C-006

電力解析攻撃における S-Box のハミング距離と消費電力の関係の調査
Investigation of the Relationship between S-Box Hamming Distance and Power Consumption in Power Analysis Attack

長友 泰樹† 請園 智玲‡
Taiki Nagatomo Tomoaki Ukezono

1. はじめに

インターネット通信における暗号鍵を狙った攻撃として，サイドチャネル攻撃が挙げられる．サイドチャネル攻撃とは，サイドチャネルと呼ばれる計算機の消費電力や計算時間などの物理的な情報を用いて計算機内部の秘匿情報の盗聴を試みる攻撃である．

また，サイドチャネルとして計算機の消費電力に着目した攻撃を，電力解析攻撃と呼ぶ．本研究は，AES[1]の暗号鍵を狙った電力解析攻撃に着目する．

電力解析攻撃の代表的な手法として，相関電力解析（CPA：Correlation Power Analysis）が挙げられる[2]．CPA は，攻撃対象とするデバイスに入力されるデータのハミング距離と動的消費電力との相関を用いて暗号鍵の取得を試みる手法である． AES は暗号処理に S-Box と呼ばれる換字処理を実現する 8 ビット入力 8 ビット出力の非線形変換モジュールを用いる．S-Box は電力解析攻撃に対する脆弱性に起因する暗号鍵の漏えいが指摘されている[2].

本研究の目的は，ASIC 実装時の S-Box の動的消費電力と入力データのハミング距離の関係を実際の LSI 設計用 EDA を用いて明らかにすることである．45nm のプロセスルールで設計した S-Box の消費電力とハミング距離の関係を調べることで，CPA が解析する電力が実際の LSI チップでどの程度の消費電力であるのかを確認するとともに，各ハミング距離での消費電力はどのような傾向を示すのかを調査し，その結果からハミング距離による電力消費傾向を意識したサイドチャネル攻撃対策を提案する．

2. 実験方法

本節では，本研究の実験方法を示す．

2.1 RTL 設計

ASIC 評価を行うために S-Box を専用回路として Verilog HDL を用いて設計した．本稿評価では合成体 S-Box とテーブル参照型の S-Box の 2 つの S-Box を設計し，実験に用いた． S-Box は既約多項式$x^8 + x^4 + x^3 + x + 1$のガロア体 GF(2^8)を入力の要素と見做し，その乗法逆元を求め，アフィン変換を出力する処理である．合成体 S-Box は同じ要素数のガロア体が同形である特性を用いて乗法逆元を GF(((2^2)^2)^2)へ同形写像して演算することで実現することができ，回路設計においては，乗算要素を GF(2^2)の乗算器を組み合わせることで設計できる．一方，テーブル参照型は入力に対する出力の対をテーブルとして定義し，S-Box の演算を省略して回路出力する設計手法である．これを Verilog HDL で設計する際は case 文として 256 の入力パターンに対し 256 の出力パターンを記述することで実現できる．本稿の評価では，この 2 種類の S-Box 実装で暗号化時に使用する S-Box と復号時に使用する S-Box^{-1} を実装した．

2.2 S-Box への入力データの生成

CMOS の動的消費電力は出力が 0 から 1 または 1 から 0 に変化する際に発生するため，動的消費電力の計測には時系列に入力を変化させる電力計測用のデータ列を用意する必要がある．このため，本稿評価における消費電力評価で S-Box 回路に入力されるデータは，時系列に並べた 1 回の入力が 8 ビットのビット列の集合として構成される．この入力データの構成時に，時系列で隣り合うデータのハミング距離を一定にすることで，指定されたハミング距離における消費電力を計測できる．本稿評価ではこの入力データを構成するためにハミング距離を指定して入力データ列を生成するプログラムを作製した．図 1 に生成される入力データの例を示す．図 1 では，3 つの入力データが上から下に時系列に並べられている．1 番目のデータと 2 番目のデータは黄色のブロックのビット位置のみが反転し，2 番目と 3 番目のデータは緑の位置で反転している．この黄色／緑の位置をプログラム中でランダムに指定することにより，ランダムな一定ハミング距離の入力データの生成を実現した．本稿実験ではこの時系列の入力数を 10,000 とし，ハミング距離 1～8 の各指定で入力データを作製した．

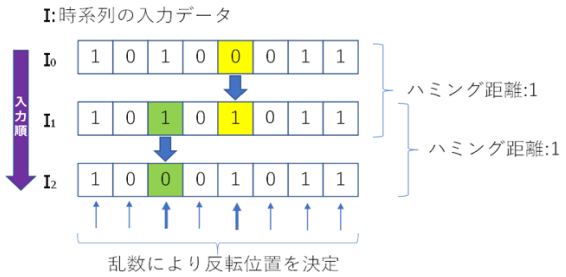

図 1 ハミング距離を 1 に指定した入力生成

2.3 Power Compiler を用いた電力測定

S-Box 回路の電力測定には Synopsys 社の Power Compiler を用いた．Power Compiler は同社の ASIC 向け論理合成ツールである Design Compiler に組み込まれる電力評価ツールである．Design Compiler はターゲットのプロセスで製造するためのセルライブラリを用いて入力である RTL を論理合成した結果のネットリスト出力する EDA であり，Power Compier は生成したネットリストを対象に電力シミュレーションをすることができる．LSI の電力消費の特性は製造プロセスと ASIC のセルライブラリ内部の設計に依存する．このため，実際の LSI を設計するためにセルライブラリ内部に記録された電力消費の情報を活用した Power Compiler は，高精度で RTL で設計した回路の消費電力を論理合成時に見積もることができる．本稿評価では，セルライブラリに 45nm のオープンセルライブラリを使用した．Power Compiler は動的消費電力を見積もるために Switching Activity Interchange Format (SAIF)ファイルを必要とする．この SAIF ファイルは 2.2 節の入力データを使ったテスト

† 福岡大学大学院　工学研究科
Graduate School of Engineering, Fukuoka University
‡ 福岡大学　工学部
Faculty of Engineering, Fukuoka University

ベンチを Synopsys 社の VCS でシミュレーションし，作成した．

3. 実験結果とサイドチャネル攻撃対策設計

本節では，2 節で説明した 2 つの S-Box 回路の電力評価の結果を示し，ハミング距離に着目したサイドチャネル攻撃耐性をもつ S-Box 設計の考察を示す．

3.1 消費電力評価

図 2，図 3 にそれぞれ合成体 S-Box，テーブル参照型 S-Box の電力評価の結果を示す．横軸は入力データ間のハミング距離，縦軸は動的消費電力を示し，青色の線が S-Box，橙色の線が S-Box^{-1} のグラフを示す．

消費電力評価の結果，消費電力の最大値は合成体 S-Box が約 845uW と大きく，テーブル参照型の S-Box は 636uW と小さい観測結果が得られた．また，各実装において S-Box と S-Box^{-1} は，ほぼ同じ電力消費傾向を示した．ハミング距離に対する電力消費の傾向に関して，合成体 S-Box はハミング距離が 1～4 の間は消費電力に大きな差が見られるが，5～8 の間では消費電力が飽和傾向にあり，差が小さくなっていることがわかる．一方，テーブル参照型の S-Box は合成体 S-Box に比べグラフがリニアに変化しており，ハミング距離の変化分の消費電力差がはっきりと確認できる．

CPA は，各ハミング距離と消費電力の相関を解析する攻撃手法である．本稿の評価は EDA によるシミュレーションベースの評価であることから，計測時の誤差やノイズが含まれない．これをふまえ，テーブル参照型の S-Box の方が 1～8 のハミング距離の全域で他のハミング距離と消費電力の関係をはっきりと区別して確認することができるため，実際の攻撃時に誤差やノイズの影響を受けて計測・解析を試行しても高い相関が得られると考えられる．他方，合成体 S-Box では，CPA の攻撃時に 5～8 のハミング距離を与えた後の電力測定で差が分かりづらく，誤差やノイズの影響を大きく受けて相関が低くなると考えられる．

以上のことから，ASIC 実装時の S-Box の実装方法により，電力解析攻撃に対する耐性が異なることが確認できた．

3.2 サイドチャネル攻撃耐性を持つ S-Box 設計考察

CPA はハミング距離と消費電力の関係をもとに相関を求め，内部情報を推測する攻撃手法である．このことから，図 2 や図 3 の電力消費のグラフが平滑化され，平坦なほど相関を求めることが困難になるといえる．

もし，ハミング距離による電力消費の傾向が図 2 または図 3 グラフの形状を逆写像にする組み合わせ回路を設計できれば，その回路を従来の S-Box と並列に配置し，同じ入力を同時に与えることで消費電力が合成され，グラフの平滑化が実現できる．例えば，ハミング距離 1 を 7 に変換，ハミング距離 3 を 5 に変換するようなデータコンバータを設計し，その出力を S-Box^{-1} の入力に選択的に与え，本来同時には駆動しない S-Box と S-Box^{-1} を同時に駆動させることで，暗号化処理時に電力消費を合成して平滑化する回路を構成することができる．また，復号の処理の場合は S-Box の入力にも同様にデータコンバータを接続することで，無駄な追加回路を極力削減しながら，暗号化と復号の両処理でサイドチャネル攻撃耐性を得ることができる．今後の研究ではこの回路構成を実際に設計し，評価していく．

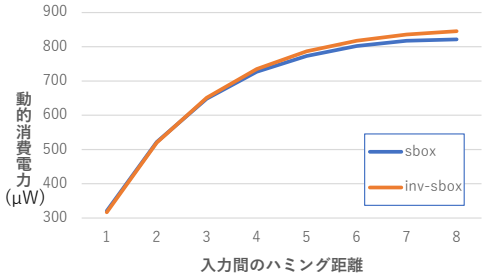

図 2 合成体 S-Box の電力評価

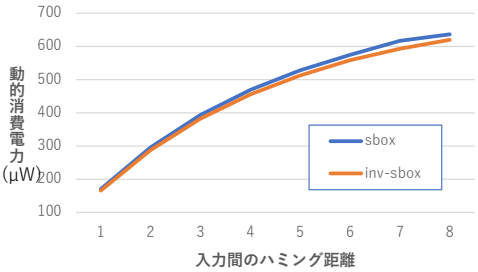

図 3 テーブル参照型 S-Box の電力評価

4. おわりに

本稿では，入力データ間のハミング距離を用いて，S-Box 回路の動的消費電力を測定した．測定の結果，上述のハミング距離と S-Box 回路の動的消費電力に明確な関係があり，合成体 S-Box の方がテーブル参照型 S-Box に比べ，5～8 のハミング距離の間で，高い耐タンパ性が確認された．

また，本稿では，ハミング距離と消費電力の関係の平滑化による，サイドチャネル攻撃への耐タンパ性向上に言及した．加えて，上述の平滑化を実現する入力データコンバータを提案し考察した．

謝辞

本研究の一部は，福岡大学の研究助成（課題番号:205008）および科学研究費補助金（研究課題:20H00590, 20K11823）の助成を受けたものである．また，本研究は東京大学大規模集積システム設計教育研究センターを通しシノプシス株式会社の協力で行われたものである．

参考文献

[1] T. Jamil, “The Rijndael algorithm,” IEEE Potentials, Vol. 23, Issue 2, pp.36--38, 2004.

[2] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with A Leakage Model,” Proc. of International Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, Vol. 3156, Springer, pp. 16--29, 2004.