃されやすいかもしれない．一般に，プロセッサ処理は電力解析攻撃に弱いという傾向がある．
- **かぎを頻繁に変更している**―― DPAやDEMAでは，同じかぎのままで，暗号演算を最低数百回はサンプリングする必要がある．
- **暗号処理がいつ行われているかを正確に（クロック精度で）とらえることが難しい**―― これがわからないと，どの時点の電力波形をサンプルしてよいかわからず，攻撃できない．ただし，暗号処理実行のタイミングを割り出すような方法の研究も行われている．
- **暗号処理の入出力データ値（平文や暗号文）をチップ外部から直接観測できない，もしくは外部から制御できない**――ただし，それでも適用できる攻撃法の研究もある．

以上の条件から大きく外れる場合，電力解析攻撃は脅威となりえます．もちろん，ある製品に搭載したシステムLSI

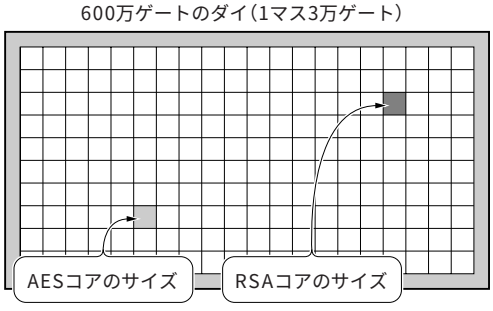



**図2　一般的なシステムLSIでは，攻撃の対象となる暗号IPは全体のごく一部でしかない**

**電力解析攻撃のターゲットは，AESやRSAといった暗号処理部である．CPUでなく専用回路で暗号演算を行う場合，どのような暗号でも2万～4万ゲート程度の回路規模なので，システムLSI全体のうち，図に示す程度の割合しかない．また，65nmや90nmといった微細なプロセスでは，暗号回路の平均消費電力は数百μW～十数mWしかない．したがって，暗号処理を専用回路で実行しているかぎり，電力解析攻撃は現状では相当難しく，今後はさらに難易度が上がる傾向にある．ただし，CPUで暗号演算を行ったり，FPGAを使ったり，あるいは古いプロセスを使うならば話は別である．**

注2：しばしば誤解されるが，「微小電力だから攻撃できない」ということではない．十分に精密な電力測定環境を用意し，十分に多量のデータ・サンプリングを行えるならば，攻撃そのものは可能である．そのためにかかるコストが現実的なものかどうかが，脅威か否かの判定基準である．