8G－01　サイドチャネル解析に対する耐性評価ツールの開発

小池正修* 川村信一† 佐野文彦* 斯波万恵* 野崎華恵†
*（株）東芝 SI 技術開発センター
†（株）東芝 研究開発センター

1 はじめに

近年，装置等に実装された暗号アルゴリズムに対して，その途中経過に関係する副次的な情報（処理時間，消費電力など）が漏洩していることを利用した解析方法，いわゆるサイドチャネル解析が提案されている[1]－[3]．また，サイドチャネル解析への対策も幾つか提案されており[5]－[8]，解析法の原理や対策に関するサーベイも報告されている[9]．

サイドチャネル解析が実装に着目した解析法であるために，考案された対策が有効であるかは最終的には実際にその対策を組み込んだ実装に対してそれぞれの解析を適用してみることで確認される．しかしながら，実装および測定はそれ自体一定の時間を要するため，製造業の立場からはできる限りその試行回数を減らすことが望ましく，また一連の開発作業の中で実装・測定後に対策不十分と判定されることはできるだけ減らしたい．さらに種々の暗号アルゴリズムに対するサイドチャネル解析対策を考案しようという場合，その各々について実装・測定によって対策の有効性を確認することは現実的でない場合も多い．

本稿ではサイドチャネル解析（特にタイミング解析，DPA（Differential Power Analysis））への対策を考案した場合に，その有効性を実装・測定以前に，ある程度の精度で確認するためのツールを開発したので，その概要を述べる．

以下，2節ではサイドチャネル解析，特にタイミング解析およびDPAについて説明する．3節ではディジタル信号処理の手法を用いて DPA の原理を検討し，DPA 対策の有効性を検証するディジタルモデルを提案する．4 節では開発したツールの概要，提案モデルによる実験例を示しその有効性を確認し，5節で本稿を結ぶ．

2 サイドチャネル解析

2.1 代表的なサイドチャネル解析

Kocher らはサイドチャネル解析として基本的と思われる以下の３種類の解析法を提案した[1]－[3]．

(a) タイミング解析
(b) SPA（Simple Power Analysis）
(c) DPA (Differential Power Analysis)

(a)は暗号の処理時間の変化から，(b)(c)は暗号装置の消費電力から鍵情報を得ようという解析手法である．SPA が１回の暗号化処理における消費電力波形を利用する手法であるのに対して，DPA は複数回の暗号化処理の電力波形を統計処理する手法である．一般にはこれらを組み合わせた手法が考えられる他，観測する物理量も電磁波・温度など様々な可能性がある．

本稿ではこれらの内，タイミング解析と DPA について述べる．

2.2 タイミング解析の具体的解析手法

タイミング解析の手法として，[4]に示された Rijndael 方式に対するタイミング解析に即して説明する．

ラウンド関数内の１つの操作である MixColumn

A Tool for Assessing Side-Channel Attack Resilience
Masanobu Koike, Shinichi Kawamura, Fumihiko Sano, Masue Shiba and Hanae Nozaki
* System Integration Technology Center, Toshiba
† Corporate Research and Development Center, Toshiba

における'02'倍算を

1　1ビット左シフト

2　キャリーが発生したら'1B'と排他的論理和（XOR）をとる

と実装している場合を考える．ここで GF(2^8)の元を'02'のように表現している．

(1) 入力する平文を先頭バイトの値に応じて分類する．S_i を先頭バイトが i $(0 \le i \le 255)$であるものの集合とする．

(2) Rijndael の 1 段目に着目し，平文の先頭バイトを MixColumn での'02'倍算までたどっていき，その MSB をターゲットビットとする．1 番目の拡大鍵 R_1 が固定であれば，この値は S_i に属するメッセージに共通である．

(3) ターゲットビットが 1 であるとき，MixColumn の'02'倍算で XOR が実行されるため，ターゲットビットが 0 のときに比べて処理時間が長く観測される．

(4) S_i に属する十分多くのメッセージを入力して処理時間の平均値を取ることで，計測誤差などの雑音を取り除く．その平均値から XOR が行われたか判断し，ターゲットビットに対応する R_1 の 1 ビットを確定することができる．$i \neq j$ なる適当な S_j に対して同じことを行うことで，R_1 の他のビットを確定することができる．2 番目以降の拡大鍵に対しても同様である．

このような解析への対策として，キャリーの有無で処理を分岐しないようにすることが挙げられる．

2.3 DPA の具体的解析手法

DPA の手法として，[3]に示された DES 方式に対する DPA 解析に即して説明する．

(1) 入力平文 m_i を取り替えながら 1,000 サンプルの DES 処理に対する消費電力波形 $v_i(t)$ を採取．ここで t は離散的な時刻を表す．

(2) DES の最終段に着目し，S ボックスの出力の 1 ビットをターゲットビットとする．DES の Feistel 構造の特徴より，暗号文 C_i（解析者に既知）からさかのぼり当該 S ボックスの入力に対応する 6 ビットが確定する．S ボックスの入力としてはこれ以外に，これと排他的論理和される 6 ビットの部分鍵 k_j があり，これを未知変数として，ターゲットとなる S ボックス出力 1 ビットを $s_i(k_j, C_i)$ と書く．

(3) 差分平均トレースを次の式により計算する．

$$T_j(t) = \sum_{i=0}^{999} \left(s_i(k_j, C_i) - \frac{1}{2} \right) v_i(t)$$

(4) k_j として 6 ビット 64 通りすべての場合について T_j を計算すると，その内の一つは実際に使われている部分鍵と一致しており，その時 T_j は値の偏り（バイアス）を示す．それ以外の場合には偏らない．

(5) 以上で 6 ビットの部分鍵が見つかったならば，この操作を他の 7 つの S ボックスに関しても適用することで 48 ビットの部分鍵を見出すことができる．残り 8 ビットの部分鍵は総当りで容易に探索できる．

3　DPA のディジタルモデル

3.1 信号処理から見た DPA

ここでは DPA の耐性評価ツール設計のために，DPA の原理について，ディジタル信号処理の手法による解析を試みる．まず i 番目のサンプルの時刻 t での消費電力 $v_i(t)$ が次のように表せるものとする．

$$v_i(t) = \alpha(t) \cdot s_i(k_0, t) + n_i(t)$$

ここで $s_i(k_0,t)$は，解析対象となる信号で 1 または 0 を値としてとる．その引数 k_0 が波形観測によって導出しようとしている部分鍵である．また$\alpha(t)$は時刻 t での s_i の寄与率，$n_i(t)$は解析ターゲット以外の信号成分であり，解析者にとっては雑音成分となる．

直流成分は以下の解析には不要なため，時刻 t における v_i の期待値を差し引いた交流成分$\Delta v_i(t)$を定義する．

$$\Delta v_i(t) = v_i(t) - E[v_i(t)]$$
$$= \alpha(t) \Delta s_i(k_0, t) + \Delta n_i(t)$$

解析者は，部分鍵を k_j とした時の信号を $s_i(k_j,t)$として$\Delta s_i(k_j,t)$と観測波形$\Delta v_i(t)$との k サンプルにわたる相関値 T_j から k_j の推定が正しいかどうかを検証す

る．ここではT_jを次のように定義する．

$$T_j = \frac{1}{k}\sum_{i=1}^{k} \Delta s_i(k_j,t)\cdot\Delta v_i(t)$$

前節で説明したDPAは部分鍵k_jの全パターンについてT_jを計算したときに，部分鍵が一致しているT_0とそれ以外T_j $(j\neq 0)$とでT_jの値が異なることに着目した解析法である．なお，今後$T_j(j\neq 0)$はT_1で代表させることにする．

ここまで定義した各変数間に，次のような関係があるものと仮定する．

(a) $s_i(k_j,t) \in\{0,1\}$， $E[s_i(k_j,t)]=1/2$

(b) $E[\Delta s_i(k_j,t)]=0$，$E[\Delta n_i(t)]=0$

(c) $E[\Delta s_i(k_j,t)\cdot\Delta s_l(k_j,t)]$
$=E[\Delta s_i(k_j,t)]\cdot E[\Delta s_l(k_j,t)]$

(d) $E[\Delta s_i(k_j,t)\cdot\Delta n_i(t)]=E[\Delta s_i(k_j,t)]\cdot E[\Delta n_i(t)]$

(e) $E[\Delta s_i(k_j,t)\cdot\Delta s_i(k_l,t)]=\sigma_s^2\delta_{jl}$
（ここでδ_{jl}はKroneckerのデルタ）

(f) $V[\Delta n_i(t)]=E[\Delta n_i(t)^2]-E[\Delta n_i(t)]^2=\sigma_n^2$

条件(a)はsが1，0を各々確率1/2でとることを表し，(b)はΔs，Δn_iの期待値が0であることを表す．条件(c)は同一部分鍵でも試行が異なればΔsは統計的に独立であるという要請から導出される．条件(d)も同様である．(e)は，部分鍵が異なるΔs間は無相関であることを表す．また(e)(f)ではΔs，Δn_iの電力をそれぞれσ_s^2，σ_n^2と定義している．なお，$\sigma_s^2=1/4$であることは容易に示せる．

この時，以下の関係式が導出できる．証明は[11]を参照．

$E[T_0]=\alpha\sigma_s^2=\alpha/4$

$E[T_1]=0$

$V[T_0]=\sigma_s^2\cdot\sigma_n^2/k$

$V[T_1]=\sigma_s^2\cdot(\sigma_n^2+\alpha^2\sigma_s^2)/k$

この結果について図1を用いて説明する．部分鍵k_0に関する推定が当たっている場合にはT_jの期待値はT_0の分布に従い，$\alpha/4$を中心に標準偏差$\sigma_0=\sqrt{V[T_0]}$で，kが十分大きければ正規分布に近づく．これに対して推定が外れている場合には，T_jの期待値はT_1の分布に従い平均0，標準偏差$\sigma_1=\sqrt{V[T_1]}$である．

ここで両者の分散は若干異なっているものの，共にサンプル数kに逆比例していることに注意．そのためkを大きくすることにより，T_0とT_1の分布はそれぞれの平均値の周りで急峻なピークを描くようになり，両者の判別が容易になる．

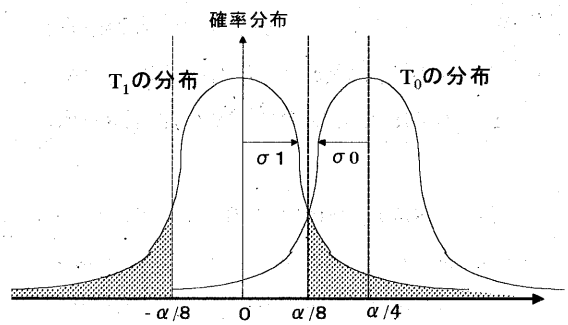


図1 T_jの期待値の分布

3.2 ディジタルモデルによる相互相関評価

前節で考察したように，DPAのポイントはアルゴリズムから決まる変数s_iと電力波形Δvとの相関を利用することである．逆にΔvのs_i成分をs_iと無相関にできるならば有効なDPA対策といえる．元々電力波形Δvにs_iに比例した成分が含まれるのは，アルゴリズムを実装する際にs_iに対応するビットが実装されるからである．従って，アルゴリズムで自然に定義された任意のビット（以下アルゴリズムビットと呼ぶ）と，実際に実装されたすべてのビット（以下では実装ビットと呼ぶ）との間に相関がなくなれば，結果として現れる電力波形Δvとアルゴリズムから決まる変数s_iとの相関で解析されることはなくなる．

このことからアルゴリズムビットs_iと実装ビットg_iとの間の相互相関をマトリックス状に計算した場合に，いずれのビット間にも顕著な相関がなくなるようにすればDPA対策となる．相互相関は次のように定義する．

$$\varphi(t,t') = \frac{\sum_{i=1}^{k} \Delta s_i(t) \cdot \Delta g_i(t')}{\sqrt{\sum_{i=1}^{k} \Delta s_i(t)^2} \sqrt{\sum_{i=1}^{k} \Delta g_i(t')^2}}$$

なお，図2の下段の実装ビットにはアルゴリズムビット s_i に変数 u_i を排他的論理和して g_i を決定する例が示されている．u_i に対して，以下のように s_i と統計的に独立で，確率 1/2 で 1 をとるという条件を課せば相関を消すことができる．但しこれが十分な対策であるためには u_i が解析者から予測不可能でなければならない．

$u_i \in \{1, 0\}$，　$E[u_i] = 1/2$

$p(s_i, u_i) = p(s_i) \cdot p(u_i)$　（s_i と統計的に独立）

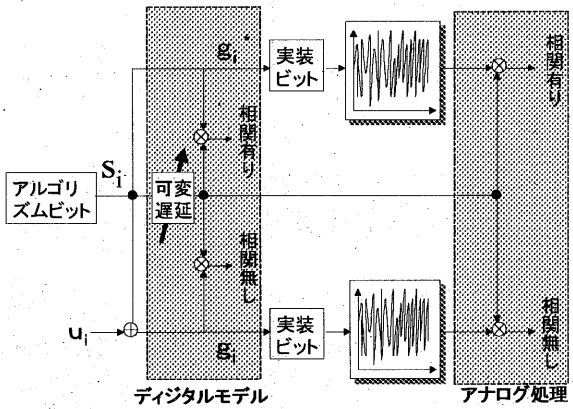


図2 ディジタルモデルでの評価

4　耐性評価ツール

4.1 ツールの必要性

サイドチャネル解析全般に対して，対策の入ったシステムの開発プロセスは図3のようになると考えられる．このようなプロセスではシステム実装後に対策の有効性を判定することになり，手戻りによる評価期間の増大が予想される．

これに対して我々は図4のような形で実装前に計算機内でタイミング解析耐性評価，DPA 耐性評価を行うフローを提案する．今回開発したツールは，計算機内で耐性評価を行うものである．

DPA が強力な解析ツールである理由の一つは対象ハードウェア個々の特性によらず，広い範囲にわたり適用できる手法だという点である．これは裏返せば，ハードウェア個々の特性を考慮せずに DPA 対策の有効性を評価しうることを示唆しており，このことが実装前に耐性評価をしようという本研究の動機づけとなっている．

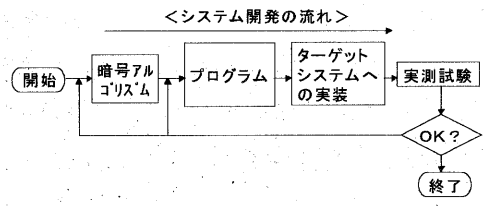
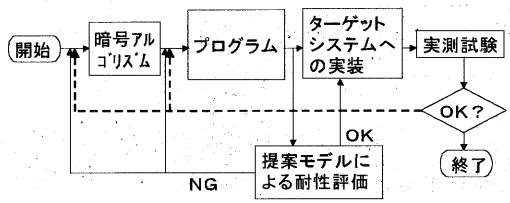


図3 従来の開発フロー



※時間のかかる実装以後の手戻りの可能性を減らす

図4 提案する開発フロー

4.2 タイミング解析耐性評価ツール

2.2で述べた例のように，タイミング解析は実装コードがデータに依存して処理時間が変化することに着目した解析方法である．そのため，開発したツールは実装したコードの処理クロックをカウントして常に一定であることを確認することで，タイミング解析への耐性を備えているかを評価する．本ツールでは実装コードはZ80で記述されているものを対象とした．評価ツールにはZ80コードをシミュレートする機能があり，実装コードを実行したときに使ったZ80命令を順に記憶する．この種類と順序が平文や鍵によって不変であれば，その実装コードはタイミング解析に対して十分耐性を有していると評価できる．そうでなければタイミング解析による解析の可能性を指摘する．

タイミング解析は処理時間に注目した解析方法であるため，処理時間を調整するための無意味なコード（NOP）を対策として組み込むことも考えられるが，その場合はSPAと組み合わせることで解析されうる．本ツールでは処理クロックのみならず実行した命令を比較しているので，そのような解析方法からの耐性も評価することができる．

4.3 DPA耐性評価ツール

開発したツールは，アルゴリズムビットと実装ビットの間の相互相関マトリックスを実際に計算し表示する．ここではアルゴリズムとしてDES方式を取り上げ，DESの定義に現れる任意のビットをアルゴリズムビットと考える．図5に今回用いたDESのアルゴリズムビットの一部を示す．図にはDESのデータランダム化部のブロック図（部分）が示されているが，データフローを表す矢印に斜線とビット数を示してある部位をアルゴリズムビットとして用いた．これらは，アルゴリズムを自然に記述した場合に各段毎独立と考えられるビットを取り出す，という方針で選定した．対策入りの実装ビットも同様の方針で切り出すことができる．

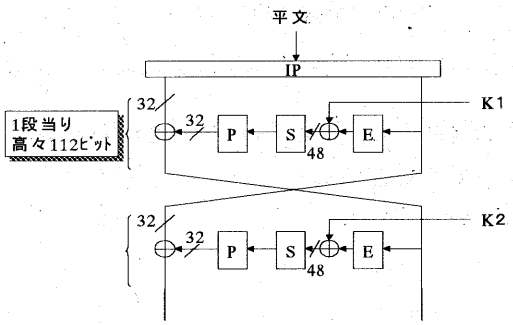


図5 DESのアルゴリズムビット例

今回の実験では実装ビットとして文献[10]に示された対策を行ったDESの実装を採用した．また対策なしの例としてはアルゴリズムビットそのものを実装ビットとした場合を実験した．

図6には対策なしの例，図7に対策ありの例を示す．x軸にアルゴリズムビット，y軸に実装ビット，z軸に相互相関係数の値を示す．両グラフとも相関をとるサンプル数としてk＝1,000を用いた．なお，相互相関係数はDESの初段から16段のすべてのアルゴリズムビットに対応して計算してみる必要があるが，表示の解像度を十分にとるために，図6，7では16段目近傍のアルゴリズムビット64ビットと実装ビット128ビットについての評価結果についてのみ示している．

対策なしの場合は当然のことながら対角成分に相関が現れている．対策ありの場合には，その相関が十分消されており対策の有効性が確認できた．

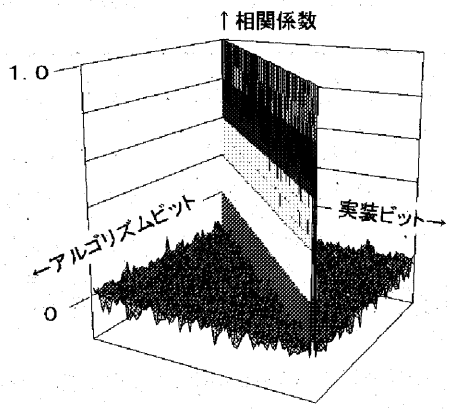


図6 対策なしの例

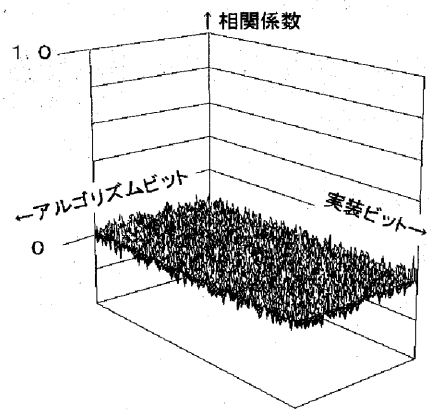


図7 対策ありの例

最後に，このように相関が打ち消されるかどうかは対策が相関を打ち消すようにできているかどうかで決まるため，多くの場合相関が打ち消されるかどうかは本ツールを用いなくても対策の内容を詳細検

討することで理論的に検証できる．しかしながら，開発の現場においては，その対策を実装する際に紛れ込んだバグなどにより折角の対策に穴が生じる可能性は否定できない．本ツールを用いれば実装・測定を経てそのバグを見出すのではなく，それ以前に論理レベルのバグを排除することが可能となる．本ツールはこのような開発の現場においての有効利用が期待できる．

5 むすび

サイドチャネル解析のうち，タイミング解析，DPA に対する耐性評価ツールについて概要を述べた．DPA については，アルゴリズムと実装されたビットとの間の相互相関を評価量とすることを提案した．このモデルは実装対象の物理特性と独立であるため，実装前に耐性評価が可能であるとともに汎用性が高い．

但し，今回提案した評価基準だけですべてのサイドチャネル解析への対策が評価できる訳ではない．またサイドチャネル解析が実装に即した解析手法であるために，解析者の経験や技量が高まればそれまで十分と考えられてきた対策が十分でなくなることもある．我々は本稿で提案した手法などを駆使し常に高い信頼性のあるセキュリティ機器を提供することを目指して行きたいと考えている．

謝辞：本研究は，情報処理振興事業協会（略称 IPA）殿よりの受託調査研究である独創的情報技術育成事業の一環として 2000 年度に「暗号のサイドチャネル解析に対する耐性評価モデルの調査研究」という名称で実施したものです．感謝申し上げます．

参考文献

[1] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", Advances in Cryptology: Proceedings of CRYPTO '96, Springer-Verlag, 1996, pp.104–113.

[2] P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis", Advances in Cryptology: Proceedings of CRYPTO '99, Springer-Verlag, 1999, pp.388–397.

[3]http://www.cryptography.com/dpa/technical/index.html, (Cryptography Research, Inc.ホームページ.)

[4] F.Koeune, J.-J. Quisquater, "A timing attack against Rijndael", UCL Report, 1999, CG1999-1, http://www.dice.ucl.ac.be/crypto/techreports.html.

[5] J.-K. Dhem, F. Koeune, P.-A. Leroux, P. Mestre, J.-J. Quisquater, J.-L. Willems, "A Practical Implementation of the Timing Attack", UCL Report, 1998,CG1998-1, http://www.dice.ucl.ac.be/crypto/techreports.html.

[6] J.-S. Coron, "Resistance Against Differential Power Ahalysis for Elliptic Curve Cryptosystems", Proceedings of CHES '99, Springer-Verlag, 1999, pp.292-302.

[7] S. Chari, C. S. Jutla, J. R. Rao, P. Rohatgi, "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", Proceedings of the Second Advanced Encryption Standard Candidate Conference, 1999.

[8] S. Chari, C. S. Jutla, J. R. Rao, P. Rohatgi, "Towards Sound Approaches to Counteract Power-Analysis Attacks", Advances in Cryptology: Proceedings of CRYPTO '99, Springer-Verlag, 1999, pp. 398–412.

[9] 情報処理振興事業協会, "スマートカードの安全性に関する調査研究", 2000, http://www.ipa.go.jp/SECURITY/enc/SmartCard

[10] L. Goubin, J. Patarin, "DES and Differential Power Analysis – The "Duplication" Method", Proceedings of CHES '99, Springer-Verlag, 1999, pp.158-172.

[11] 川村，小池，斯波，佐野，野崎，"サイドチャネル解析への耐性評価モデル"，SCIS2001，2001．