暗号モジュールの実装攻撃対策技術

Tamper-Resistant Technique for Cryptographic Modules

野崎　華恵　　藤崎　浩一　　川村　信一
■ NOZAKI Hanae　■ FUJISAKI Koichi　■ KAWAMURA Shinichi

暗号モジュールでは，本来の暗号化・復号機能に加えて，内部の秘密情報の不正読出しや機能の改変を防止する技術が求められている。最近，現実的な脅威となり始めた，暗号モジュール中の秘密鍵を巧妙に解読する実装攻撃の出現により，それに対抗できる耐タンパー技術の重要性が高まっている。

東芝は，金融系カードや電子パスポートなどの暗号モジュールの開発で耐タンパー実装に注力しており，対策と耐性評価の両面から技術力の向上を図っている。また，社会貢献の観点からも，安全性の評価基準の確立を目指した取組みを行っている。

Cryptographic modules are required to resist illegal reading of internal secret information or tampering with cryptographic functions. A tamper-resistant technique against implementation attacks, which have recently become a real threat posed by revealing the secret keys in cryptographic modules, has become increasingly important.

Toshiba has been developing and improving tamper-resistant techniques for both countermeasures and security evaluation in implementation of cryptographic modules for financial cards, e-passports, and so on. We are also aiming to contribute to the establishment of global security standards.

1　まえがき

暗号は安全なIT システムを構築するための基盤技術として，様々な応用分野に適用されている。システムの構築では，要求される安全性を保証しうる暗号アルゴリズムの採用が大前提となる。しかし，暗号アルゴリズム自体の安全性は十分でも，その実装法によって秘密情報が漏えいする危険性がある。

暗号アルゴリズムをソフトウェアやハードウェアとして実装した暗号モジュールに対する攻撃は実装攻撃と呼ばれており，各種手法が知られている。これらの攻撃に対抗して，暗号モジュール中の秘密情報の不正読出しや機能の改変を防ぐ技術が耐タンパー技術である（**図1**）。従来，暗号モジュールの開発では，高速化，小型化，低コスト化などを目指した設計に主眼が置かれていた。しかし，実装攻撃が現実的な脅威として認識され始めてから，安全性すなわち耐タンパー性の確保が，特にICカードのような小型の暗号モジュールの開発において最重要課題となっている。

東芝は，いろいろな実装攻撃に対応するために耐タンパー技術を開発している。ここでは，その技術の概要や，暗号モジュール開発での取組み，また，安全性の評価基準策定への貢献などについて述べる。

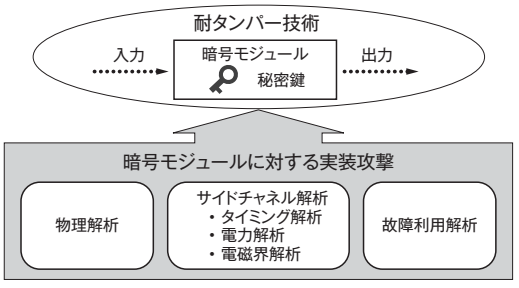

図1．暗号モジュールの耐タンパー技術 ― 暗号モジュールに対する実装攻撃に対抗して，暗号モジュール中の秘密情報の不正読出しや機能の改変を防ぐ。

Tamper-resistant technique for cryptographic modules

2　実装攻撃

暗号モジュールに対する実装攻撃は，物理解析，サイドチャネル解析，及び故障利用解析に大別される[(1)]。物理解析は破壊型攻撃とも呼ばれ，比較的古くから知られている。一方，サイドチャネル解析及び故障利用解析は非破壊型攻撃であり，1990年代後半にあいついで提案された。特にサイドチャネル解析は，処理時間や消費電力など暗号モジュールからの漏えい情報を利用して秘密鍵を推定する手法であり，攻撃が比較的容易なことから現実的な脅威となっている。

2.1　物理解析

暗号回路のパッケージを除去し，暗号回路内部を直接観測して秘密情報を推定する。代表的なプローブ解析では，ICの配線やメモリセルに探針（プローブ）を当てて，ビットの値を読み取る。プローブ解析の実行には，回路のレイアウト情報などデバイスに関する知識とともに，高度なスキルや実験設備が必要である。

2.2 タイミング解析

タイミング解析は，暗号の処理時間に基づいて秘密鍵を推定する攻撃法である。暗号処理中に秘密鍵の値に依存した条件分岐があり，かつ，分岐ごとに処理時間が異なる場合に攻撃が成立する。このような条件分岐は，処理時間の短縮やメモリサイズの削減を目的とした最適化で導入されるケースが多い。暗号アルゴリズム自体は安全でも，不用意な実装によって秘密鍵が漏えいする端的な例である。

2.3 電力解析

暗号処理中の消費電力の変動を利用して秘密鍵を推定する攻撃が電力解析である。

2.3.1 SPA　消費電力の測定波形（以下，電力トレースと言う）1サンプルに対して，波形の形状から秘密鍵を推定する。秘密鍵の値に応じて処理A又はBが実行され，かつ，処理A，Bの電力トレースがそれぞれ特徴的な形状を示す場合，波形を識別することで秘密鍵を特定できる。ただし，SPA（Simple Power Analysis）の実行には，実装アルゴリズムに関する情報をある程度必要とする。

2.3.2 DPA　暗号処理を繰り返し実行し，測定した電力トレースに対して統計処理を行い秘密鍵を推定する。ノイズや測定誤差の影響が平均化処理によって軽減されるDPA（Differential Power Analysis）は，SPAよりも強力な攻撃である。また，実装アルゴリズムの詳細を知る必要がない点もDPAの脅威を増大させている。

DPAでは，秘密鍵に依存した暗号処理中間データの値を推定し，その推定値と電力トレースとの相関を計算する。推定が正しかった場合は高い相関が得られ，秘密鍵に依存した処理のタイミングで相関値にピークが生じるが，推定がまちがっていた場合，有意な相関は得られない。よって，相関ピークの有無から秘密鍵を特定できる（**図2**）。

2.4 電磁界解析

電磁界解析では，消費電力の代わりに電磁界の変動を利用して秘密鍵を推定する。攻撃原理は電力解析と同じであり，SEMA（Simple Electromagnetic Analysis）とDEMA（Differential Electromagnetic Analysis）が存在する。電磁界解析の特徴は，暗号回路の局所的な電磁界の変動を観測する点にあり，電力解析よりもS/N比（信号と雑音の比）に優れた解析ができる。

2.5 故障利用解析

暗号処理中に電圧変動などの外乱を与えて一過性の計算誤りを発生させ，出力される異常な演算結果に基づいて秘密鍵を推定する。故障の誘発には，放射線やレーザ照射，電圧印加などの実験設備を要する。また，実装アルゴリズムの特定の処理に合わせて，意図した故障をタイミングよく発生させる必要があるため，攻撃の難度は高い。

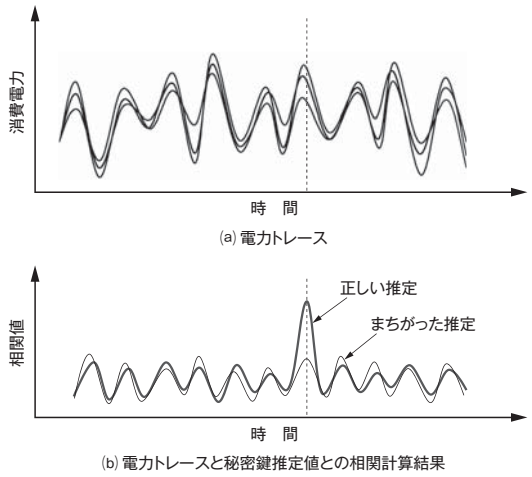

図2. DPAの攻撃原理 — 秘密鍵を推定しながら電力トレースの統計処理を行うと，推定が正しかった場合，相関値にピークが生じる。

Principle of Differential Power Analysis (DPA) attack

3 実装攻撃への対策技術

実装攻撃に対する対策技術を，設計レベルに分けて述べる。

3.1 ハードウェアレベルの対策

物理解析に対してはハードウェアレベルの対策が重要であり，電圧検知，温度検知，周波数検知など各種センサの搭載が有効である。また，パッケージを物理的に除去しようとするとICチップ自体が壊れるコーティングなど，破壊行為を妨げる技術も開発されている。

故障利用解析に対してもセンサーの組込みが有効であるが，高度なスキルを持っている攻撃者に対しては，後述する実装アルゴリズムレベルでの対策との併用が要求される。

電力解析や電磁界解析は，内部信号の値が消費電力や電磁界の変動として観測されることを利用する。よって，内部信号の値によらず消費電力を一定化する，ノイズを付加して変動を見えにくくするなどの対策が考えられる。ただし，ノイズの付加は統計処理を用いるDPAやDEMAの本質的な対策になりえない，ハードウェア対策は回路規模やコストの増大を招くなどの理由から，電力解析や電磁界解析に対しては次節で述べるアルゴリズムレベルの対策が不可欠となっている。

3.2 実装アルゴリズムレベルの対策

DPAやDEMAに対する現実的な対策は，暗号処理の中間変数を乱数によってランダム化する手法である。これにより，秘密鍵の推定が正しい場合でも電力トレースとの相関は得られなくなり，秘密鍵の特定が困難になる。

SPAやSEMAに対しては，秘密鍵の値に依存した処理を依存しない処理に置き換える処置が必要である。そのような変更がアルゴリズム的に困難な場合は，ダミー演算の追加によって擬似的に同じ処理を実行させる。

タイミング解析に対する対策はSPAやSEMA対策と同じであり，秘密鍵に依存した条件分岐を排除する，ダミー演算を追加して処理時間を一定にする，などの対策が求められる。

故障利用解析に対しては，データの偶奇性を調べるパリティチェックなどを使った，一般的な誤り検出の適用が考えられる。暗号アルゴリズム固有の対策としては，計算誤りの有無を確認するため検算も有効である。計算誤りが検出された場合は，発生したタイミングや値などの情報を漏えいさせない処置も必要になる。

以上のように，実装攻撃への対策手法は，処理時間，回路の規模とメモリサイズ，コストなどを犠牲にしなければ実現が困難な技術ばかりである。性能やコストの悪化を最小限に抑えて十分な耐タンパー性をいかに実現するかが，暗号モジュール開発での大きな課題と言える。

4　暗号モジュール開発での取組み

これまで述べてきたように，ここ十数年で，サイドチャネル解析を中心に暗号モジュールに対する実装攻撃は急激に拡大しており，各種攻撃に対する十分な安全性の確保が暗号モジュールメーカーの急務となっている。

暗号モジュールの開発では，攻撃を無効化若しくは攻撃の脅威を十分低減しうる対策手法の開発が最重要課題である。それと同時に，考案した対策の有効性の確認も開発プロセスに欠かせない要素となる。この耐性評価では攻撃と同等の解析を行うが，攻撃者との違いは，より安全サイドからぜい弱性の有無を確認するために，網羅的な耐性評価が要求される点にある。また，考案した対策固有のぜい弱性が存在しないかを確認する目的で，既存攻撃の改良や新規攻撃も検討する必要がある。

すなわち暗号モジュールの開発では，対策考案，耐性評価，攻撃検討をサイクルとして回しながら，耐タンパー性の向上を図っていくことが重要である（**図3**）。

当社は，暗号モジュールの開発を進めており，金融系カードや電子パスポート向けに，共通鍵暗号の米国標準DES（Data Encryption Standard），AES（Advanced Encryption Standard）や，公開鍵暗号のデファクトスタンダードであるRSA暗号(注1)やだ円曲線暗号などの耐タンパー化を行っている。特に金融向けICカードは，耐タンパー性基準に関する業界認定を取得するとともに，情報セキュリティ国際評価基準であるCC（Common Criteria）の最新Ver.3.1について，業界標準の評価保証レベルEAL4+の認定を受けている。

当社は，設計上流段階におけるアルゴリズムレベルの対策開発と耐性評価にも取り組んでいる。現実的な脅威がもっとも高いとされる電力解析をターゲットとして，実装効率のよい対策法や，設計上流段階における耐性評価手法の開発に注力している。特に耐性評価に関しては，計算機シミュレーションによるDPA耐性評価モデル[2]，DPAでの鍵判定効率を向上させる評価手法[3]，及びRSA暗号に対するタイミング解析の改良[4]などの提案を行っている。

（注1）　Rivest，Shamir，Adlemanの3人が開発した公開鍵暗号方式。

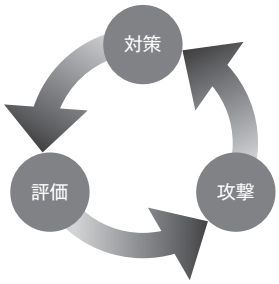

図3．暗号モジュールの開発プロセス — 対策考案，耐性評価，攻撃検討を繰り返すことで，耐タンパー性を向上させる。

Process of cryptographic module development

5　耐タンパー性の評価基準

5.1　標準化動向

2001年に発行されたFIPS（Federal Information Processing Standard）140-2は，暗号モジュールの安全性に関する米国連邦標準規格であり，これに基づいてISO（国際標準化機構）/IEC（国際電気標準会議）19790が2006年に制定された。国内でも，ISO/IEC 19790に準拠した“暗号モジュール試験及び認証制度”の正式運用が，独立行政法人 情報処理推進機構によって2007年から開始されている。

現在，FIPS 140-3への改定作業がNIST（米国国立標準技術研究所）によって進められている。現行のFIPS 140-2では考慮されていない，サイドチャネル解析に対する安全性要件の規格化に向けて，日本でも財団法人 日本規格協会の下部組織であるINSTAC（情報技術標準化研究センター）を中心に，NISTへの提言や意見交換を行っている。

5.2　標準プラットフォーム開発

サイドチャネル解析の提案以降，攻撃法や対策手法に関する多数の論文が発表されている。しかし，特に初期の論文に共通する問題として，攻撃の脅威や対策の有効性を第三者が客観的に判断できないという状況が生じた。この原因は，提案手法を独自の実装プラットフォームに適用した結果が報告されていることにあり，サイドチャネル解析に対する安全性評価基準の検討を困難にする要因の一つになっている。

この状況を受け，安全性評価基準の策定には共通の実装プラットフォームに対する解析データの蓄積が不可欠であるという認識に立ち，標準プラットフォーム開発の動きが始まってい

る。国内では，INSTACによるサイドチャネル解析評価用標準ボードの開発を先駆けとして，独立行政法人 産業技術総合研究所と東北大学の共同によるSASEBO（Side-channel Attack Standard Evaluation Board）の開発にその思想が引き継がれている。

当社は，INSTAC標準ボードの仕様開発に主要メンバーとして参画するとともに，同ボードに対するDPA実証実験を通して，耐タンパー性評価基準確立への貢献を目指している。以下，DPA耐性評価事例[5]について述べる。

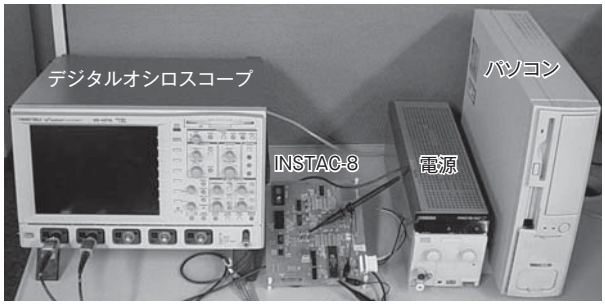

図4. DPA実験環境 — 評価用標準ボードINSTAC-8で暗号処理を実行させ，オシロスコープで測定した消費電力をパソコンで解析する。
Experimental setup of DPA

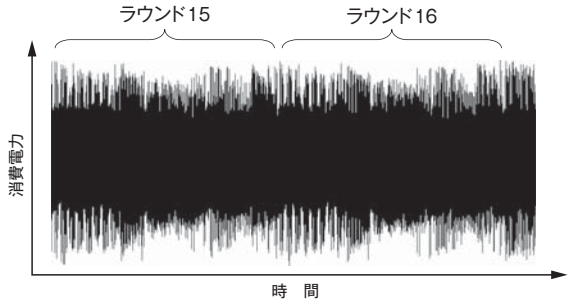

図5. DES暗号化の実行中に測定した電力トレース — DESの繰返し処理（ラウンド1～16）の2回分に対応した波形パターンを目視でき，暗号処理の内部信号に依存した消費電力波形が測定されている。
Power consumption during Data Encryption Standard (DES) encryption

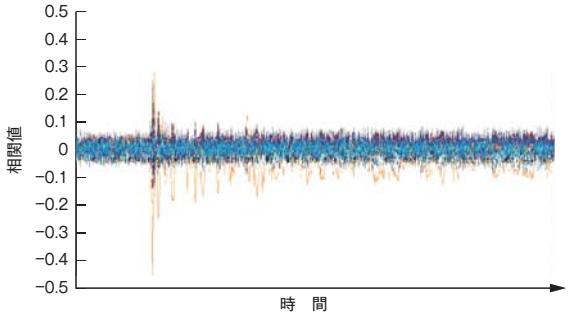

図6. 測定した電力トレース3,000サンプルに対するDPAの実行結果 — DPAを実行し，鍵候補ごとの相関値を色を変えて表示している。絶対値として最大を示すオレンジ色が正しい鍵の相関値である。
DPA correlations for secret key candidates

8ビットCPU搭載のサイドチャネル解析評価用標準ボードINSTAC-8を用いたDPA実験環境を**図4**に，また，DES暗号化の実行中に測定した電力トレースを**図5**に示す。

測定した電力トレースに対するDPAの実行結果を**図6**に示す。DESの6ビット部分鍵の全候補に対する相関計算を行った結果，正しい鍵でピークが出現しており，秘密鍵が特定されたことを意味する。DPA対策として，3.2節で述べた中間変数のランダム化処理を施すと図6の相関ピークは消え，DPA耐性が実現する。

6　あとがき

暗号モジュールに対する実装攻撃は発展途上にあり，今後もより強力な攻撃へと進化が続くことが予想される。製品仕様の制約のなかで引き続き耐タンパー性を向上させていくには，十分な安全性レベルの下限を見極めて，実装性能とのバランスを追求することが不可欠になると考えられる。そのためにも，当社が取り組んでいる対策と耐性評価の両面で，攻撃の進化を常に視野に入れながら，耐タンパー技術力の強化に更に注力していく。

文　献

(1) 神永正博，ほか．情報セキュリティの理論と技術．東京，森北出版，2005，218p.
(2) 川村信一，ほか．“サイドチャネル解析への耐性評価モデル”．2001年 暗号と情報セキュリティシンポジウム（SCIS）．大磯，2001-01，電子情報通信学会 情報セキュリティ研究専門委員会．2001，p.519－524.
(3) 三宅秀享，ほか．“S-BOXの特性を利用したDPA評価手法”．2005年暗号と情報セキュリティシンポジウム（SCIS）．舞子，2005-01，電子情報通信学会 情報セキュリティ研究専門委員会．2005，4E1-1（CD-ROM）.
(4) Tomoeda, Y., et al. An SPA-based Extension of Schindler's Timing Attack against RSA using CRT. IEICE Transactions on Fundamentals of Electronics. **E88-A**, 1, 2005, p.147－153.
(5) 藤崎浩一，ほか．8bitCPUを対象とした電力解析用評価環境の開発と実証実験．電子情報通信学会技術研究報告．**104**，200，2004，p.95－102.


野崎　華恵　NOZAKI Hanae, Ph.D.
研究開発センター コンピュータ・ネットワークラボラトリー 主任研究員，理博。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.


藤崎　浩一　FUJISAKI Koichi
研究開発センター コンピュータ・ネットワークラボラトリー 研究主務。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.


川村　信一　KAWAMURA Shinichi, D.Eng.
研究開発センター コンピュータ・ネットワークラボラトリー研究主幹，工博。暗号及びセキュリティ技術の研究・開発に従事。電子情報通信学会，情報処理学会，IACR，SITA会員。IEEEシニア会員。
Computer & Network Systems Lab.