Keywords you should know. 第58回

知っておきたいキーワード

サイドチャネル攻撃

本間尚文†，(正会員)青木孝文†

† 東北大学 大学院情報科学研究科

"Side-channel Attack" by Naofumi Homma and Takafumi Aoki (Graduate School of Information Sciences, Tohoku University, Sendai)

キーワード：組込みシステム，ハードウェアセキュリティ，暗号モジュール，電力解析攻撃，安全性評価

暗号モジュールの普及

身の回りのあらゆる機器がネットワークを介して結合される高度な情報化社会においては，プライバシーの保護や高信頼な電子商取引が必須であり，情報セキュリティをいかに実現するかがますます重要となります．暗号はそのような社会システムを構築する上で欠かすことのできない基盤技術であり，近年ではソフトウェアやハードウェアで暗号を実装した専用の暗号モジュールが民生品に幅広く搭載されています．例えば，暗号モジュールを搭載したICカードでは，リーダーとの間でディジタル署名などの演算を実行することで真贋を判定するとともに，データ通信の秘匿性を保証しています．こうした暗号モジュールは，従来の磁気ストライプなどと比べ，不正な情報の読出しや内部機能の改変に対する耐性（耐タンパー性）が高く，偽造も困難であることから，更なる応用範囲の拡大が期待されています．

暗号モジュールへのサイドチャネル攻撃

暗号モジュールには，通常専門家により充分に安全性評価が行われた暗号アルゴリズムが利用されます．そのため，アルゴリズムの欠陥から暗号化前のデータ（平文）や秘密鍵が漏洩する心配はほとんどありません．しかし，近年，その実装上の脆弱性から秘密情報を奪う実装攻撃の危険性が指摘されています．実装攻撃は，モジュールのパッケージを剥がして内部構造や回路動作を解析する侵襲攻撃と，モジュールに手を加えない非侵襲攻撃に大別されます．侵襲攻撃は極めて強力ですが，高価な装置と高いスキルが必要で，ごく限られた人にしか実行できません．これに対して非侵襲攻撃は，比較的安価な設備で実行できて攻撃の痕跡も残らないため，より現実的な脅威と考えられています．その中でも特に注目を集めているのが，モジュール動作中に観測される非正規の情報（サイドチャネル情報）を利用するサイドチャネル攻撃です．

図1に代表的なサイドチャネル攻撃を示します．サイドチャネル情報の観測を基本とする受動的な攻撃としては，これまで，処理時間を利用するタイミング攻撃，電力変動を利用する電力解析攻撃，漏洩電磁波を利用する電磁波解析攻撃，発生する音を利用する音響解析攻撃などが知られています．また，外部から暗号モジュールが誤動作するような操作を能動的に加えて，その誤った演算結果から秘密情報を導出する故障利用攻撃もあります．誤動作の誘発に電源電圧やクロック信号といった非正規の入出力を用いることから，故障利用攻撃も，しばしばサイドチャネル攻撃の一つとみなされます．サイドチャネル攻撃は，情報セキュリティ関連の学会でも高い関心を集めていて，近年では攻撃や対策の理論研究だけでなく，実際のモジュールを対象とした実証研究も増加しています．

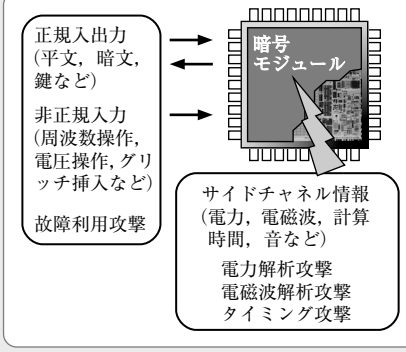

図1 暗号モジュールに対するサイドチャネル攻撃

映像情報メディア学会誌 Vol. 64, No. 11, pp. 1576～1579 (2010)

電力解析攻撃

サイドチャネル攻撃の中でも，最も有名な攻撃が電力解析攻撃です．電力解析攻撃では，通常，**図2**のように，モジュール動作中に生じる電力（電圧）の時間変化をディジタルオシロスコープなどの計測器で観測し，その波形をPCで加工・処理して暗号化・復号処理の内容を推定します．1990年代後半に，Kocherらによって単純電力解析（SPA：Simple Power Analysis）と差分電力解析（DPA: Differential Power Analysis）が発表されたのを機に，現在もその拡張や対策が盛んに研究されています．

また，電力の代わりに漏洩電磁波の波形を用いても同様の攻撃（電磁波解析攻撃）が可能であることが知られています．

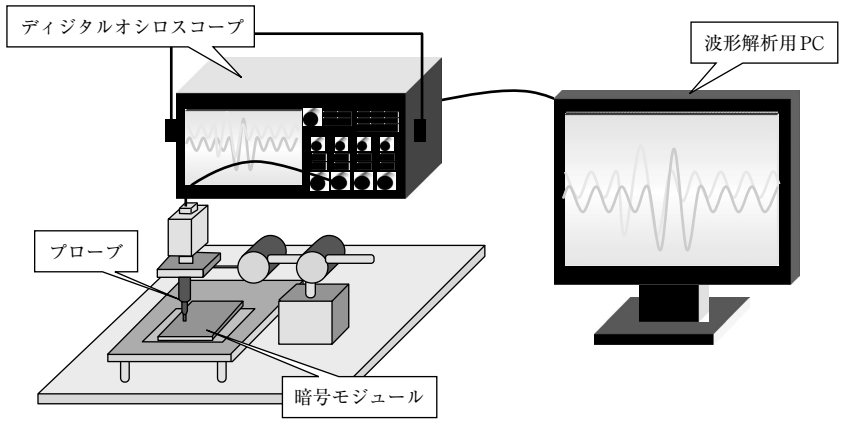

図2　電力解析攻撃のセットアップ

単純電力解析（SPA）

SPAは，測定した一つもしくは複数の電力波形を直接調べることで鍵を求める攻撃です．**図3**に，SPAのイメージを示します．ある暗号化処理が秘密鍵に応じてAとBという演算の繰り返しで実行される場合，このAとBの電力波形を見分けることで，その秘密鍵を推定することができます．

SPAは，1回の暗号化，もしくは，復号に多くの計算を必要とする公開鍵暗号（RSA暗号など）のモジュールに有効とされています．特に，ソフトウェア実装された暗号モジュールでは，しばしば演算により命令系列が異なっているため，その違いを波形から容易に見分けられる場合があります．ハードウェア実装された暗号モジュールの場合でも，入力を選択したSPAを用いれば，鍵を推定することが可能です．例えば，入力の異なる複数波形を用いるSPAでは，特徴的な波形パターンが得られる入力を選択し，波形間で同一波形パターンの生じる位置を比較することで，秘密情報を推定します．近年では，モジュールの動作に応じて入力を動的に変更するSPAの危険性も指摘されています．

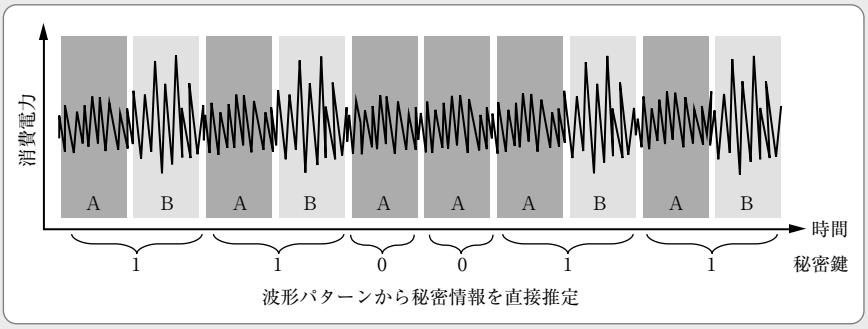

図3　単純電力解析（SPA）

差分電力解析（DPA）

DPAは，大量の電力波形を統計処理することで鍵を求める攻撃です．**図4**にDPAの概要を示します．攻撃者は，まず，入力を変えながら大量の電力波形とそれに対応する暗文を取得します．次に，鍵の一部を推定し，取得した暗文と推定した鍵の値から電力値を推定します．その後，推定した電力値とある時刻の電力波形との間の相関係数を計算します．これをすべての時間インデックスに対して行い，

☞

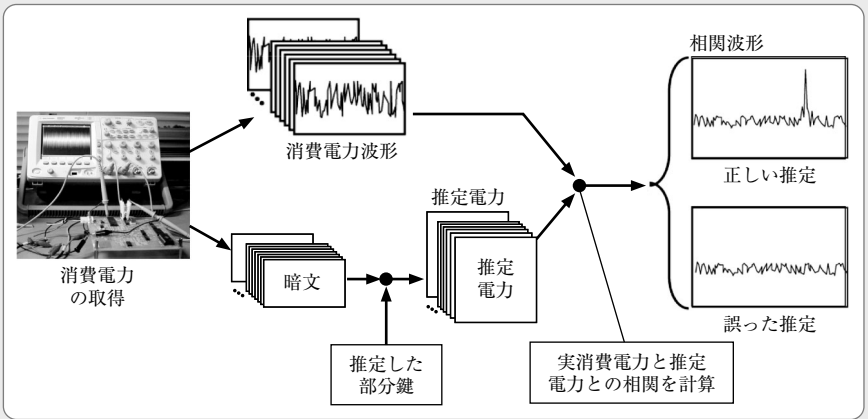

図4　差分電力解析（DPA）

☞ ある推定鍵における1次元の相関係数波形を求めます．鍵の推定が正しかった場合，この相関波形のどこかに高い相関値が得られることになります．DPAは，数百から数十万といった波形数を必要とする一方で，SPAのように攻撃対象となるモジュールのアルゴリズムや構造に関する詳細な知識を必要としません．また，ノイズに対しても強いことから，電力波形のデータ依存性が低く，SPAに耐性がある共通鍵暗号（DESやAESなど）のモジュールに対しても有効な攻撃と考えられています．

近年では，攻撃対象となる演算の範囲を広げるような選択平文DPAへの拡張も見られます．

サイドチャネル攻撃への対策

一方で，サイドチャネル攻撃への対策も盛んに研究されています．対策手法には，大きく分けてサイドチャネル情報（消費電力や漏洩電磁波）の隠蔽（ハイディング）と遮蔽（マスキング）があります．ハイディングとは，モジュールから得られるサイドチャネル情報と内部処理や中間値との依存関係を隠す対策です．電力解析攻撃へのハイディング対策では，計算される値に依らず常にランダムな量もしくは一定量の電力を消費することで解析を不可能とします．**図5**にハイディング対策の例を示します．未対策の電力波形では，AとBの演算が秘密情報に応じて出現するため，その波形パターンから秘密情報が推定されてしまいます．これに対して，対策を施した電力波形では，実際には計算結果を利用しないBのダミー演算が挿入されて，AとBの演算が秘密情報に依らず交互に出現します．これにより，計算時間は増加しますが，波形パターンから秘密情報が推定されるのを防いでいます．一方，マスキングとは，演算に用いる値にあらかじめ乱数による変換を施し，サイドチャネル情報とアルゴリズムによって決まる（マスクされていない時の）真の中間値との関係を独立とする対策です．電力解析攻撃へのマスキング対策では，消費電力と中間値の関係を推定できたとしても，その中間値自体は真の中間値と無関係なため解析が不可能となります．これまで，アルゴリズム，アーキテクチャ，回路方式などの設計レベルでさまざまなハイディングやマスキングの対策が提案されています[1]．

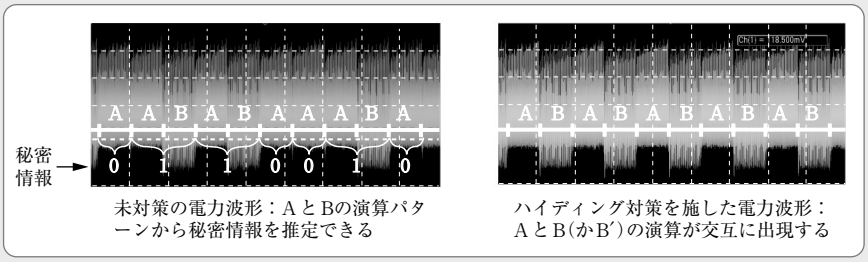

図5 アルゴリズムレベルでの電力解析攻撃対策の例

暗号モジュールの安全性評価に向けた取組み

現在，暗号モジュール製品のセキュリティ評価に関しては，第三者が評価・認証する制度的枠組みが整備されています．

一つは，情報セキュリティ製品の国際評価標準規格ISO/IEC 15408（Common Criteria）に基づく制度です．これは暗号だけでなく，情報セキュリティ製品全般を対象としており，開発者が定めたセキュリティ目標が正しく実装され，かつ，想定した環境において矛盾なく動作することを第三者機関が検証するものです．ISO/IEC15408には，EAL（Evaluation Assurance Level）という7段階の検証レベルが設定されていて，大まかに分類すると，EAL1〜3が一般民生用，EAL4が政府機関向け，EAL5〜7が軍や政府最高機密機関レベルとなります．ただしEALは，開発者が定めたセキュリティ目標が正しく実装されているかどうかの指針であり，セキュリティ強度を示すものではない点に注意が必要です．

もう一つは，米国国立標準技術研究所NISTによる米国連邦標準FIPS（Federal Information Processing Standard）140-2を基に策定されたISO/IEC 19790に基づく制度です．この国際標準規格は，暗号モジュールが満たすべきセキュリティ要件として，暗号アルゴリズムやインタフェース，物理セキュリティ，暗号鍵管理など11項目を定めていて，満たされた条件の強度に応じて4段階のレベル付けを行います．国内では，これらの標準に準拠した「暗号モジュール試験および認証制度（JCMVP: Japan Cryptographic Validation Program）が，IPA（情報処理推進機構）によって運用されています．しかし，サイドチャネル攻撃に関しては「その他の攻撃への対処」の項目に分類されていて，具体的な評価指標はまだ定められていません．NISTは現在，サイドチャネル攻撃などの最新の研究結果を取り入れたFIPS140-3への改訂作業に取組んでいて，それと並行してISO/IEC標準の改訂も進められています．

国内でも，電子政府推奨暗号の安全性評価プロジェクトCRYPTRECにおいて，暗号実装委員会にサイドチャネル解析WGを設置して，サイドチャネル攻撃に対する評価・試験基準の検討と実験ノウハウの蓄積に取組んでいます[2]．また，サイドチャネル攻撃の標準的な評価環境を提供することを目的として，サイドチャネル攻撃 ☞

☞ 実験用標準評価ボード（SASEBO）と，同ボードで利用可能な国際標準暗号アルゴリズムのハードウェアIPが，産業技術総合研究所と東北大学によって開発・公開されています[3]．SASEBOは現在，CRYPTRECやNISTを含む国内外70を越える企業・大学・研究機関で利用されていて，第3者機関による攻撃・対策検証の進展に寄与することが期待されています．

今後の展望

サイドチャネル攻撃は，現在でも日々新たな攻撃手法・対策手法が提案されていて，今後も半導体製造技術や計測・解析技術の進歩によって発展していくと予想されます．暗号モジュールの設計者は，本稿で解説したSPAとDPAを基本として踏まえた上で，サイドチャネル攻撃への適切な対策を施すことが重要となります．論理的には攻撃可能な対策であっても，攻撃のコストを増大させるという点では意味があり，実装形態によってはその攻撃手法が使えない場合も考えられます．システム全体に対してどのような脅威があるかを考え，それに対する対策を重点的に採ることが必要となります．また，利用者側でも，そうした対策がきちんと取られている製品かどうかを意識していくことが大切となるでしょう．

参 考 文 献

1）S. Mangard, E. Oswald and T. Popp: "Power Analysis Attacks - Revealing the Secrets of Smart Cards", Springer（2007）
2）CRYPTREC報告書，http://www.cryptrec.go.jp/report.html
3）Side-channel Attack Standard Evaluation Board:，http://www.rcis.aist.go.jp/special/SASEBO/

本間（ほんま） 尚文（なおふみ） 2001年，東北大学大学院情報科学研究科博士課程修了．同年，同研究科助手，2007年，同助教．2009年，同准教授となり，現在に至る．2002年～2006年，科学技術振興機構さきがけ研究者を兼任．CRYPTREC暗号実装委員会委員および同サイドチャネル解析WG委員．ハードウェアアルゴリズム，VLSI設計技術，ハードウェアセキュリティに関する研究に従事．

青木（あおき） 孝文（たかふみ） 1992年，東北大学大学院工学研究科博士課程修了．同年，同大学助手．1994年，同大大学院情報科学研究科助手．1996年，同助教授．2002年，同教授となり，現在に至る．超高速ディジタル計算の理論，画像センシング，映像信号処理，バイオメトリクス，VLSI設計技術，分子コンピューティングに関する研究に従事．英国電気学会フレミング賞およびマウントバッテン賞ほかを受賞．正会員．

キーワード募集中

この企画で解説して欲しいキーワードを会員の皆様から募集します．ホームページ（http://www.ite.or.jp）の会員の声より入力可能です．また電子メール（ite@ite.or.jp），FAX（03-3432-4675）等でも受け付けますので，是非，編集部までお寄せください．（編集委員会）