耐タンパー暗号モジュールの安全性評価を効率化する組込み型相関電力解析

Built-in Determined Sub-Key Correlation Power Analysis for Efficient Security Evaluation of Tamper-Resistant Cryptographic Modules

駒野　雄一　　清水　秀夫　　川村　信一
■KOMANO Yuichi　■SHIMIZU Hideo　■KAWAMURA Shinichi

ICカードなどに組み込まれる電子デバイスで暗号処理を実現する暗号モジュールには，内部の秘密鍵の漏えいや機能の改変を防ぐための対策として，耐タンパー技術が用いられる。

東芝は，製品の開発段階において耐タンパー技術の安全性評価を効率化することができる組込み型相関電力解析（BS-CPA：Build-in Determined Sub-Key Correlation Power Analysis）を開発した。BS-CPAを利用して暗号モジュールの脆弱（ぜいじゃく）性を効率よく発見することで，工程の後戻りと製品コストを削減することができる。

Tamper-resistance techniques are required to protect cryptographic modules against the extraction of secret keys and the conversion of functions.

Toshiba has developed BS-CPA (built-in determined sub-key correlation power analysis), which makes it possible to rapidly evaluate the security of cryptographic modules early in the development process for devices such as integrated circuit (IC) cards and so on.　BS-CPA can reduce the impact of process retrogression and decrease device costs through efficient detection of the vulnerability of cryptographic modules.

1　まえがき

暗号と情報セキュリティは，情報システムの安全性と信頼性を高めるために不可欠な技術であり，様々な分野に応用されている。暗号処理を行う回路やプログラムをひとくくりにしたものを暗号モジュールと呼び，通信内容の秘匿や改ざん防止を実現するために，クレジットカードや電子パスポートなどに組み込まれている。暗号モジュールには，アルゴリズムの安全性が十分に検証された暗号方式が実装される。しかし，実装の特性や不備を解析して，暗号モジュール内部の秘密鍵を不正に入手する実装攻撃が存在する。実装攻撃への対策技術は耐タンパー技術と呼ばれている。

東芝は，耐タンパー暗号モジュールの開発と製品への応用を進めている[1]。耐タンパー暗号モジュールの開発では，開発中のモジュールの脆弱性を早期に発見し，設計にフィードバックするための情報を得る安全性評価技術が重要になる。

ここでは，耐タンパー暗号モジュールの開発における安全性評価技術の位置づけと，当社が安全性評価の一部を効率化するために開発している独自技術である“組込み型相関電力解析（BS-CPA：Build-in Determined Sub-Key Correlation Power Analysis）”[2]について述べる。

2　暗号モジュールへの実装攻撃

暗号モジュールに対する実装攻撃の例を**図1**に示す。

実装攻撃は物理的攻撃，サイドチャネル攻撃，及び故障利用解析に分類される。以下に，それぞれの特徴について述べ，サイドチャネル攻撃がもっとも実施しやすく大きな脅威であると考えられていることを示す。

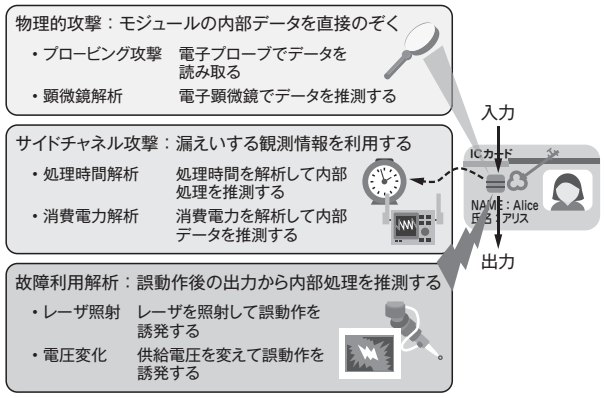


図1．暗号モジュールに対する実装攻撃 ― それぞれの実装攻撃の脅威を見積もり，耐タンパー暗号モジュールを開発する必要がある。
Attacks against cryptographic module

2.1　物理的攻撃

暗号モジュールのパッケージを剥がして基板上の配線やメモリセルを露出させ，電子プローブや電子顕微鏡を利用して秘密鍵を直接観測する攻撃である。パッケージの剥離や観測場所の特定には，特殊な機材や技能，及び攻撃対象モジュールの実装に関する知識が必要である。

2.2　サイドチャネル攻撃

暗号モジュール動作時の処理時間や消費電力を観測し，統

計処理して秘密鍵を特定する攻撃である。サイドチャネル攻撃にはオシロスコープなどの機材が必要となるが，攻撃に必要な機材を物理的攻撃よりも少ないコストで準備することができる。また，攻撃対象モジュールの実装に関する知識が十分でなくても攻撃できることから，物理的攻撃に比べて攻撃を実施しやすい。

2.3　故障利用解析

暗号モジュールにレーザを照射したり供給電圧を変化させたりして誤動作を誘発し，暗号モジュールの出力から秘密鍵を特定する攻撃である。

故障利用解析に必要な機材のコストは誤動作の誘発方法ごとに異なる。例えば，レーザ照射を伴う攻撃ではパッケージを剝離するために特殊な機材が必要になるが，供給電圧変化を伴う攻撃には特殊な機材を準備する必要はない。しかしいずれの攻撃においても，適切なタイミングと箇所で誤動作を誘発する必要があり，故障利用解析では攻撃対象モジュールに関する知識と，特殊な技能が不可欠で，実装攻撃の中でもっとも実現が困難である。

3　暗号モジュールの安全性評価

3.1　暗号モジュールの認定制度

暗号モジュールの実装に関しては，米国の商務省国立標準技術研究所（NIST）がFIPS 140-2（Federal Information Processing Standard 140-2）を標準文書として定めている。NISTとカナダのCSEC（Communications Security Establishment Canada）は，製品に搭載される暗号モジュールがFIPS 140-2に準拠することを保障する制度として，暗号モジュール評価プログラム（CMVP）を共同で設立している。CMVPでは，NIST及びCSECが認定した評価機関が暗号モジュールを試験し，試験報告に基づいて，暗号モジュールがFIPS 140-2に準拠することをNIST及びCSECが認定する。

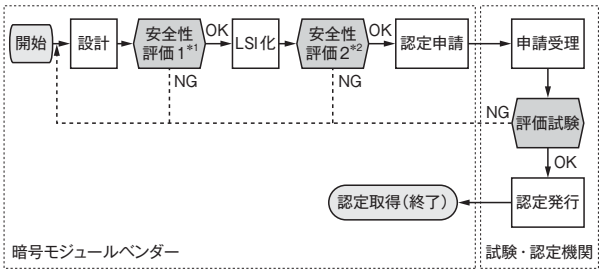
わが国でも，独立行政法人 情報処理推進機構（IPA）がJCMVP（Japan CMVP）を運用し，暗号モジュール実装の認定制度を確立している。多くの業界で第三者による認定を取得することが暗号モジュールの調達要件とされており，暗号モジュールベンダーには認定を取得できるモジュールの開発が求められている。

3.2　暗号モジュールの開発プロセスと安全性評価

暗号モジュールの開発プロセスを**図2**に示す。

認定申請では，所定の申請文書を作成する必要があり，試験機関の評価試験にも時間を要することから，評価試験後の後戻りを削減するために暗号モジュールベンダーは，認定申請前に内部で安全性評価を実施する。

暗号モジュールベンダー内部の安全性評価でも，早期に脆弱性を発見できれば工程の後戻りを削減できるため，工程の合間に安全性評価を複数回にわたり実施する。後工程で脆弱性が発見されたときに，後戻りを惜しんで付加的な対策が施されると，回路規模や消費電力などの増加による製品コストの増大につながるおそれがある。そのため，シミュレーションデータを用いて設計段階早期に性能を評価することは，製品コストを削減するための重要な役割を担っている。当社でも内部評価を活用しながら，暗号モジュールの開発を行っている。



OK：評価，試験に合格
NG：評価，試験に不合格

*1：シミュレーションによる評価
*2：実機観測データによる評価

図2．暗号モジュールの開発プロセス — 暗号モジュールベンダーは，設計開発段階に独自試験を実施することで，脆弱性を早期に発見して工程の後戻りを減らすとともに，本質的な改善を実現する。

Process of cryptographic module development

4　BS-CPA

4.1　CPAの概要

代表的なサイドチャネル攻撃として相関電力解析（CPA：Correlation Power Analysis）[3]が広く研究され，耐タンパー暗号モジュールの安全性評価にも利用されている。CPAの攻撃手順を**図3**に示す。

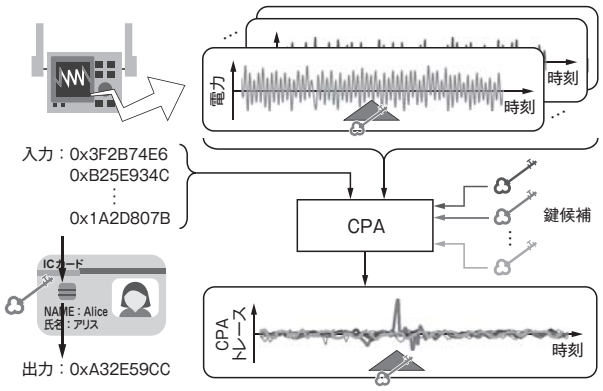


図3．CPAの攻撃手順 — 攻撃者は攻撃対象モジュールに複数の入力を与えて電力波形を収集する。その後，入力と鍵候補から内部状態を推定し，推定値と消費電力波形の相関を計算する。高い相関を示す鍵候補を暗号モジュールの秘密鍵と推定して出力する。

Process of CPA

CPAにおいて，鍵候補が暗号モジュールの秘密鍵に一致する場合は，推定した内部状態が暗号モジュール内部で処理される実際の状態に一致する。一方，鍵候補と秘密鍵が異なる場合は，推定した内部状態と暗号モジュール内部で処理される実際の状態とが異なる。一般的に，暗号モジュールの消費電力は，暗号モジュールの内部状態に依存する。そのためCPAでは，鍵候補が秘密鍵に一致する場合にだけ内部状態の推定値と消費電力との相関が高くなり，暗号モジュールの秘密鍵を推定することができる。

4.2 CPAの課題

暗号モジュールの秘密鍵の鍵候補の数が多い場合，鍵候補ごとに相関を計算することは計算量的に困難である。そこでCPAでは，暗号モジュールの処理単位で秘密鍵を部分鍵に分割し，部分鍵の候補に対して相関を計算する。

例えば，標準暗号（AES：Advanced Encryption Standard）[4]の秘密鍵は128ビット（要求する強度に応じて192ビット，256ビットも選択可能）であり，秘密鍵の候補数は2^{128}となるため，全ての鍵候補について相関を計算することは事実上不可能である。ところが，AESは実装効率を高めるために，内部では8ビット単位でデータが処理される（ただしその後，処理単位をまたいでデータを攪拌（かくはん）し，一連の処理を繰り返すことで強度を高めている）。そこで，秘密鍵を8ビットの部分鍵に16分割し，部分鍵ごとにCPAを実施する。このとき，一つの部分鍵の候補数は2^8（=256）であるため，全ての鍵候補について相関を計算できる。秘密鍵全体を推定するためには，部分鍵の個数だけ解析を繰り返せばよく，相関を256×16（$=2^{12}$）回計算することになるが，2^{128}よりも大幅に計算回数を削減できる。

しかしCPAでは，着目していない15個の部分鍵から計算される内部状態に起因する消費電力がノイズ成分として作用する。そのため，有意な相関を得るためには入力（消費電力波形）の数を増やす必要があるが，前述した安全性評価を実施する際に，波形のシミュレーションに多くの時間を要したり，波形の取得数に制限があったりする場合には，脆弱性を見過ごしてしまうおそれがある。

4.3 BS-CPAの戦略と効果

4.3.1 BS-CPAの戦略　BS-CPAは，安全性評価や評価試験で用いられるCPAに必要となる消費電力波形の数を削減する技術である。BS-CPAは，以下の二つの戦略を採用する。

(1) 既知の部分鍵を利用して推測する内部状態のビット数を増やす。

(2) 部分鍵を組み込むごとに消費電力波形を再利用する。

AESに対するBS-CPAを例に，戦略(1)の概要を**図4**に示す。

図4では，部分鍵1と部分鍵2に対応するデータの状態を推定する。部分鍵1と部分鍵2の鍵候補を同時に調べる場合には（図4(a)），$(2^8)^2$（=65,536）通りについて状態を推定しなければならない。部分鍵2が既知の場合には（図4(b)），データ2は部分鍵2から一意に計算される。そのため，部分鍵1の鍵候補として2^8（=256）通りを考え，それぞれで状態を推定すればよい。

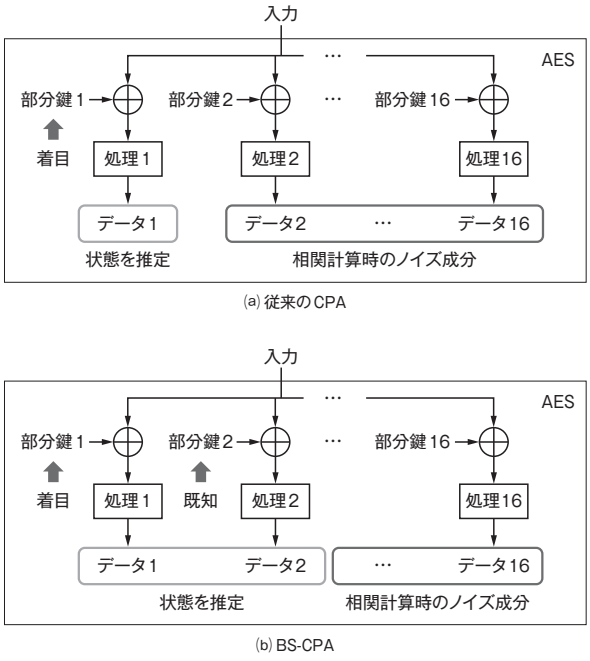


図4．既知鍵を組み込むCPA ― 従来のCPAでは，着目しない部分鍵に対応するデータは解析のノイズ成分になる。BS-CPAでは，既知の部分鍵に対応するデータを推定する状態に加え，ノイズ成分を削減することで解析効率を向上させる。

CPA using determined sub-keys

戦略(2)では，部分鍵を順番に特定する際に消費電力波形を再利用する。この戦略が効果を発揮するのは，部分鍵ごとに解析に必要な消費電力波形の数が異なる場合である。相関の計算では，推移性が成り立たない。例えば，系列Aと系列Cの相関及び系列Bと系列Cの相関と，系列（A+B）と系列Cの相関に依存関係がない。そのため，既知の部分鍵を組み込んで新たな系列（A+B）を推定すれば，その部分鍵を特定するために利用した波形系列Cを再利用したとしても，新たな部分鍵を特定することができる。

4.3.2 BS-CPAにおける鍵の特定手順　前述の戦略に基づき，BS-CPAでは以下の手順で鍵を特定する。

(1) 既知の部分鍵を内部状態の推定に組み込み，未知の部分鍵それぞれを並列にCPAで探索する。ある部分鍵が特定されたら，以下の処理を実行する。

(2) 未知の部分鍵が存在する場合，特定された部分鍵を既知の部分鍵に追加し，解析に用いる消費電力波形を初期状態に戻し，(1)の処理に戻る。

(3) 全ての部分鍵が特定されたら，処理を終了する。

4.3.3 BS-CPAの効果

BS-CPAの戦略(1)により，それぞれの部分鍵の解析に必要な消費電力波形の数を削減できる。更に，戦略(2)により，解析に必要な消費電力波形の総数を削減できる。

開発したBS-CPAの効果をDPA（Differential Power Analysis）コンテスト[5]で確認した。DPAコンテストは，Télécom ParisTech大学が主催するサイドチャネル攻撃の技術を競うコンテストで，参加者は公開された消費電力波形にサイドチャネル攻撃を行い，解析に必要な波形数を競う。BS-CPAは，CPAで必要になる消費電力波形を40％以上削減し，2009年4月にもっとも効率の良い解析手法となった。その後ルールの改定を経て，2009年8月に，公開された消費電力波形から攻撃に適した波形を選ぶことを許すという条件の下で結果を競う第4部門で，もっとも効率の良い解析手法に選ばれている。

5 あとがき

ここでは，暗号モジュール開発時の安全性評価を効率化する手法として，BS-CPAについて述べた。BS-CPAを利用して暗号モジュールの脆弱性を効率的に発見することで，工程の後戻りを減らし，製品コストを削減できる。BS-CPAの戦略をCPA以外の解析手法にも適用することで，それらの解析手法を用いる安全性評価の効率を向上させることができる。

文 献

(1) 野崎華恵 他. 暗号モジュールの実装攻撃対策技術. 東芝レビュー. 64, 7, 2009, p.28－31.
(2) Komano, Y. et al. BS-CPA: Built-In Determined Sub-Key Correlation Power Analysis. IEICE Transactions on Fundamentals. E93-A, 9, 2010, p.1632－1638.
(3) Brier, E. et al. "Correlation Power Analysis with a Leakage Model". Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2004. LNCS 3156, Cambridge, MA, USA, 2004-08, Springer, p.16－29.
(4) FIPS 197: 2001. ADVANCED ENCRYPTION STANDARD (AES).
(5) DPA contest. "Welcome to the DPA contest website". ＜http://www.dpacontest.org/home/＞, (accessed 2011-09-21).

駒野 雄一 KOMANO Yuichi, D.Sci.
研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー研究主務，博士（理学）。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，IEEE，IACR会員。
Computer Architecture & Security Systems Lab.

清水 秀夫 SHIMIZU Hideo, D.Eng.
研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー主任研究員，博士（工学）。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，日本セキュリティ・マネジメント学会会員。
Computer Architecture & Security Systems Lab.

川村 信一 KAWAMURA Shinichi, D.Eng.
独立行政法人 産業技術総合研究所 情報セキュリティ研究センター副研究センター長，工博。暗号技術及び暗号応用システムの研究・開発に従事。
National Institute of Advanced Industrial Science and Technology