8 ビットマイコンにおける DES に対する

差分電力解析のセキュリティ評価に関する研究

日大生産工(学部)　○山本 孝一　　日大生産工　　栃窪 孝也

1　はじめに

現在、IC カードは Suica や住民基本台帳といった様々なもので使われている。これは、磁気カードに比べて、データの不正取得や改ざんが難しいためである。IC カードで用いられているセキュリティ技術の 1 つに暗号化技術がある。これは、用途に応じて共通鍵暗号方式と公開鍵暗号方式の 2 種類がある。共通鍵暗号方式は、事前に利用者同士でのカギ共有が必要であり、認証レスポンスが速いという特徴を持っている。公開鍵暗号方式は、事前に利用者同士でのカギ共有の必要はなく、デジタル署名として使うこともできるという特徴を持っている。現在の暗号は全数探索攻撃などの攻撃に対して、膨大な時間が必要なため安全とされているが、昨今サイドチャネルアタック[1][2]と呼ばれる IC カード等の暗号デバイスの処理時間や消費電力などを測定することで秘密情報を特定する攻撃方法が報告された。IC カードは、従来は耐タンパー性や物理的な観点から安全性が確認されているが、サイドチャネルアタックによる消費電力などの観点から攻撃に対して有効な手段が確立されていない。

本研究では、共通鍵暗号 DES に対するサイドチャネルアタックの一種である差分電力解析(以降 DPA と記す)のセキュリティ評価に関して、ソフトウェアシミュレータを使って検証する。既存のシミュレータ[3]はノイズや取り込み誤差などを考慮しておらず、厳密なシミュレータとは言えない。そこでソフトウェアシミュレータ上でノイズも疑似的に発生させた方法を提案する。そして、ノイズと試行回数との関係を明らかにする。

2　共通鍵暗号 DES

共通鍵暗号 DES とは、1976 年に米国政府と IBM で共同開発された暗号であり、平文を 64 ビットのブロック単位で暗号化・復号する。

拡大鍵処理の詳細は、まず鍵の縮約型転置 PC-1 によって 64 ビットの入力ビット列を 56 ビットにする。縮約転置されたビット列を左 28 ビットと右 28 ビットに分割し、左右の値をそれぞれ C_0、D_0 とする。C_{i-1}、D_{i-1} をそれぞれ左シフトした結果を C_i、D_i とする(1≦i≦16)。C_i、D_i を連接し 56 ビットの値とする。この値を鍵の縮約型転置 PC-2 にかけた 48 ビットの値が鍵 K_i となる。以上のことを、鍵 K_{16} が求まるまで繰り返す。

暗号化の処理では、平文 64 ビットに初期転置 IP を実行し、転置されたビット列を左側 32 ビット L_0、右側 32 ビット R_0 の 32 ビットずつに分割する。R_{i-1} をそのまま L_i とする($L_i=R_{i-1}$)。R_{i-1} と鍵 K_i を関数 f で計算した結果の値と L_{i-1} の排他的論理和の結果を R_i とする($R_i=L_{i-1}\oplus f(R_{i-1}, K_i)$)。この処理を R_{16} と L_{16} になるまで繰り返し、R_{16} と L_{16} を連接し、最終転置 IP^{-1}(初期転置 IP の逆転置)をかけ、その結果が出力になる(図 1)。

関数 f の詳細は、入力 R_{i-1}(32 ビット)と K_i(48 ビット)に対し、R_{i-1} を拡大転置(48 ビット)し、この結果と K_i を排他的論理和にかける。この結果求まるビット列を 6 ビットずつに分割し、8 つのビット列を得る。この 8 つのビット列を SBOX 処理にかけ、SBOX の出力 4 ビット×8 を得る。この結果を連接したものに転置 P をかけ、関数 f の出力とする(図 2)。

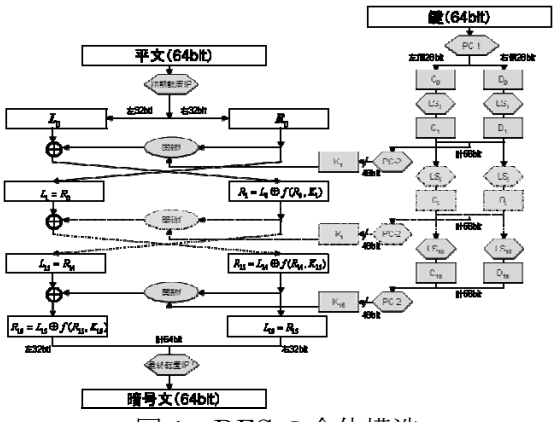

図 1　DES の全体構造

A Study on Differential Power Analysis
on 8 Bit Microcomputers

Kouichi YAMAMOTO and Kouya TOCHIKUBO

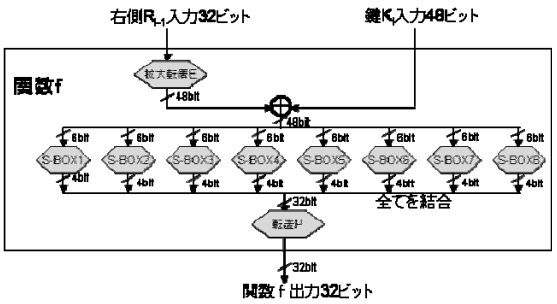

図２　関数 f の内部

3　DPA の概要

DPA とは、暗号処理中のデバイスの消費電力を複数回測定し、その平均から秘密鍵を推測する攻撃のことである。消費電力を複数回測定する理由は、電力を測定する上での取り込み誤差などを最小限に抑えるためである。

DPA では、DES 暗号の第 16 段(図 1)に入る鍵の一部のある 1 ビットの値に注目し、値が 0 か 1 かによって測定した消費電力のデータを 2 つのグループに分類する。鍵を予想すると、その予想鍵と測定した暗号文から、注目するビットが 0 か 1 かの予想値が得られる。この予想値を返す関数を選択関数と呼ぶ。注目するビットが 0 か 1 かによって、そのビットが関係する演算の消費電力には差が生じる。予想鍵が正しいならば選択関数の値と実際の注目するビットが一致するため、測定した消費電力の平均値をグループ毎に分類すると、消費電力に大きな差が生じる。これに対して、予想鍵が正しくないならば、選択関数の値と注目するビットは一致しないため、測定結果はほぼランダムに分類され、測定した消費電力をグループ毎に分類すると大きな差は生じない。すなわち、グループ間の消費電力の絶対値の差が最大の予想鍵が正しいことが期待できる[1][2][4]。

4　DPA の測定方法

DES に対する DPA の手順を以下に示す。

(1)　m 回暗号化プロセスを観測し、第 16 段の消費電力トレース $T_1,\cdots,T_m$ と暗号文 $C_1,\cdots,C_m$ を得る。m は 1000 回程で十分である。

(2) 鍵に依存した選択関数 D を以下のように定める。ただし、$K_{(16,1)}$は第 16 段で SBOX1 に供給される 6 ビットの部分鍵の予想値、C_6 は $K_{(16,1)}$とされる暗号文の 6 ビット、$SBOX_1(x)$は SBOX1 に 6 ビットの x が供給された場合の出力結果の 1 ビット目、C_1 は $SBOX_1(x)$と XOR する暗号文の 1 ビットである(図 3)。

$$D(C_1,C_6,K16_{(16,1)})=C_1 \oplus SBOX_1(C_6 \oplus K_{(16,1)}) \quad \cdots (1)$$

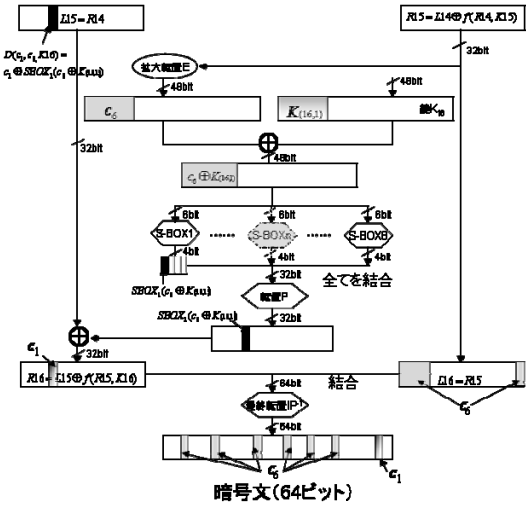

図３　DES の第 16 段から暗号文出力まで

(3) 選択関数 D により測定した消費電力トレース T1,…,Tm を、D=0 であるグループ S_0 と、D=1 であるグループ S_1 に分ける。

$$S_0=\{T_i \mid D(\cdot,\cdot,\cdot)=0\} \ , \ S_1=\{T_i \mid D(\cdot,\cdot,\cdot)=1\}$$

(4) それぞれのグループについて消費電力の平均値を求める。

$$A_0=\frac{1}{|S_0|}\sum_{T_i \in S_0} T_i \ , \ A_1=\frac{1}{|S_1|}\sum_{T_i \in S_1} T_i \qquad \cdots(2)$$

$$(|S_0|+|S_1|=m)$$

(5) 電力差分 ΔD を求める。

$$\Delta D=A_0-A_1 \qquad \cdots(3)$$

このとき、部分鍵 $K_{(16,1)}$の予想が正しい場合、得られた電力差分 ΔD は、参照値が 0 であるときと 1 であるときの消費電力の差となり、参照値が演算に用いられる領域でパルスが現れ、電力差分 ΔD が大きくなる。部分鍵 K_{16} の予想が正しくない場合、選択関数 D はほぼランダムに 0 か 1 を返すため、電力差分 ΔD はほぼ 0 になる。

(6) すべての $K_{16}(0\sim63)$ について繰り返 SBOX1 に関係する部分鍵 6 ビットを得る。

(7)　8 つの SBOX すべてについて 1～6 を行うことで 64 ビットの鍵を求めることができる。

消費電力トレースがない場合、鍵を求めるのに 2^{56} 通りの探索が必要であるのに対し、消費電力トレースがある場合、上記のように $8\times2^{56}=2^9$ 通りの探索で鍵を求めることができるのが DPA 解析の特徴である。

5　シミュレーションによる測定方法

ここでは、ソフトウェアによるシミュレーション方法を示す。この方法は実際のデバイスで測定する方法に比べ計算機能力、時間的に低コストであり、アルゴリズム中の数値表現方法や選択関数の比較検討に有用であると考えられる。

5.1　消費電力の近似モデル

ソフトウェアによるシミュレーションでは、以下のように消費電力を決定する。

- 消費電力は注目されるビットを含むビット列のハミングウェイトで決定する
- 直前のビットの状態は考慮しない
- トレース T は注目するビットが演算される瞬間の時刻のみを考える

今回の実験では選択関数は(1)式を用いるため、消費電力 P は L15 の 32 ビットパターンから決定する。ハードウェア実装での全体の消費電力(電流)は 8mA、注目ビットの電力差は 40 μA と読み取れるため、今回の実験では同じ比(10000:50)を用いる[1]。

$$P = 10000 + (0\ \text{のビットの数}) \times 25 - (1\ \text{のビットの数}) \times 25$$

$$\Leftrightarrow\quad P = 9200 + (0\ \text{のビットの数}) \times 50 \qquad \ldots(4)$$

5.2　ノイズ（取込み誤差）

今回は、5.1 で説明した消費電力 P においてノイズ(取込み誤差)を擬似的に発生させる。

- 誤差 3%のとき

$$P = 9200 + (0\ \text{のビットの数}) \times 50 + \text{RANDOM}(-300\sim300)$$

- 誤差 5%のとき

$$P = 9200 + (0\ \text{のビットの数}) \times 50 + \text{RANDOM}(-500\sim500) \qquad \ldots(5)$$

6　実験結果

図 4～9 は、横軸は部分鍵の予想値 K_{16}(0~63)、縦軸は電力差分 ΔD であることを表している。ΔD の絶対値が最大になる K_{16} が正しいと部分鍵だと期待できる。正しい部分鍵 K_{16} の値は 20 である。DPA 解析を行う上で、入力する平文はランダム、測定点と鍵は同じ、ノイズはランダムなど全て同じ条件で実験を行った。違いは、測定回数だけである。

6.1　測定回数と攻撃結果の関係(誤差なし)

測定回数 500 回(図 4)、測定回数 1000 回(図 5)の両方とも絶対値の最大値が 20 になっており成功している。測定回数 500 回の場合でも精度は粗いが成功することが分かった。測定回数 1000 回では、ほとんどの場合成功する。

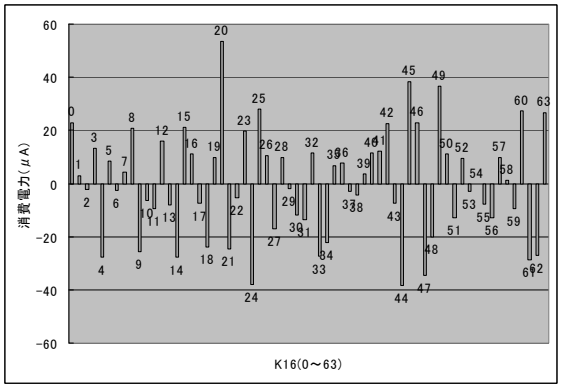

図 4　測定回数 500 回
の実行結果(取込み誤差なし)

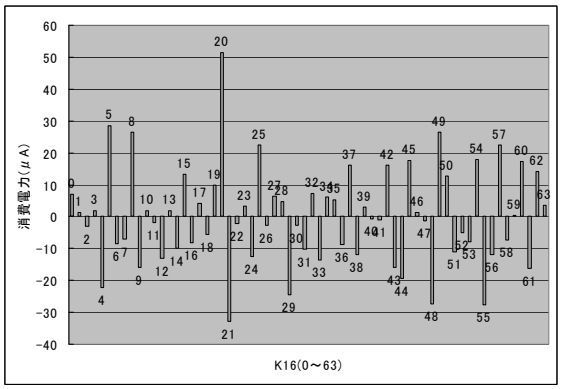

図 5　測定回数 1000 回
の実行結果(取込み誤差なし)

6.2 測定回数と攻撃結果の関係(誤差3%)

測定回数を 500 回(図 6)に減らした場合、成功したが全体的に SBOX の予想鍵を半分は間違えている結果になった。測定回数 1000 回(図 7)では、取込み誤差が 3%でもうまくいったことから、Kocher らの実験結果[1]と近い値になっていることが分かる。

6.3 測定回数と攻撃結果の関係(誤差5%)

測定回数 1000 回(図 8)では、8 個の SBOX のうち半数近くが失敗しているので、誤差 5%の場合は測定回数を増やさないとうまくいかない。そこで、ノイズを消去するために測定回数 3000 回(図 9)に増やすとかなりの精度で成功するようになった。

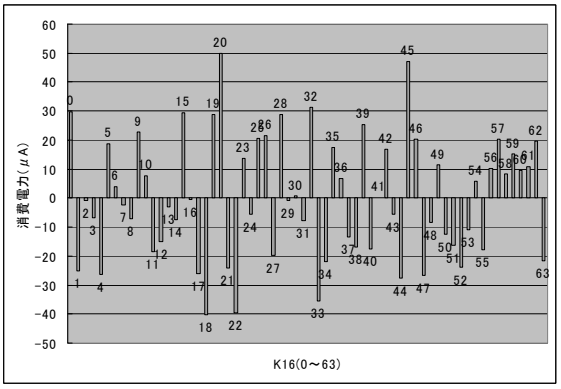

図 6　測定回数 500 回
の実行結果(取込み誤差 3%)

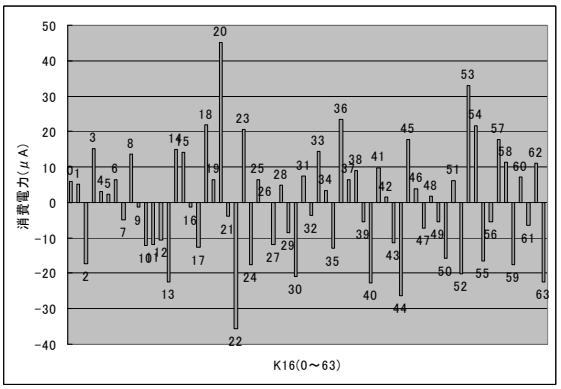

図 7　測定回数 1000 回
の実行結果(取込み誤差 3%)

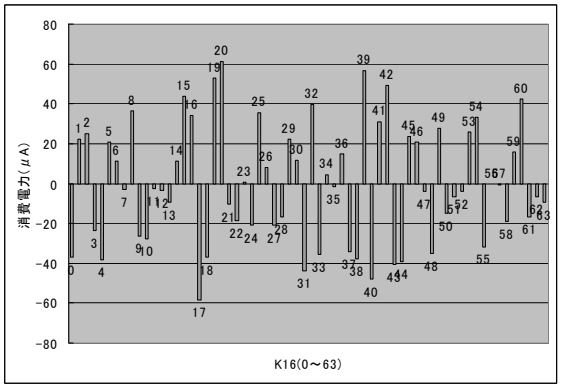

図 8　測定回数 1000 回
の実行結果(取込み誤差 5%)

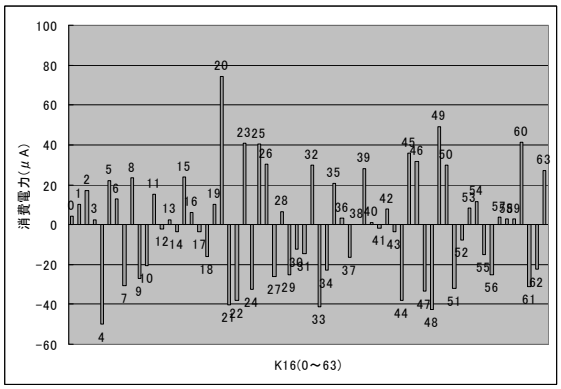

図 9　測定回数 3000 回
の実行結果(取込み誤差 5%)

7　おわりに

ノイズ(取込み誤差)を擬似的に発生させた DPA のソフトウェアシミュレータを開発し、取込み誤差なし、取込み誤差 3%、取込み誤差 5%の場合の正しい鍵を得るために必要な試行回数を明らかにした。

実験結果から、オシロスコープからの取込み誤差やノイズは 3%以内に収めるか、誤差を圧倒的多数の測定を行いほとんどわからなくする必要があることが分かった。そしてこれらの実験結果から、プログラム上でノイズを加えることにより、サイドチャネルアタックの攻撃時間を延ばすことが期待できることを確認することができた。

今後の課題として、8 ビットマイコンでの実際に計測した結果とソフトウェアシミュレータでの結果を比較し、ソフトウェアシミュレータの有効性を検証することである。

「参考文献」

[1] P. Kocher, J. Jaffe, and B. Jun, “Introduction to Differential Power Analysis and Related Attacks," 1998, available at http://www.cryptography.com/resources/whitepapers/DPA-technical.html

[2] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis", Proceedings of CRYPTO '99, Springer-Verlag, pp.388-397, 1999.

[3] 佐々木 明彦 他：“シミュレーションによる DES 実装の DPA 耐性評価,” 電子情報通信学 会 ,Vol.103,No.712(20040308) pp.25-30 (2004)

[4] “耐タンパー性標準化調査研究委員会報告書 2003~2006 活動報告,” 財団法人　日本規格協会 , 情報技術標準化研究センター

[5] 情報処理振興事業協会：“平成 11 年度スマートカードの安全性に関する調査 調査報告書,” http://www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/report/SmartCard/index.html

[6] 岩井 啓輔 他：“サイドチャネル攻撃評価用自動測定ソフトウェアの開発,” 電子情報通信学会 , ISEC2008-2 pp.9-14 (2008.2)

[7] 川村 信一：“耐タンパー技術の動向,” 情報ｾｷｭﾘﾃｨと VLSI 技術に関する研究会 , http://imailab-www.iis.u-tokyo.ac.jp/ITSEC_VLSI04/ITSEC_&_VLSI-2.pdf (2003)