平成 14 年度

耐タンパー性調査研究委員会報告書

平成 15 年 3 月

財団法人　日本規格協会

情報技術標準化研究センター

目次

1. 耐タンパー性評価技術の標準化動向

電子商取引や動画像コンテンツ配信などのサービスを実現するシステムは、暗号技術やデジタル署名などの情報セキュリティ技術を基盤として構築されている。しかし、そのようなシステムは暗号化・復号・署名生成のための鍵をはじめとする秘密情報を厳重に管理することが非常に重要である。このため、耐タンパー性を有する暗号モジュールの重要性が日増しに高まっている。耐タンパー性を有するモジュールとは、暗号化・復号・署名生成のための鍵をはじめとする秘密情報や秘密情報の処理メカニズムを外部から不当に観測・改変することや秘密情報を処理するメカニズムを不当に改変することが極めて困難であるように意図して作られたハードウェアやソフトウェアのモジュールである。

米国では、暗号モジュールの実装面での安全性評価をいち早く重視し、1995 年から FIPS に定め、ＩＴ応用システム、製品業界の指導を進めてきた。具体的には、1994 年に NIST が暗号モジュールのセキュリティ要件を規定した FIPS-140(Security Requirements for Cryptographic Module)を発行し、1995 年からカナダと共に FIPS-140 を基にした暗号モジュール評価制度 CMVP(Cryptographic Module Validation Program)により、暗号モジュールの評価・認定を行っている。CMVP では、暗号アルゴリズムが正しく実装されているかどうかの評価と暗号モジュールの耐タンパー性の評価により暗号モジュールの認定を行っている。現在では、200 を超える製品が CMVP のもとで評価・認定されている。また、英、独、仏などの諸外国も独自の評価基準を持ち、政府調達品などの評価を行っている[付録１]。一方、わが国では、耐タンパー性評価基準すら確立されていないのが現状である。

耐タンパー性評価基準の国際標準はこれまでのところ存在しなかった。このため、製品のグローバルな流通を考えた場合に様々な弊害が生じていた。しかし、平成 14 年の 10 月の ISO/IEC JTC1 の会合において、米国が FIPS 140-2 のニューワークアイテムとしての提案を行った。この提案には、英、仏、独の情報セキュリティ先進国も注目しており、ISO 標準化提案の成り行きには十分な注意が必要である。なお、米国の提案に関する審議が順調に進んだ場合、平成 15 年にはワーキングドラフトとして承認され、平成 16 年には IS 発行となる。

以上より、わが国でも早期に耐タンパー性評価基準を確立、国内標準化を進め、国内での安全なシステム構築を推進するとともに、国際標準化においてもわが国の基準の折込を狙いつつその推進の一翼を担う必要がある。

2. 活動状況

2.1. WG 発足経緯

日本では経済産業省・総務省主導による CRYPTREC 活動の元、公募された暗号アルゴリズムの安全性評価が進められ、電子政府向けの安全な暗号アルゴリズムのガイドラインがまとめられつつある。しかし、暗号応用システムを調達する側にとってみれば、安全性が評価され確認された暗号アルゴリズムであることの確認だけでは十分ではなく、その暗号アルゴリズムが正しく実装されているかどうかの確認、および実装された暗号アルゴリズムの改ざん防止や暗号化鍵の秘匿など、実装面での安全性のレベルを確認する必要が有る。

このような暗号技術の実装面での安全性に関する評価基準の策定や、その安全な実装を実現する耐タンパー技術の研究開発促進が日本として急務との認識の下、日本規格協会主催の第６回ＩＴ標準化戦略委員会・幹事会（平成１３年１２月２６日）へ耐タンパー性調査研究を新規調査研究テーマとして、提案し了承された。

その後、横浜国大・松本教授に委員長就任を要請、了承いただくとともに、事務局を日本規格協会とし、また国内 IT 製品開発主要企業の協力を確認の上、調査研究を進める体制案を策定、平成１４年１月２１日のＩＴ標準化戦略委員会へ「耐タンパー性調査研究のための WG」設置の提案を行った。提案内容は次のとおり。

[活動の目的]

耐タンパー技術の調査及び耐タンパー性評価技術の調査を実施し、システムや製品の耐タンパー性に関する客観的な評価尺度の確立するとともに、耐タンパー性評価に関するガイドライン（JIS TR の発行）を作成することを通じて、実装面でも安全なシステムや製品の開発・普及を促進し、国際的な競争力を 醸成するするとともに電子政府や高セキュリティを求められる民間システムの安全性向上に貢献する。

2.2. **活動体制**

「耐タンパー性調査研究」メンバ一覧

（委員長）	松本　勉	横浜国立大学大学院
（幹事）	才所　敏明	株式会社東芝
（委員）	小松　文子	日本電気株式会社
	近藤　潤一	三菱電機株式会社
	瀬戸　洋一	株式会社日立製作所
	鳥居　直哉	株式会社富士通研究所
	山岸　篤弘	情報処理振興事業協会
（オブザーバ）	川村　信一	株式会社東芝
	栃窪　孝也	株式会社東芝
	網島　和博	情報処理振興事業協会
	石田　修一	株式会社日立製作所
（事務局）	山中　正幸	財団法人日本規格協会

2.3. 今年度の活動成果

今年度は短時間の技術討議ではあったが、攻撃技術・耐タンパー技術についての代表的論文の精読と専門家による討議を行い、今後の具体的議論に不可欠な技術の内容、現状や動向についての共通認識を得ることができた。

また、このような個々の技術論文内容の討議だけでなく、その整理・体系化についても討議を行い、攻撃技術・耐タンパー技術の一つの整理の視点、整理の方向性を、技術体系案として提示できた。今後の議論のスタートラインを設定できたと考える。

以上の活動を通じ、攻撃技術や耐タンパー技術についての各社技術者・研究者の議論の場を創設できた。

耐タンパー性確保が現状では実装ノウハウに強く依存しているがために、会社の枠を超えた攻撃技術や耐タンパー技術に関する議論は難しいとの見方もあったが、本 WG での活発な議論を通じ、その不安は払拭された。

具体的成果物は以下の通り。

①耐タンパー関連主要論文要約

②技術の体系化の試案

１）耐タンパー関連主要論文要約

調査対象論文の分野は、以下の通り。成果である個々の論文の要約は第４章を参照いただきたい。

侵入型解析法関連（２件）
フォールト・ベース攻撃(２件)
タイミング攻撃（１件）
共通鍵暗号系に対する電力解析攻撃(３件)
公開鍵暗号系に対する電力解析攻撃（４件）
アタックの拡張（3 件）

２）耐タンパー技術体系試案作成

＜暗号モジュールに対する解析のモデル案＞

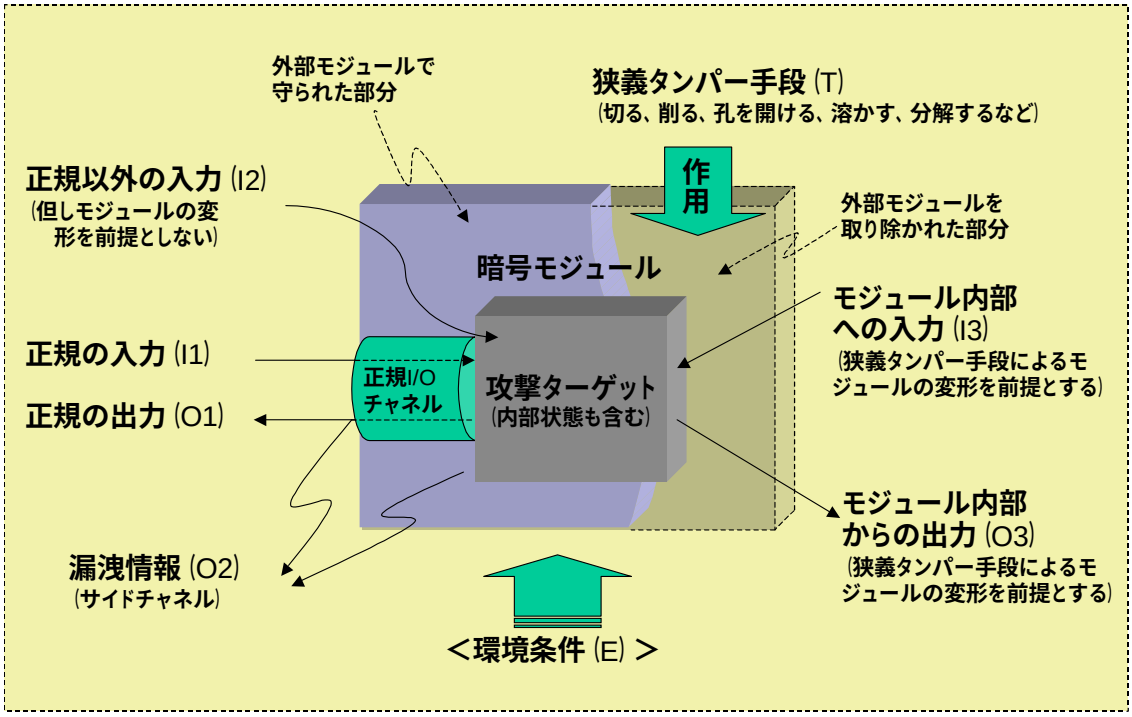


図１．１　暗号モジュールに対する解析のモデル

表１．１　暗号モジュールへの操作の分類

		内容	具体例
入力	正規の入力 (I1)	正規I/Oからの想定された信号入力	各種データポートからの入力、キーパッドからの入力など
	正規以外の入力 (I2)	正規I/Oからの規格外の信号入力、およびモジュールの変形を前提としない信号やエネルギーの注入	規格外の電圧の信号、規格外の周波数の信号 モジュール外から電界、磁界、電磁波、放射線などを照射
	モジュール内部への入力 (I3)	狭義タンパー手段に基づくモジュールの変形を前提として入力される信号	プローブ用ニードルによるターゲットへの直接信号入力 ターゲットへの光・電磁波、分子線、イオン線の直接照射など
出力	正規の出力 (O1)	正規IOからの想定された信号出力	各種データポートからの出力、液晶パネルやディスプレイへの表示、音の出力など
	漏洩情報 (O2)	正規IOからの想定外の漏洩情報、およびモジュールの変形を前提としない内部からの漏洩情報	処理時間変化、消費電力の変化、輻射電磁波など、いわゆるサイドチャネル情報
	モジュール内部からの出力 (O3)	狭義タンパー手段に基づくモジュールの変形を前提として取り出される信号	回路パターンの解析（入力を必ずしも必要としない）、 プローブ用ニードルによる内部信号観測、 ターゲットモジュールからの輻射電磁波の観測、温度変化の観測など
狭義タンパー手段 (T)		モジュールの変形を起こすための物理的、化学的、または機械的手段	切る、削る、孔を開ける、溶かす、分解するなど
環境条件 (E)		モジュールを取り巻く環境条件	温度、光、大気の組成 定常的な磁界、電解の印加など（非定常な印加はI2に分類）

＜攻撃に使用する入出力による攻撃手法の分類の試み＞

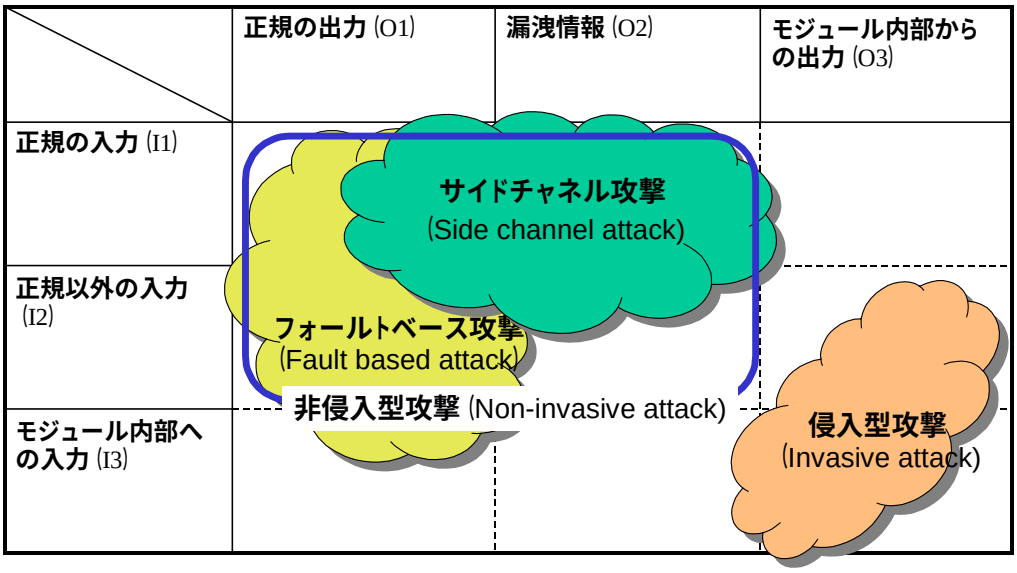


図１．２　攻撃に使用する入出力による攻撃手法の分類

＜対策の分類の試み＞

表１．２　対策の分類

カテゴリ	対策例
防止	モジュールや筐体を堅牢に構成、筐体内を樹脂で充填、チップ表面を金属膜などでシールドする、回路構造を複雑にする、規格外の信号をフィルタ、アクセス制御など
検知	各種センサー：狭義タンパー手法による物理的作用を検知、外部からの規格外の信号の検知、フォールトの検知（誤り訂正符号、検算）など
反応	メモリー内容のクリア、機能の自己破壊、警報による報知など
痕跡	攻撃の痕跡が残す仕組み：特殊シールによる封印、モジュールへのアクセスログなど
低減	漏洩情報の低減 （※漏洩情報は上記、「防止」から「痕跡」までの対策では必ずしもカバーされない）

2.4. 来年度以降の活動予定

今年度は、攻撃技術・耐タンパー技術についての議論を軌道に乗せることができた。今後さらに議論と調査研究を進め、わが国の耐タンパー技術力強化と IT 製品への適用を促進するとともに、新たな耐タンパー性評価の視点を把握、ISO の場へ日本から提案、本分野でのわが国の国際貢献と、日本の IT 製品の国際競争力強化を狙う必要がある。

具体的には、次の活動が必要と考えられる。

(ア) 日本としての攻撃技術の体系化の深耕

学界・産業界での先端研究の調査・追試を通じ、攻撃技術の最新状況を把握、攻撃技術の体系の見直しと細分化を続け、日本としての攻撃技術の体系確立を目指す。

(イ) 先進諸国の耐タンパー技術力の評価

欧米先行企業・機関の想定攻撃技術の調査・追試を通じ、先進諸国の耐タンパー技術や評価基準の攻撃技術へのカバレッジを把握、対応が不十分な攻撃技術や、新たな脅威として可能性がある未検討の攻撃技術の抽出を目指す。

(ウ) 日本独自の耐タンパー技術の深堀

先進諸国で不十分あるいは未検討の攻撃技術に対し、調査・試作・検証を通じ、日本としていち早く耐タンパー技術を獲得、日本の IT 製品への早期実装を目指す。

(エ) 日本独自の評価の視点の提案

日本の優れた IT 製品の安全性が適正に評価されるよう、評価基準や、評価技術についての調査研究を進め、国際標準への折込を目指す。

3. 耐タンパー性概説

3.1. 耐タンパー性とは

電子商取引や動画像コンテンツ配信などのサービスを実現するシステムは、暗号技術やデジタル署名などの情報セキュリティ技術を基盤として構築されている。しかし、そのようなシステムは暗号化・復号・署名生成のための鍵をはじめとする秘密情報を厳重に管理することが非常に重要である。このため、耐タンパー性を有するモジュールの重要性が日増しに高まっている。耐タンパー性を有するモジュールとは、暗号化・復号・署名生成のための鍵をはじめとする秘密情報や秘密情報の処理メカニズムを外部から不当に観測・改変することや秘密情報を処理するメカニズムを不当に改変することが極めて困難であるように意図して作られたハードウェアやソフトウェアのモジュールである。ハードウェアに対する耐タンパー技術としては、以下のようなものが知られている。

- 暗号処理回路とメモリなどの１チップ化
  暗号処理回路とメモリ回路を別の LSI にすると、インタフェース回路パッド部分や配線部分を流れる信号を解析されてしまうため、１チップ化することでインタフェース回路パッド部分や配線部分の解析を困難にする。

- モジュール表面のコーティング
  外部から回路パターンが判別できないようにモジュールの表面をコーティングする。また、攻撃の痕跡が残るようなコーティングを行うことにより、攻撃を検知することもできる。さらに、剥がすと回路パターンまで壊れてしまうようなコーティングも存在する。

- クロック周波数の異常を検出
  モジュールが誤動作を起こすまでクロック周波数を変化させるという攻撃を防ぐため、クロック周波数の異常を検出し規定周波数以外ではモジュールが動作しないようにする。

- 電圧の異常を検出
  モジュールが誤動作を起こすまで電圧を変化させるという攻撃を防ぐため、電圧の異常を検出し規定電圧以外ではモジュールが動作しないようにする。

- バスのスクランブル
  バスを流れる信号の解析を困難にするため、バスを流れる信号のスクランブルを行う。スクランブル以外にもダミーの信号を流すことにより解析を困難にす

ることができる。

- LSI 検査パッドの除去
  LSI の機能検査用のアドレスパッドなどがあると内部動作を解析しやすいので、検査終了後には検査用のアドレスパッドを除去する必要がある。

- 光検知によるメモリの消去
  光を検知する回路を組み込み、LSI の回路パターンなどを露出させると光を検知し、メモリに記憶されていた秘密情報やプログラム等を消去する。

- 消費電力の変動を抑える実装
  消費電力の変動を調べることで内部の秘密情報が解析されることを防ぐため、消費電力の変動を抑える実装が必要となる。

- 処理時間の変動を抑える実装
  処理時間の変動を調べることで内部の秘密情報が解析されることを防ぐため、処理時間の変動を抑える実装が必要となる。

また、ソフトウェアに対する耐タンパー技術としては、以下のものが知られている。

- 実行コードの暗号化
  コードを暗号化し、実行時に必要な部分のみがメモリ上に復号するようにすることで、ディスアセンブルなどの静的解析を困難にする。

- 難読化
  対象となるコードを等価でかつ分かりにくいコードに置き換えることでディスアセンブルなどの静的解析を困難にする。

- 改ざん検出コードの挿入
  処理をバイパスするなどのモジュール改ざんを防ぐために、モジュールの Hash 値を随時検証するメカニズムを組込む。

- デバッガ検知コードの挿入
  デバッガが起動されているかをモニターするコードを埋め込み、実行時にデバッガが起動されている場合にはモジュールを強制終了する等の処理を行うこと

でデバッガによる動的解析を防ぐ。

3.2. 耐タンパー性へのニーズ増大

暗号技術を基礎としたシステムは、システムで使われる機器で鍵などの秘密情報が安全に守られているという前提のもとに成り立っている。したがって、耐タンパー性に関連する市場としては、IC カード市場や電子認証などの暗号技術を基礎とした市場全体が対象と考えられる。

02 年度の IC カードの国内市場規模は前年からほぼ倍増の 3654 万枚。今後、クレジットカードや鉄道の乗車券などで多く使われるようになり、05 年度は 3 億 7540 万枚、10 年度は 7 億 5270 万枚に達すると予測している。金額ベースでも、02 年度が 182 億 7000 万円だったのが、05 年度は 1126 億 2000 万円、10 年度が 1505 億 4000 万円と急速な普及を予測している。

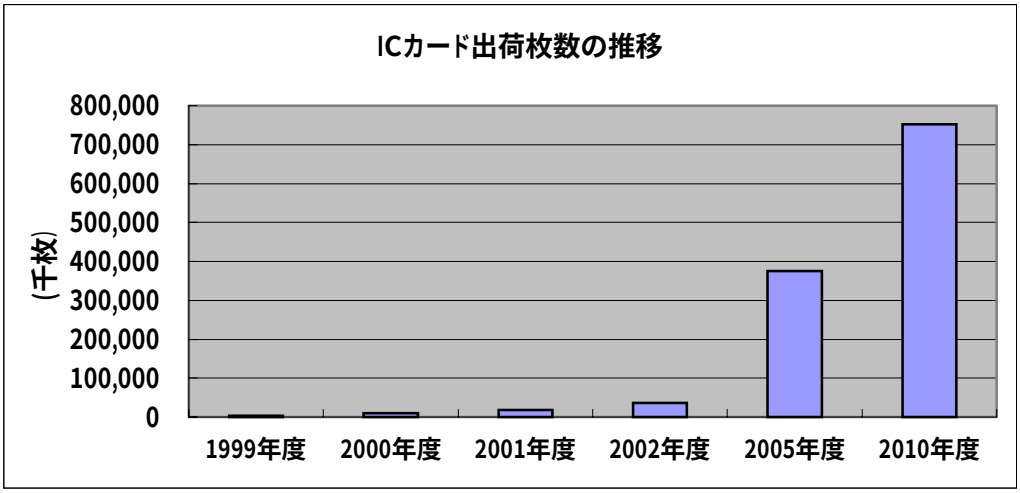


図２．１　IC カード出荷枚数予測（矢野経済研究所調べ）

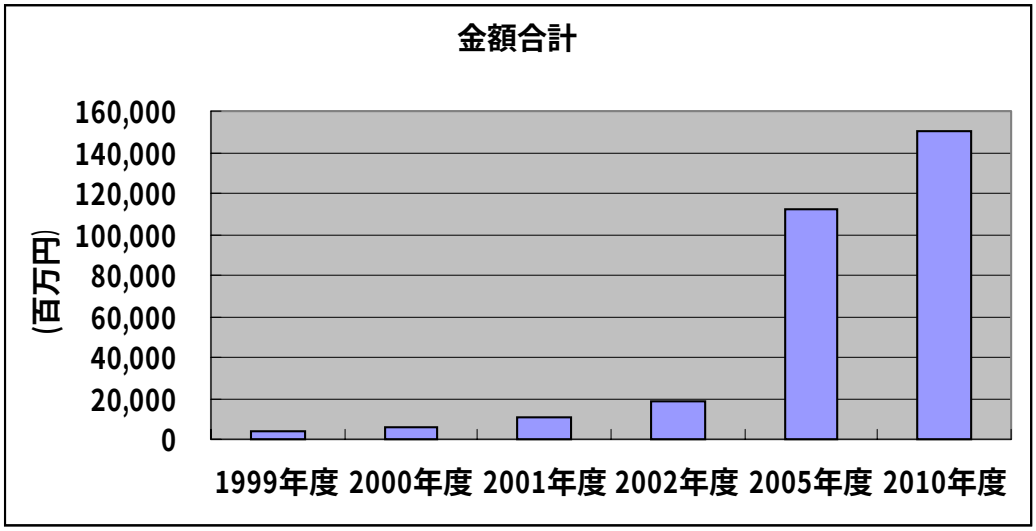


図２．２　IC カード出荷枚数予測（金額ベース）（矢野経済研究所調べ）

金融分野では民間金融機関と郵便貯金が年内に IC カードの規格共通化を目指しており、将来的にキャッシュカード、クレジットカード、電子マネーを 1 枚のカードで賄えるようになるという。また、行政分野で来年 8 月から住民基本台帳カードで IC カードが導入されており、交通分野で既に導入した JR 東日本以外でも IC カード化を検討している。また、物流分野でバーコードの代わりに IC タグを利用する動きが高まっており、ファストフード店や地域商店街で IC カードを利用した決済やポイントサービスを導入する動きが出ている。これに伴い、IC カード用チップの国内市場規模も 02 年度の 4019 万個（160 億 7800 万円）から 05 年度に 4 億 1294 万個（1032 億 3500 万円）、10 年度に 8 億 2797 万個（1324 億 7500 万円）と大幅な拡大傾向にある[7]。

次に、CA 関連製品や鍵管理装置などのさまざまな耐タンパーモジュールが使われている電子認証ビジネスの市場規模を考える。総務省が行った電子認証ビジネス市場規模調査では、現在、最も広く利用されている公開鍵基盤（Public Key Infrastructure）による電子認証ビジネス市場を「電子証明書関連サービス（個人向け）」、「電子証明書関連サービス（法人・団体等向け）」、「ソフトウェア」の 3 領域に分けこれを調査対象とし、我が国の主要な電子認証ビジネス事業者に対するアンケート及びインタビュー結果から、それぞれの市場について平成 18 年（2006 年）度までの市場規模を予測し、これをベースに市場に影響を与える促進要因を加味して推計している。平成 13 年（2001 年）度の電子認証ビジネス市場規模は約 63.4 億円と推計され、未だ電子認証ビジネスは立ち上がりの段階であることが示唆されている。しかし、今後の電子認証ビジネス市場規模は順調に拡大する事が予想され、平成 18 年（2006 年）度には約 419.5 億円にまで市場規模が拡大するものと予測されている。

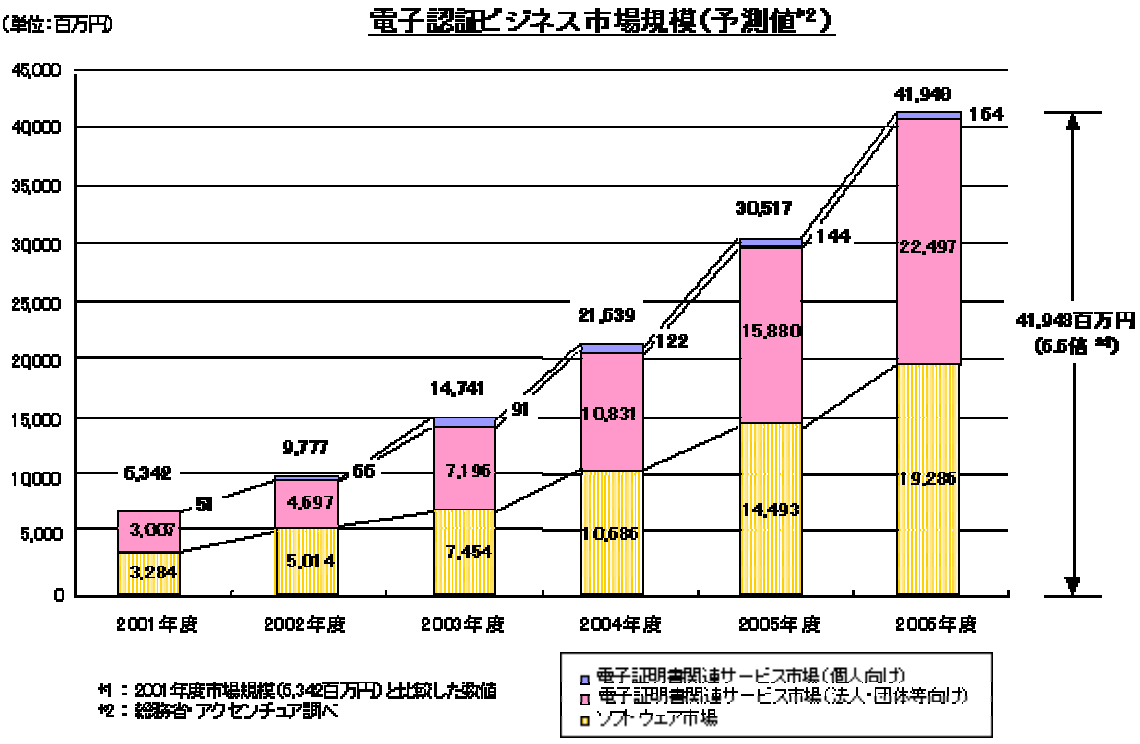


図２．３　電子認証ビジネスの市場規模予測（総務省調べ）

そして、調査の結果、平成 15 年（2003 年）度に開始される「電子政府」が電子認証ビジネス市場の拡大に果たす役割として非常に大きいことが予想されており、電子政府の要因を考慮しない場合に比べて、その効果は約 2.5 倍あることが推定されている[8]。

その他にも DVD プレーヤや DVD を再生する PC ソフトウェアなどにも耐タンパー技術は使われている。IC カードの市場や電子認証ビジネスは耐タンパー性評価関連の市場のごく一部であることを鑑みても、耐タンパー性へのニーズは計り知れない。

3.3. 耐タンパー技術が抱える課題

これまで述べてきたように耐タンパー技術は、安全なシステム構築する上で欠かすことのできない技術であるが、その技術の詳細は公開されないのが普通である。その理由としては、耐タンパー技術が攻撃（タンパー）に対する対策技術なので、対策技術を公開することは攻撃のヒントを与えることになるという点や攻撃者のほうが一般に有利な分野である点が挙げられる。また、攻撃手法も必ずしもオープンになっていないのが現状である。そして、情報を公開しないがゆえに、ノウハウや情報の管理が必要になり、さらに、評価の尺度が明確でないという問題も生じる。また、実際に製品を作る場合は、対策技術とコストとのバランスも考慮する必要があるため十分な対策なされていない場合がある。なお、攻撃手法も日々進歩しているので対策技術もそれに応じて進歩させていく必要がある。

また、電子政府構想が進む中、国内の耐タンパー性評価基準が確立されていないため、暗号モジュールはメーカ独自の基準で製造されている。よって、製品の安全性にはばらつきが生じ、利用する側も安心して製品を使うことができないのが現状である。したがって、早急に国内の耐タンパー性評価基準を確立する必要がある。

4. 耐タンパー技術の体系試案

4.1. 試案作成の方針

耐タンパーモジュールを実現する技術を体系的に整理した例は、これまであまり知られていない。そこで、この章ではハードウェアで実現されたモジュールを念頭において、攻撃手法とそれに対する対策という観点から、耐タンパー技術の整理を試みる。あくまで試案であり概念的に未整理の部分もあるため、今後大幅な見直しを要する可能性があることを最初にことわっておきたい。しかし、そのような試行を重ねることによって、耐タンパー技術についての共通の認識が形作られてゆくことを期待するものである。

本報告書で展開する試案作成の方針を以下に挙げる。

（1）対象をハードウェアで実現されたモジュールに限定する。
（2）タンパーの手段を物理的・化学的・機械的作用に限定せず、広く捉える。
（3）個々の攻撃手段や対策を洗い出すのではなく、大括りの概念での整理を目指す。
（4）攻撃者が最終的に達成しようとするゴールは分類する上であまり重視しない。

これらの方針の各々について、補足説明する。

（1）のように対象をハードウェアモジュールに限定したのは、ソフトウェアの場合に比べ発表されている文献数が多く概念整理に適していると考えたからである。ソフトウェアの耐タンパー性も重要であるが、今回は対象としなかった。ソフトウェアに対する耐タンパー技術の整理は今後の課題である。

タンパーという言葉は本来、モジュールを切る、孔を開ける、削る、溶かす、分解するなど、モジュールの変形を伴う直接的な作用を指すものと思われる。本報告ではこれを狭義のタンパー手段と呼ぶことにする。しかしながら、近年多くの研究成果が発表されているサイドチャネルを用いた解析は、モジュールの変形を前提とせずにモジュール内の秘密鍵を導出しようとする手法である。このような手法も含めて耐タンパー技術を検討するためには、検討範囲を狭義のタンパー技術に限定せずに、両者を合わせて議論することが必要である。そこで、（2）に挙げたように、ここでは両者を合わせた、（広義の）タンパー技術を対象とする。

これまで個々の解析手法について論じられることはあっても、耐タンパー技術を議論する基盤となる概念の整理はあまりされていない。そこで（3）のように大括りの概念で耐タンパー技術を整理することにした。具体的な攻撃手段やそれに対応する具体的な対策を網羅的に洗い出すという作業は、今後の課題である。

攻撃者が達成しようとするゴールは幾つか考えられる。暗号のハードウェアモジュール

であれば、内部の秘密鍵情報の取り出すというゴールがまず考えられる。また、モジュールの内部状態を本来の状態から変更し、本来とは違う動作をさせることをゴールとする攻撃者も考えられる。また単にモジュールを破壊し機能を停止させることもゴールとなりうる。（4）に述べたように、今回の体系ではこのようなゴールの区別せずに、手段の分類を中心に検討した。ゴールの違いに着目した体系化も可能と思われるが、今回は範囲外とした。

4.2. 暗号モジュールに対する解析のモデル

図３．１に暗号モジュールに対する解析のモデルを示した。以下、この図を参照しながら説明を進める。

図の中央に描かれている「暗号モジュール」が解析の対象となる。暗号モジュールの具体例としては、IC カード、暗号 LSI、暗号装置などが挙げられる。

図３．１では攻撃対象となる「攻撃ターゲット」とそれを保護するための外部モジュールを区別して描いている。IC カードの場合を例にとると、IC チップが攻撃ターゲットであり、IC チップを取り巻いているプラスチックカードが外部モジュールに当たる。パッケージに収められた暗号 LSI であれば、モジュール内の LSI チップが攻撃ターゲットであり、プラスチックやセラミックのパッケージが外部モジュールとなる。暗号装置であれば、筐体は外部モジュールの一部を構成する。

暗号モジュールに備わっている正規の入出力手段を、図では「正規 I/O チャネル」として示している。暗号モジュールに対して変形などの特別の操作を加えることなく利用できチャネルであるため、解析手段の分類を考える際に最初に注目すべき個所と考えられる。

図で外部モジュールの一部を破線で描いてあるが、この部分は狭義のタンパー手段によって外部モジュールが取り除かれた部分を表しており、それ以外の部分は外部モジュールで守られている様子を表している。

外部モジュールを取り除かれた部分では、攻撃ターゲットに対して直接操作を加えたり、ターゲットから直接情報を得ることができる。一方、外部モジュールで覆われている部分についても何らかの形で攻撃ターゲットに影響を及ぼす入力を与えたり、漏洩情報が得られる可能性がある。

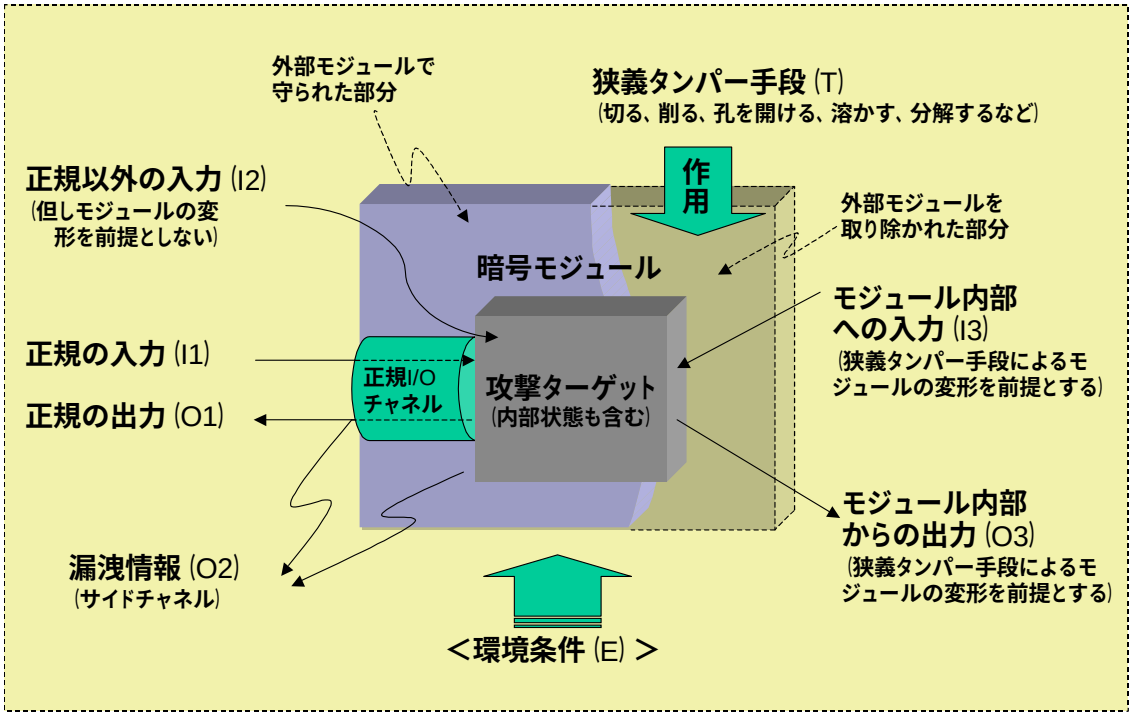


図３．１　暗号モジュールに対する解析のモデル

以上のような考察から、図３．１では攻撃者がモジュールの解析に際して使用できる操作や信号を８通りに分類し、それぞれ記号 T、I1～I3、O1～O3、E で表している。その名称を以下に挙げる：

・正規の入力（I１）
・正規以の入力（I2）
・モジュール内部への入力（I3）
・正規の出力（O1）
・漏洩情報（O2）
・モジュール内部からの出力（O3）
・狭義のタンパー手段（T）
・環境条件（E）

各々について、詳しく説明する。その要点を表３．１にまとめた。

I1：　正規の I/O チャネルからの規定通りの入力信号。各種データポートからの入力信号、キーパッドからの入力などが該当する。

I2：　I1 で規定されていない信号やエネルギーの入力である。ただし、モジュールの物理的変形などを前提とするものはここに含めない。正規の I/O から入力される規定外の信号と

して、例えば規定外の電圧や周波数を持った信号が挙げられる。また正規の I/O を利用せずに、モジュールに対して直接、電解・磁界・電磁波・放射線などを当てることで攻撃ターゲットに影響を及ぼすという手段も考えられる。

I3：　狭義のタンパー手段によって、モジュールを何らかの形で変形させた後、攻撃ターゲットへの直接的な信号やエネルギーの入力をおこなう場合がこれにあたる。具体例として、プローブ用のニードルを内部バスに接続して電気信号を送り込むことや、光や電磁波を照射すること、分子やイオンなど各種粒子線を照射することなどが挙げられる。

O1：　正規 I/O チャネルからの設計時に想定された出力信号である。各種データポートからの出力信号、液晶パネルやディスプレイへの表示、音の出力などが具体例として挙げられる。

O2：　漏洩情報を指す。正規の I/O チャネルから漏れる想定外の情報や、モジュール自身から漏洩する情報がここに含まれる。但し、モジュールの変形を前提としないものに、限定する。モジュールの処理時間の変化、消費電力の変化、モジュールから輻射される電磁波などが具体例である。

O3：　狭義のタンパー手段によって、モジュールを何らかの形で変形させた後、内部バスなどから直接得られる情報である。
　例えば、回路パターンの観察はここに含まれる。これにより配線情報、ROM 内容、ロジック内容などを読み取ることができる。また、プローブ用のニードルによって、内部信号を観測するという手段もここに含まれる。さらに、輻射される電解・磁界・電磁波・温度変化の観測も具体例である。

T：　狭義のタンパー手段であり、解析対象を切る、削る、孔を開ける、溶かす、分解するなど様々な手段が含まれる。本報告では、T は I3 や O3 を実現するための前処理と考えることにする。T の具体例を分類してゆく作業も重要であるが、本報告ではこれ以上の検討はしない。

E：　解析対象を取り巻く環境条件であり、温度や光、大気の組成などが含まれる。また、定常的な電界や磁界の印加などもここに含める。非定常な印加は I2 に含めるのが良い。E についても T 同様に、本報告ではこれ以上の検討をしない。

　次節ではここに挙げた８つの項目の内、T と E を除く I1～I3、O1～O3 に着目して攻撃を分類する。

表３．１　暗号モジュールへの操作の分類

		内容	具体例
入力	正規の入力 (I1)	正規I/Oからの想定された信号入力	各種データポートからの入力、キーパッドからの入力など
	正規以外の入力 (I2)	正規I/Oからの規格外の信号入力、およびモジュールの変形を前提としない信号やエネルギーの注入	規格外の電圧の信号、規格外の周波数の信号 モジュール外から電界、磁界、電磁波、放射線などを照射
	モジュール内部への入力 (I3)	狭義タンパー手段に基づくモジュールの変形を前提として入力される信号	プローブ用ニードルによるターゲットへの直接信号入力 ターゲットへの光・電磁波、分子線、イオン線の直接照射など
出力	正規の出力 (O1)	正規IOからの想定された信号出力	各種データポートからの出力、液晶パネルやディスプレイへの表示、音の出力など
	漏洩情報 (O2)	正規IOからの想定外の漏洩情報、およびモジュールの変形を前提としない内部からの漏洩情報	処理時間変化、消費電力の変化、輻射電磁波など、いわゆるサイドチャネル情報
	モジュール内部からの出力 (O3)	狭義タンパー手段に基づくモジュールの変形を前提として取り出される信号	回路パターンの解析 (入力を必ずしも必要としない)、 プローブ用ニードルによる内部信号観測、 ターゲットモジュールからの輻射電磁波の観測、温度変化の観測など
狭義タンパー手段 (T)		モジュールの変形を起こすための物理的、化学的、または機械的手段	切る、削る、孔を開ける、溶かす、分解するなど
環境条件 (E)		モジュールを取り巻く環境条件	温度、光、大気の組成 定常的な磁界、電解の印加など (非定常な印加はI2に分類)

4.3. 操作の組合せと対応する典型的攻撃手法

前節で列挙した操作手段 I1～I3、O1～O3 の６種類の組合せによって具体的な解析が構成されるとものとして、解析手法を整理する（図３．２）。回路パターンの観察のように、解析手段として入力を要しない場合もあるが、ここでは入力無しの場合を別扱いにすることはせず、入力３種類・出力３種類に対応する合計９通りのパターンを考える。

原理的にはこれら９通りすべての場合について、対応する解析手法を構成できると考えられるものの、現実的にはすべての組合せが一様に重要という訳ではない。幾つかの代表的な解析手法を、表の特定の領域に対応付けることができると思われる。

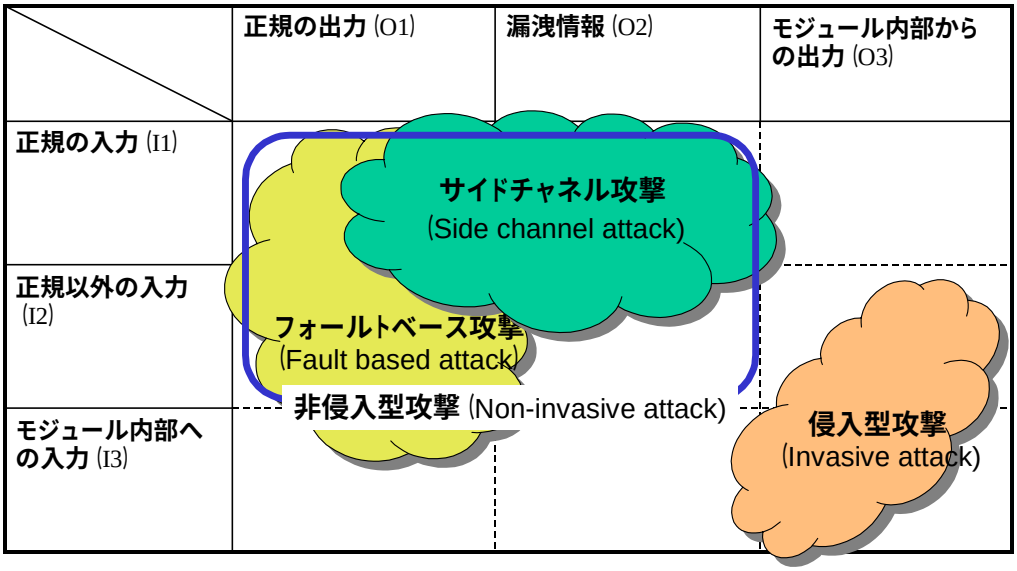


図３．２　攻撃に使用する入出力による攻撃手法の分類

例えば、サイドチャネル攻撃で主として使用する出力情報は O2 である。また、その時利用する入力情報は、原理的には I1、I2、I3 のいずれの可能性もある。しかし、サイドチャネル攻撃はモジュールの変形を起こさずに解析できる場合に意味があるため、典型的なサイドチャネル攻撃を考える場合、モジュールの変形を必要とする I3 を除外して良い。さらに、I1 と I2 を比較した場合には、不正の検知がより難しいという意味で、正規の入力 I1 のみを与えるサイドチャネル攻撃がより重要である。従って、サイドチャネル攻撃の典型例は、（I1、O2）の組を利用する場合と考えられる。図３．２では（I1、O2）を中心とする雲形図形でサイドチャネル攻撃を図示した。また、雲形が（I1、O2）からはみだしているのは、それ以外の組合せでもサイドチャネル攻撃がありうることを示唆している。

これと同様の考察により、典型的なフォールトベース攻撃は（I2、O1）の組合せで実現される。ここでも雲形図形により（I2、O1）以外の組合せの存在を示唆している。

また、侵入型攻撃（Invasive attack）と呼ばれる解析手法は、もともと狭義のタンパーを前提とするモジュール内部への解析を指しているため、（I3,O3）の組合せが最も典型的な場合と考えられる。I3 の関係する行と、O3 が関係する列以外は、モジュールの変形を要さない攻撃になるので、その部分は非侵入型攻撃（Non-invasive attack）として図示した。

4.4. 対策の分類

この節では対策の分類について考える。狭義のタンパー手法への対策として、検知（detection）、反応（response）、痕跡（evidence）といったカテゴリ分けがこれまでに知られている。今回は広義のタンパーを考察の対象としていることに対応して、これら３つのカテゴリに加えて防止（block）と低減（reduction）という２つのカテゴリを追加する。以下、各カテゴリについて説明する。表３．２にその内容をまとめた。

・防止（block）

筐体などモジュール自体を狭義のタンパー手法に対して十分堅牢にしておく。この対策が有効ならば、I3 または O３が関係する攻撃手法は防ぐことができる。

チップレベルでは部分的に回路を解析から守るために、回路表面に何らかのシールドを施すといった対策も考えられる。また、回路パターンを観察しようという攻撃者に対しては、回路構造を複雑にすることで観察を困難にする手段も考えられる。これらはいずれも O3 に対する防御手段の例である。

なお、I1 の入力に対しては、それが正規の入力であるかどうかを確認する手段が必要である。例えば、規格外の信号をモジュール内へ通過させないフィルタがその例である。また、パスワードはじめ様々なアクセス制御機構も、正規の入力以外を防止するための確認手段と考えられる。

・検知（detection）

（I1,O1,O2）以外の手段を組合せた解析の場合には、原理的には何らかの異常を検知することが可能と思われる。異常の検知手段として、各種のセンサーが用いられる。

I3,O3 が前提としている狭義のタンパー手段に対しては、物理的変形を引き起こす作用を検出することが可能と考えられる。圧力センサーや温度センサーがその例となる。

I2 の場合には、物理的変形を検出する手段は用いることができないので、それ以外の異常を検知する必要がある。外部から規格外の信号が入力された場合には、それを検知する。電圧や周波数についての異常を検知することは可能である。

I2 を利用する解析手段の典型例として前節で挙げたフォールトベース攻撃であれば、フォールトを誘起する外部からの作用を検知するか、そうでない場合でも誘起されたフォールトを検出する手段が有効と考えられる。演算結果の検算や、誤り検出符号の利用が考えられる。

ここまで（I1,O1,O2）以外の手段を用いる解析について考察したが、（I1,O1,O2）を用いる解析の場合でも、検知できる可能性はある。例えば、差分電力解析（DPA=Differential Power Analysis）を行う場合、いくつかの入力に対応する電力波形を採取する必要がある。そのために解析にあたっては、短時間の内に暗号化処理のような特定の処理を多数回呼び出すことが考えられる。これを異常として検出できる可能性がある。

・反応（response）

解析されていることをモジュール自身が検知した場合には、攻撃を無効にするための何らかの反応が必要である。

メモリー内容をクリアする、モジュールの機能の一部または全部を自ら破壊する、何らかの不正を検知したことを警報により報知するなどが、その例として挙げられる。

・痕跡（evidence）

解析が試みられた場合に、仮に解析を防ぐことができないとしても、解析があったことを痕跡として残すという対応は有効である。

たとえば、筐体に特殊なシールを用いて封印をし、攻撃者が筐体の分解を試みた場合には、本体は元に戻せたとしてもシールの復元が困難であるため痕跡が残る、という対策がある。

既に挙げた検知・反応によりメモリー上にモジュール自身が痕跡を記録するといった手段も考えられる。モジュールの処理履歴（ログ）も、このような対策のひとつと考えられる。

・低減（reduction）

ここまでの対策は、漏洩情報（O2）の直接的な対策にはなっていない。いわゆるサイドチャネル攻撃の多くに対して、ここまでの対策は必ずしも有効ではない。漏洩情報に対する直接的な対策としては、漏洩情報そのものを低減することが考えられる。漏洩情報をノイズによって隠蔽する方法も今回はここに含めることにする。

表３．２　対策の分類

カテゴリ	対策例
防止	モジュールや筐体を堅牢に構成、筐体内を樹脂で充填、チップ表面を金属膜などでシールドする、回路構造を複雑にする、規格外の信号をフィルタ、アクセス制御など
検知	各種センサー：狭義タンパー手法による物理的作用を検知、外部からの規格外の信号の検知、フォールトの検知（誤り訂正符号、検算）など
反応	メモリー内容のクリア、機能の自己破壊、警報による報知など
痕跡	攻撃の痕跡が残す仕組み：特殊シールによる封印、モジュールへのアクセスログなど
低減	漏洩情報の低減 （※漏洩情報は上記、「防止」から「痕跡」までの対策では必ずしもカバーされない）

4.5. 今後の課題

ここまで攻撃手段と対策の分類を行ってきた。これをさらに深めるには、各カテゴリに属する具体的な手段の調査を進める必要がある。また、得られた具体的な攻撃手段と対策手段とを対応付けることも必要である。このとき予想される大きな問題は、攻撃手段と対策を対応づけたとしても、対策の有効性や強度を客観的に示す指標が必ずしも得られていないことである。ある種の仮定を置いたりコストとメリットを考慮することによって、現実的な基準を作ることができると良い。その場合に、基準をどのような形で誰が作るのかも重大な課題となる。また、そのような現実的基準は恐らく時間と共に陳腐化するため常に更新してゆく必要があろう。

5. 耐タンパー関連論文調査

本年度は、付録 3 にある論文の中から選んだ下記のキーペーパーを中心に調査を行った。

◎侵入型解析法

a. R. Anderson, M. Kuhn "Tamper Resistance – a Cautionary Note"*-----2nd USENIX Workshop on Electronic Commerce, 1996*

b. O. Kommerling, M. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors", *-----USENIX Workshop on Smartcard Technology*, 1999.

◎非侵入型解析法（サイドチャネル攻撃）

(1) フォールト・ベース攻撃

c. D. Boneh, R. A. DeMillo, R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults", *-----Advances in Cryptology: Proceedings of Eurocrypt '97, and J.Cryptology, Vol.14, No.2, pp.101-120*

d. S.Skorobogatov and R.Anderson, “Optical fault induction attacks”, CHES2002

(2)タイミング攻撃

e. P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", *CRYPTO '96*

(3)電力解析攻撃

共通鍵暗号系に対する電力解析攻撃

f. P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis", *CRYPTO '99*

g. L. Goubin, J. Patarin, "DES and Differential Power Analysis", *CHES '99*

h. M.Akkar and C.Giraud, "An Implementation of DES and AES, Secure against Some Attacks", CHES'01

公開鍵暗号系に対する電力解析攻撃

【ＲＳＡ関連】

i. T. S. Messerges, E. A. Dabbish, R. H. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards", *CHES '99*

j. V.Klima, T.Rosa, “Further Results and Considerations on Side Channel Attacks on RSA”, CHES2002

【楕円曲線暗号関連】

k. [Cor99] J.-S. Coron, "Resistance Against Differential Power Analysis for Elliptic Curbe Cryptosystems", *CHES '99*
l. E. Brier and Marc Joye, “Weierstra Elliptic Curves and Side-Channel Attacks”, PCK’02

アタックの拡張

m. T. S. Messerges, “Using Second-Order Power Analysis to Attack DPA Resistant Software”----- *Proceedings of CHES '00*
n. S.Agrawal, B.Archambeault, J.R.Rao, P.Rohatgi, “The EM side-channel(s)”, CHES2002
o. Shamir, ”Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies”----- *Proceedings of CHES '00*

5.1. **侵入型解析法**

5.1.1. Tamper Resistance - a Cautionary Note(Anderson and Kuhn)

- 文献情報

発行年	1996 年
文献名	Proceeding of Second USENIX Workshop on Electric Commerce
タイトル	Tamper Resistance ― Cautionary Note
著者	Ross Anderson, Markus Kuhn

耐タンパと言われているスマートカード・ディバイスにおいても脆弱性が存在することに注意を促した論文である。解析（攻撃：Attack）例について記載されているが、解析原理・対策については解説されていない。

IBM 製品においては、耐タンパのレベルとし以下の３分類がされている。これらについての例を記述している。

クラス１　（外部の賢者）

一般的には高度の知識をもつが、対象システムに対しては不十分な知識のみもつ。

クラス２　（内部の知識を持ったもの）

実用的な教育と技術を持つ。対象システムの各部分についてはそれぞれ知識のばらつきはあるが、アクセスする可能性をもつ。

クラス３　（資金力のある組織）

資金力の背景の下に、必要な技術力をカバーしたチーム。

- 攻撃対象

シングルチップ。主にスマートカードにおける EEPROM を対象としている。

- 攻撃の原理・前提

クラス１攻撃

（１）非侵入攻撃（Non-invasive attacks）

・　PIC16C84　microcontroller,DS5000 security processor

・ 異常電圧と温度が EEPROM 書き込み操作を引き起こす。対策として、電圧や環境変化のセンサーが組み込まれているが逆に強度を低下させることもあるため注意が必要である。

・ 電源とクロック一時誤りを繰り返しにより発生させ、メモリ内をダンプすることが可能

である。

(2)物理攻撃(physical attacks)

- 溶剤（硝酸）によるチップの取り出し
- フッ化水素（hydrogen fluoride）とともに dry　etching
- 顕微鏡などを利用してプロービングする。

クラス 2 攻撃　先進的な攻撃（Advanced　Attack）

(1)　Intel　80386 を 2 週間で解析。

- Shottky effect を利用して N と P ドープ層を開示し、リバースエンジニアする手法。
- チップレイアウトや機能が開示されると次のような IBM によって開発された強力な観察手法が存在する。（電圧を監視可能な crystal of lithium niobate に置く。与えられた電荷領域（electric field）に従って対象の屈折インデックス（refractive index）が変化し、grazing　入射角（投射角？）での水晶を通過する紫外線レーザ光線によって、下位のシリコンのポテンシャルを読み出すことが可能である）
- 本解析（攻撃）に対しては Conformeal glues といわれるチップコーティングが有効と言われる。これは不透明で伝導性があるが除去に対して強い抵抗があり、FIPS においても参照されている。

(2)　FIB（focussed ion beam）　ワークステーションによる解析。

ほとんどすべての CPU とのバスが切断され EEPROM と CPU だけが残される状態で、攻撃者はマイクロプロービング針か electro-optical プローブですべての EEPROM 内容を読み出すことが可能である。

5.1.2. Design Principles for Tamper-Resistant Smartcard　Processors(Kommerling and Kuhn)

- 文献情報

発行年	1999 年
文献名	Proceeding of USENIX Workshop on Smartcard Technology (Smartcard ’99)
タイトル	Design Principles for Tamper – Resident Smart processors
著者	Oliver Koemmerling, Markus Kuhn

- 攻撃対象

シングルチップ。主にスマートカードにおける EEPROM を対象としている。

スマートカードプロセッサより、保護されたソフトウェアおよびデータを抽出する技術を記述している。この技術は、手動マイクロプロービング(manual microprobing)、レーザカッティング(laser cutting),焦点イオンビーム、グリッチ攻撃（glitch）、電力分析である。

- 攻撃の原理・前提

タンパ技術を以下の４分類にしている。また、それぞれ侵入攻撃（マイクロプロービング）と非侵入攻撃（残りの３技術）としている。

- **マイクロプロービング**
  チップ表面に直接アクセスし、回路の観察、変更、干渉すること
- **ソフトウェア攻撃**
  通常のインタフェースを利用し、脆弱性を探索すること
- **盗聴**
  通常の操作中に電磁波等を監視すること
- **故障生成**
  誤動作を生成させるような異常な環境条件を利用する

- 攻撃方法

侵入攻撃

(1) スマートカードのパッケージ除去(Depackaging of smartcard)

60℃の硝酸、その他の環境によってチップパッケージを除去する。

(2) レイアウト　再構成 (Layout Reconstruction)

チップ表面を高感度の光学顕微鏡などで撮影することで、基本的なデータやアドレスバスなどの構造が速やかに識別可能である。

(3) マニュアルマイクロプロービング（　Manual Micropobing ）

侵入攻撃においては最も重要なツールが、マイクロプロービングワークステーションである。

(4) メモリ読み出し技術（Memory Read-out Techniques）

マイクロプロービングはすべてのバスとレコード、メモリの値を観察するために使用されるが、同時にすべてのデータとバスアドレスを観察することはできない。このためにいくつかの技法が使用される。ひとつは、同じトランザクションを複数回繰り返し 2-4 のプローブを使用する。プロセッサがそれぞれ同じメモリアクセスシーケンスを実行するから、部分的なバス信号を完全なものに結合できる。トランザクションの繰り返しは、プロセッサがすべてのメモリ位置にアクセスするのに充分でないこともある。（有料 TV では放送局からの署名つきメッセージによってのみ活性化されるメモリが実装されている例がある）

(5) 粒子光線技術（particle beam Techniques）

非侵入攻撃

(1) グリッチ攻撃

フリップフロップに対する誤った状態を引き起こす故障を生成させ、ほぼ任意の命令に置

換することである。多くの文献で論じられ最も有効で実際的な攻撃である。クロック信号、電力供給、外部磁場の三つの方法が知られている。この攻撃では特に条件分岐や診断命令をリプレースすること、繰り返し時間の延長、繰り返し時間の減少に利用する。
クロック信号グリッチは単純で実用的である。一時的にクロック周波数を１または 1/2 増やし、フリップフロップが新状態になる前の入力をサンプリングする。電力変動は、ゲート入力とタンパセンサーの電力閾値を上げる。

(2) 電流分析（current Analysis）
電力供給において 10-15Ωの抵抗を使うと、カードで消費される電力を AD 変換し計測できること。

- 可能な対策

1 乱数クロックシグナル（Randomized Clock Signal）
非侵入攻撃については、特定の命令が実行される時刻を予想することを要求する。各クロックで同じ入力があれば、厳密に決定できるプロセッサは常にリセットの後の同じ命令を C クロックサイクルで実行する。従って、明らかな対策としては、観察可能な動作とオペレーション間に乱数時間の遅れを挿入することである。攻撃者が相互相関関係分析をする場合もあるため、ここでは、クロックサイクルレベルでのタイミング乱数を導入することを勧める。

2 乱数マルチスレッド（Randomized multithreading）
アルゴリズム実行を決定困難にするため、命令レベルで、ランダムに複数のスレッドスケジュールリングをすること。

3 強固な低周波数センサー（ Robust Low-frequency Sensor）
低周波数の場合に、バスオブザベーションが容易になるため、一般にスマートカードに低周波数センサーが存在するが、これを不活性にすることが可能であるため、センサーへの攻撃に対してはプロセッサすべての障害とすべきである。

4 破壊的テスト回路（ Destruction of Test Circuitry）
生産工程におけるマイクロコントローラのテストのための回路が不活性な状態でテスト後もチップ上に残っているが、攻撃者はこの回路の FIB やマイクロプロービングで接続し、すべてのメモリ内容をダンプすることが可能である。したがって、テスト回路は完全に破壊しておかなければならない。

5 プログラムカウンタの制約 (Restricted Program Counter)

プログラムカウンタをアドレスパタン生成として悪用することや、分岐や呼び出し、リターン命令が実行されるプロセッサをリセットする watchdog カウンタを切り離すことは、多くのトランジスタを要求しまた、容易に不活性にできる。ここでは、アドレス空間すべてに使用するプログラムカウンタを提供しないことを推奨する。16 ビットのプログラムカウンタは、7 ビットのオフセットカウンタと 16 ビットのセグメントレジスタにすればよい。

6　最上位層のセンサーメッシュ（ Top-layer Sensor Meshes ）

実際の回路上のセンサーメッシュを形成した金属層は、いかなる信号も伝達しない。CPU ST16SF48A やバッテリバッファ SRAM である DS5002FPM,DS1954 に見られる。しかし、欠陥のあるメッシュもあり、メモリゼロ化をソフトウェアが実行する場合もある。

- 他の文献との関係

非侵入攻撃に関する、各関連論文を参照しているが特記すべき関連はない模様である。

5.2. フォールト・ベース攻撃

5.2.1. On the Importance of Checking Cryptographic Protocols for Faults(Boneh, DeMillo and Lipton)

- 文献情報

発行年	1997 年
文献名	Advances in Cryptology --- Eurocrypt '97, LNCS 1233, pp. 37--51
タイトル	On the Importance of Checking Cryptographic Protocols for Faults
著者	Dan Boneh, Richard A. DeMillo, and Richard J. Lipton

発行年	1996 年
文献名	J. Cryptology, Vol. 14, No. 2, pp. 101--119(上記論文の拡張版)
タイトル	On the Importance of Eliminating Errors in Cryptographic Computations
著者	Dan Boneh, Richard A. DeMillo, and Richard J. Lipton

- 攻撃対象

故障利用解析による

1. 公開鍵系
   - CRT を利用した RSA
   - CRT を利用しない RSA
2. 認証スキーム
   - Fiat-Shamir スキーム
   - Schnorr スキーム

に対する攻撃方法である.

- 攻撃の原理・前提

予め定められたプロトコルによって外部と通信し合うブラックボックス中の秘密情報を, ブラックボックスとの通信において得られる出力から導出する. その際, ブラックボックス内でハード的またはソフト的に生じたエラーによって間違った演算結果が出力されることを仮定しており, この間違った出力値を利用して秘密情報を推定する.

- 攻撃方法

a. 公開鍵系に対する攻撃法

以下では、RSA における公開鍵 e を, N(=pq), 秘密鍵を d, p, q, メッセージを M, 署名を S とする。

a.1 CRT を利用した RSA

$S_p(=M^d \bmod p)$ と $S_q(=M^d \bmod q)$ から

$$S = S_q + ((S_p - S_q) * (q^{-1} \bmod p) \bmod p) * q$$

によって $S(=M^d \bmod N)$ を求める CRT モードにおいて、S_p の計算時にエラーを導入し $\hat{S}_p$ とする。$\hat{S}_p$ から計算された出力 $\hat{S}$ は、$(S-\hat{S}) \bmod q = 0$ という性質を持つ。これを利用して $\gcd(S-\hat{S}, N)$ から q を求める。攻撃には S と $\hat{S}$ を用いるため、この方法では同じメッセージ M をブラックボックスに 2 回処理させる必要がある。

Lenstra による改良：1 回のべき乗剰余演算で攻撃を可能にするため、$\gcd(S-\hat{S}, N)$ の代わりに $\gcd(S-\hat{S}^e, N)$ を用いて q を求める。

- 可能な対策

1. 出力を返す前に値をチェックする --- 例えば公開鍵による RSA 署名の検証を行う. 公開鍵が短ければこの方法は効率的であるが，通常，付加的な検証はパフォーマンスの低下を招く.

CRT を利用した RSA に対しては故障利用解析が窮めて脅威的であるため,
検証を必ず行う必要があり，例えば Shamir によるテクニックが有効である.

[Shamir の方法]

乱数 r を用いて $S'_p = M^d \bmod (p*r)$ と $S'_q = M^q \bmod (q*r)$ を計算する.

$S'_p \bmod r = S'_q \bmod r$ が成り立つかどうかを判定することで，S'_p の計算中に導入されたエラーを検出する.

2. デバイスの内部状態が外部から影響を受けないようにする --- Fiat-Shamir スキームのような複数ラウンド認証スキームに対しては，デバイスの初期状態が影響を受けないようにすることが重要であり，例えばエラー検出ビットによる内部メモリの保護を行う.

3. 処理中にランダムネスを導入する --- 例えば同じメッセージに対して毎回異なる署名を作成する Bellare と Rogaway によるスキームでは，攻撃者がメッセージを知ることがで

きないため CRT を利用した RSA の対策として有効である.

- 他の文献との関係

Bellcore アタックとして知られる CRT を利用した RSA に対して 1996 年に提案された故障利用解析に関する論文であり，この後，Biham と Shamir による故障差分解析などの提案が行われるようになった.

5.2.2. Optical fault induction attacks(Skorobogatov and Anderson)

- 文献情報

Sergei Skorobogatov, Ross Anderson, ``Optical Fault Induction Attacks'', CHES2002

- 攻撃対象

ハードウェアに対する攻撃である。マイクロコントローラ、スマートカードなどのハードウェアに光を照射することによって故障を起こさせる.このため、すべてのハードウェアが攻撃対象となる。

- 攻撃の原理・前提

CMOS トランジスタでは、トランジスタに放射線を照射することによってトランジスタが導通状態となり、ソフトエラーとして知られている。同様の現象がパルスレーザーでも可能であることが報告されている。本文献では，チップ表面のトランジスタに光を照射することによってトランジスタを導通状態にし、それによってハードウェアに故障を引き起こし、これを利用して過去に報告されている故障攻撃を行う。文献で実際に行われた攻撃では、チップ表面を光に照射するために、パッケージを開け，チップを剥き出しにできることが前提である。しかし、将来的には X 線や赤外線を用いたチップ裏面からの照射も可能性として指摘されている。

- 攻撃方法

文献で報告された攻撃では、 光源として、 カメラ用フラッシュランプ、 レーザーポインタが用いられた。カメラ用フラッシュを用いたものでは、 光を照射する領域を制限するためにアルミホイルに小さな穴をあけたものを用いている。このような設備でチップ内の SRAM のメモリセルに光を照射し、 SRAM の内容を 0 にセットしたり、 1 にセットしたりできることを確認した。すなわち、 SRAM の内容を任意の値に書き換えることができることを示した。レーザーポインタを用いた方法でも、 同様の結果が得られた。実際に鍵の抽出は、 行っていないが、 このようにメモリ内容を書き換えることによって故障を起こさせることが可能であるので、

1) D. Boneh, R. A. DeMillo, R. J. Lipton, ``On the Inportance of Checking Cryptographic Protocols for Faults, Adbances in Cryptology - Eurocrypt 97'', Springer LNCS vol 1233 pp37-51.
2) R. J. Anderson, Markus G. Kuhn, ``Low Cost Attacks on Tamper Resistant Devices'', in M.Lomas et al. (ed.), Security protocols, 5th Internarional Workshop, Paris, France, April 7-9, 1997

に示されているような故障解析を適用することが可能である。また、 上記の文献で報告された実験では、 メモリセルの状態を変えることが報告されているが、 同様にレジスタの内容も書き換えることが可能であるとも指摘している。

- 可能な対策

自己同期 2 線式論理回路(Self-timed dual-rail logic の有効性が以下の論文に示されている。

1) S. W. Moore, R. J. Anderson, M. G. Kuhn, ``Improving Smartcard Security using Self-Timed Circuit Technology'', Forth AciD-WG Workshop, Gernoble, ISBN 2-913329-44-6, 2000
2) S. W. Moore, R. J. Anderson, P. Cunnigham, R. Mullins, G. Taylor, ``Improving Smartcard Security using Self-Timed Circuit Technology'', Asynch 2002, proceedings published by IEEE Computer Society Press

2 線式では、 'LL'、 'LH'、 'HL'に意味を持たせている。'LL'は、 静止状態でデータの 0/1 は、 'LH'と'HL'で表される。2 線式では、 'HH'状態が現れると、 回路全体に伝播し、 回路をロックするという特性がある。対策では、 'HH'をエラー信号とする。'HH'は、 タンパーのセンサとして意識的に生成され、 2 線式の特性として、 回路全体に伝播し、 ロックさせる。

5.3. **タイミング攻撃**

5.3.1. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems(Kocher)

- 文献情報

発行年	1996 年
文献名	Advances in Cryptology – CRYPTO'96, pp. pp.104-113
タイトル	Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems
著者	Paul C. Kocher

- 攻撃対象

Diffie-Hellman, RSA, DSS
(Further Work で共通鍵暗号への適用可能性も示唆している)

- 攻撃の原理・前提

不必要な処理のバイパス、条件分岐、RAM キャッシュヒットなど多くの原因により、各入力毎に処理時間が異なる。その原因の主となるものは、平文（もしくは暗号文）や秘密鍵によるものである。このような処理時間の微妙な違いを元に秘密鍵を求める。前提として、攻撃者はターゲットとなる製品の実装方法を知っているものとする。（実際には、タイミング情報から推測することができる）

- 攻撃方法

1. A Simple Mudular Expronentiator

Let s_0=1.
For k=0 upto w-1:
  If (bit k of x) is 1 **then**
    Let R_k=(s_k・y) mod n.
  Else
    Let R_k=s_k.
  Let s_{k+1}=R^2_k mod n.
EndFor.
Return (R_{w-1}).

Simple Modular Exponentiation Algorithm (R = y^x mod n, x: w bits)

Simple Modular Exponentiation Algorithm を使用すると、秘密鍵のビットにより処理が異なる。ビットが 1 の時は 2 乗算と乗算、0 の時には 2 乗算のみを行うという処理の違いにより、処理時間が異なるため攻撃が可能となる。

2. Montgomery Multiplication and the CRT

Modular Reduction 処理は、処理時間の差を生み出す原因となるが、特にべき乗剰余算処理中に多く起こる。Montgomery 乗算は、この影響を軽減してくれるが、多少の影響は残っているため攻撃は可能となる。

$$m_p = m \bmod p$$
$$m_q = m \bmod q$$
$$s_p = m_p^{d_p} \bmod p$$
$$s_q = m_q^{d_q} \bmod q$$
$$x = ((s_q - s_p) A \bmod q) \cdot p + s_p$$

Chinese Remainder Theorem $(x = m^d \bmod n, A = p^{-1} \bmod q)$

CRT を使った場合は、最初の 2 式などの Modular Reduction 処理が攻撃しやすい。m として p に近いと思われるものを選択し、それが実際に p より大きければ Reduction 処理が行われることで処理時間が長く、小さければ Reduction 処理が行われないので処理時間は短いということで秘密鍵である p が特定できるようになる。

3. Digital Signature Standard

$$genetare \text{ random number } k$$
$$r = (g^k \bmod p) \bmod q$$
$$s = k^{-1}(H(m) + x \cdot r) \bmod q$$

Digital Signature Standard (x: secret key)

$s = (k^{-1}(H(m) + x \cdot r)) \bmod q$ の処理において、一般に $(H(m) + x \cdot r) \bmod q$ の計算が先に行われることが多い。Modular Reduction 処理の時間が一定でないとすると、全体の署名時間は $(x \cdot r) \bmod q$ の処理時間と相関があるため、攻撃者はハッシュ値である $H(m)$ を計算しておき、その影響を除去しておく。$x \cdot r$ の MSB がまず最初に Modular Reduction に使用されるため、x の上位ビットが Modular Reduction の処理時間と相関を持つ（r の値は

既知であるため)。よって x の MSB が推測でき、同様にして下位のビットも求めていくことで攻撃が可能となる。

- 可能な対策

1.すべての処理を正確に同じにする
→コンパイラの最適化や RAM キャッシュヒットなど様々な原因により非常に難しい。

2.Ramdom Delay などを挿入することで、各処理の正確な時間が計れないようにする
→攻撃者が必要となるサンプル数が増えるだけで、完全な対策にはならない

3. Message Blinding を施す(0 入力に対してはシステム側で reject する)
→特殊な実装をしていなければ、この攻撃に耐えうるだろう。Blinding 値の計算には時間がかかるが、なるべく各入力に対して変えたほうがよい

- 他の文献との関係

Kocher の論文は、攻撃法の原理を示しているだけであり、実際に攻撃を行ってはいない。Dhem らは、RSA、Diffie-Hellman に対して、実際にタイミング解析を行い、秘密鍵を推定している[DK+98]。また、Koeune らは、Rijndael へのタイミング解析の適用方法を提案している[KQ99]。

5.4. 共通鍵暗号系に対する電力解析攻撃

5.4.1. Differential Power Analysis (Kocher, Jaffe and Jun)

- 文献情報

発行年	1999 年
文献名	Advances in Cryptology – CRYPTO'99, pp. 388–397
タイトル	Differential Power Analysis
著者	Paul C. Kocher, Joshua Jaffe and Benjamin Jun

- 攻撃対象

  DES

  概要　：暗号システムの設計者は, 秘密情報を用いた計算が行われるときには安全な環境で実行されていると仮定することがある. しかし現実にはコンピュータやマイクロチップからプロセスや命令に関する情報が漏れている場合がある. この論文は, 消費電力を用いて暗号方式が実装されているデバイスから秘密鍵を求める手法である Differential Power Analysis を提案し, 解析に成功したことを報告している. またこの解析手法に対する対策についても述べている.

- 攻撃の原理・前提

  攻撃の前提

  ・ $M_{1...m}$ の平文を暗号文 $C_{1...m}$ に暗号化する m 回の暗号化処理を観測し, その際に k 個の測定点を持つ電力波形 $T_{1...m}[1...k]$を測定できる.

  ・ 暗号化処理の結果である暗号文 $C_{1...m}$ を記録できる（平文は必要としない）.

  攻撃の原理

  DPA 選択関数（DPA selection function）$D(C,b,K_S)$ を用意する. DPA 選択関数は, DES の復号処理における第 16 ラウンドでの L の中間値を計算する関数である. b は 32bit の L のうち注目するビット位置（$0 \le b < 32$）を表す. K_s は拡大鍵のうち, b に対応する S box へ入力する 6bit 分の値（$0 \le K_s < 2^6$）を表す.

  ・ $\Delta_D[1...k]$ を計算する.

$$\Delta_D[j] = \frac{\sum_{i=1}^{m} D(C_i, b, K_S) T_i[j]}{\sum_{i=1}^{m} D(C_i, b, K_S)} - \frac{\sum_{i=1}^{m} (1 - D(C_i, b, K_S)) T_i[j]}{\sum_{i=1}^{m} (1 - D(C_i, b, K_S))}$$
$$\approx 2\left(\frac{\sum_{i=1}^{m} D(C_i, b, K_{Ss}) T_i[j]}{\sum_{i=1}^{m} D(C_i, b, K_S)} - \frac{\sum_{i=1}^{m} T_i[j]}{m} \right)$$

上式は，$D(C_i, b, K_s)$ が“1”の場合と“0”の場合の波形の平均値を計算し，その差分を求める式である．計算した Δ_D をグラフ表示すると，予想した拡大鍵が正しい場合には DPA 選択関数が計算したビットに関係のある範囲にだけスパイクが立つ（それ以外の範囲は平坦な）波形が得られる．それに対して，予想した拡大鍵が異なる場合にはスパイクの無い平坦な波形となる．電力波形とデータのビット値に関係性があるために，このような現象が起きる．

- 攻撃方法

  上記の計算（及び測定）を行い，b に対応する 8 つの K_S を求める．これにより，48bit の秘密鍵を求めることができる．残りの 8 ビットについては全数探索を行うか，次の 1 ラウンドについても同様の計算を行うことで求めることが可能である．

  論文では DES を攻撃対象とし，1000 回及び 10000 回の測定を行って攻撃を行っていた（Fig.4，Fig5）．

  T-DES の場合には，3 回目の DES で使用される鍵から求め，その求めた鍵を使用して暗号文を復号し，2 回目の DES の攻撃に使用する．

- 可能な対策
  - シグナルサイズを減少させる．
    - constant execution path code を使う．
    - ハミング重みや状態遷移を平均化する．
    - 物理的なシールドをデバイスに施す．
  - ノイズを加える．
    - 電力を平坦化する．
    - 実行のタイミングや順序をランダマイズする．
  - 実装する H/W について現実的な仮定をおいた暗号システムをデザインする．
    - ハッシュ関数を使用するなどして非線形な鍵のアップデートを行う．

- 他の文献との関係

・他の DPA に関する多くの文献の元となる論文である．

5.4.2. DES and Differential Power Analysis(Goubin and Patarin)

- 文献情報

発行年	1999 年
文献名	CHES'99
タイトル	DES and Differential Power Analysis
著者	Louis Goubin, Jacques Patarin

- 攻撃対象

共通鍵アルゴリズム、公開鍵アルゴリズム全般
（例として DES と RSA を取り上げている）

概要　　：暗号アルゴリズム中に出現する各中間変数 V を処理過程において一切登場させない。具体的には、V を復元可能な複数の変数 $V_1,\cdots,V_k$ に分割して別々に計算する。こうすることによって、攻撃者が V の値に基いて DPA を適用しても V に依存した偏りが観測されないので秘密情報が守られる。

- 攻撃の原理・前提

本論文で想定している攻撃は、以下のような ”普通の ” DPA である。

[3.1]原理

・秘密鍵に依存する中間変数の値に応じて、ターゲットチップの消費電力に差が生じる。

・中間変数の値に基いて測定データを統計処理することによって、上記差分情報が観測され、秘密鍵の値がわかる。

[3.2]前提

・処理の過程で現われる中間変数であって、秘密鍵の一部と入力データより計算可能なものが存在する。

・SPA によって測定波形のタイミング合わせが可能である。

・ターゲットチップの実装に関する特別な知識は不要。

- 攻撃方法

以下は DES を例にした攻撃方法である。

①異なる 1000 個の入力（$E_n;n=1..1000$）に対して、消費電力波形（$C_n;n=1..1000$）を測定する。また、これらの平均波形（MC）を求める。

②1 つ目の S-Box の出力に影響する 6 ビットの鍵の値を仮定する。当該 S-Box の出力の 1 ビットに着目し、仮定した鍵の値において、その 1 ビットが 0 になるか 1 になるかを計算して入力 E_n を 2 つのカテゴリに分類する。

③得られた 2 つのカテゴリのうち、一方に含まれるものの平均波形 MC'を求め、MC と MC'

を比較する。両者間に有意差が見られれば、想定した 6 ビットの鍵が正解である。有意差が見られなければ、鍵の値の仮定を変えて②を繰り返す。
④2 つ目から 8 つ目までの S-Box に対して、上記②と③の手順を繰り返す。これによって 56 ビットの秘密鍵のうち、48 ビットが特定できる。
⑤残りの 8 ビットは全数探索で求める。
（②-④において、S-Box の出力の 1 ビットだけではなく、4 ビット全てに着目して入力を 16 のカテゴリに分類し、出力が 1111 となるカテゴリの平均波形を MC'としてもよい。この場合、測定回数を増やす必要があるが、結果の信頼性が高くなる。（訳注）ビット毎に差分情報の正負が一律とならない実装もあるので、常に信頼性が高くなるわけではない。）

RSA については具体的な攻撃方法は示されていないが、"square-and-multiply"箇所で連続した中間変数の値に着目して DPA を適用することで、鍵の各ビットの値が順に特定されると述べている。

- 可能な対策

一般的な対策として、まず以下の 3 つを挙げている。
・波形のタイミング合わせを困難にするために、ランダムなタイミングシフトを挿入する。
・危険な命令を電力波形から解析するのが困難な命令に置き換える。
・与えられたアルゴリズムに対して、DPA が適用できないような実装方法を採用する。

本論文では、この最後の対策について主に検討し、Duplication Method を提案している。その基本的な考え方は、「次の条件を満たすような関数 f によって、中間変数 V を $V = f(V_1,...,V_k)$となるような $V_1,...,V_k$ に置き換える（訳注）簡単に言うと、アルゴリズムから予測される中間変数（中間状態）を処理の過程に直接登場させないことで、実装を知らない攻撃者に測定データ分類用の中間変数を計算できなくする」というもの。
条件 1：1 から k までの任意の i について、V_i がもともとの中間変数 V に依存しないこと。
条件 2：$V_1,...,V_k$ に基く変換が V を計算することなく実現できること。

（以下、DES の例）

Duplication Method の実装例として、k=2 として $V = f(V_1,V_2) = V_1 \wedge V_2$ を選んでいる。その上で、V に関する処理と V_1,V_2 に関する処理を次のように対応させる。
・V に関する線形の変換は、同様の変換を V_1,V_2 の双方に実施する。
・V と他の変数の XOR は、V_1,V_2 とそれぞれに対応する他の変数との XOR に置き換える。
（$V \wedge V' \rightarrow V_1 \wedge V_1', V_2 \wedge V_2'$ ； $V = f(V_1,V_2), V' = f(V_1',V_2'), \rightarrow f(V \wedge V') = f(V_1 \wedge V_1',V_2 \wedge V_2')$）
・V と鍵のみに依存する値との XOR は、同じ値との XOR を V_1 または V_2 の一方のみに実施する。

・S-Box による変換は、12 ビット入力の 2 つの S-Box を新設して対応させる。

（$V'=S(V)$ → $V_1' = S_1'(V_1,V_2)$, $V_2' = S_2'(V_1,V_2) = S(V_1 \wedge V_2) \wedge S_1'(V_1,V_2)$ → $V' = f(V_1',V_2') = V_1' \wedge V_2'$

；　S_1'による変換は秘密にしておく）

この実装例では巨大な S-Box が必要なため、スマートカードには適用できない。スマートカードへの実装を可能とするような変形も紹介されている。

変形 1：新設する 8 組の S-Box の S_1'を共有することで S-Box の数を減らす。（16 個→9 個）

変形 2：新設する S-Box を 6 ビット入力のものとし、その入力は変形 2 において新設するファンクション $\psi(V_1 \wedge V_2)$の出力とすることで 1 つの S-Box のサイズを減らす。

変形 3：変形 1 と変形 2 を同時に採用する。

変形 4：(V_1',V_2')を作るために、2 つの S-Box の代わりに V_1',V_2'の一次または二次の多項式を用いる。

（以下、RSA の例）

Duplication Method を適用し、"square-and-multiply"を行っている箇所を以下のように変更する。DES の例と同じく k=2 であり、$V \equiv f(V_1,V_2)=V_1 \times V_2 \pmod n$としている。

1. $z \leftarrow 1$;
   For i=m-1 downto 0
2. $z \leftarrow z^2 \pmod n$;
3. if $d_i=1$ then $z \leftarrow z \times x \pmod n$;

（通常の"square-and-multiply"）

→

1. $z_1 \leftarrow 1$;　$z_2 \leftarrow 1$;
   For i=m-1 downto 0
2. $z_1 \leftarrow z_1^2 \pmod n$;　$z_2 \leftarrow z_2^2 \pmod n$;
3. if $d_i=1$ then
   $z_1 \leftarrow z_1 \times x_1 \pmod n$;　$z_2 \leftarrow z_2 \times x_2 \pmod n$;

（Duplication Method 適用後）

ここで(x_1,x_2)、(z_1,z_2)は次の条件を満たすように選ばれる変数である。

$x \equiv x_1 \times x_2 \pmod n$　　$z \equiv z_1 \times z_2 \pmod n$

- 他の文献との関係

・攻撃方法は'98 の Kocher 等の"Introduction to Differential Power Analysis and Related Attacks"
(http://www.cryptography.com/dpa/technical/index.html にて入手可)に基く。

・本論文で示された対策（Duplication Method）は特許出願中（論文発表時）。

5.4.3. An Implementation of DES and AES, Secure against Some Attacks(Akkar and

Giraud)

- 文献情報

発行年	2001 年
文献名	CHES2001
タイトル	An Implementation of DES and AES, Secure against Some Attacks
著者	Mehdi-Laurent Akkar and Christophe Giraud

- 攻撃対象

本論文では，一般的な共通鍵ブロック暗号(特に T-DES，AES)に対する DPA を想定している．

概要　：　DES と AES へのサイドチャネル攻撃に対する対策案. masking method［1］の改良版．DES と AES に対してそれぞれ別の対策法を提案している.DES は S-box のサイズが小さいため，乱数を用いたテーブル書き換え方式を提案している.一方，AES は S-box のサイズが大きいため，DES と同様の手法を適用すると要求される RAM 領域が非常におおきくなり，Smart Card 等への実装が事実上不可能になる．そこで著者らは RAM を使用しない adapted masking method を提案している．

これらの提案におけるポイントは，データパス上で「生」の中間値を処理せずに，必ず乱数値と XOR(もしくはガロア体上の乗算)された値を用いて処理することにある．

提案されている手法の基本的な手順は以下の通り．

1．　メッセージと乱数を XOR(もしくは⊗)する．

2．　非線形関数を乱数に応じて再構築し，期待値との整合性をとる．もしくは復元可能な状態にできるような構造にする．(S-box の構造に依存).

3．　非線形出力に再び乱数と XOR し，処理を繰り返す．

4．　暗号文出力直前に乱数を打ち消し，期待値を出力する．

＊　⊕ は XOR　⊗はガロア体上の乗算を表す

- 攻撃の原理・前提

DPA の攻撃原理を簡単に説明する．ブロック暗号の鍵情報を含んだ処理の一部を F(X,K)する.F(X,K)の 1 ビットに着目し,その値が “ 1”の場合と“ 0 ”の場合の電力波形の平均値を算出し， 最終的にその差分値を求める． ここで K の値は攻撃者が想定するものを用い，X は攻撃者が任意に選んだ平文(もしくは暗号文)である． 想定した K が正しい場合には 着目したビットに関する電力差分波形において,スパイクが観測される．想定が間違っていた場合は,スパイクの無い平坦な電力差分波形となる．電力波形とデータのビット値に関係性があるために，このような現象が起きる．詳細は Paul C. Kocher らの“ Differential Power Analysis”，CRYPTO’99 を参照．

- 攻撃方法

ブロック暗号では,処理の一部に S-box と呼ばれるランダム性の高いテーブルを用いて暗号化処理を行うことが多い． この場合,S-box の入力前に拡大鍵と XOR をし,その出力を用いてテーブル参照を行う． ブロック暗号に対する DPA は S-box の入力を想定し,S-box の出力のある 1 ビットに着目した電力波形によって行うのが一般的である.詳細は Paul C. Kocher らの“ Differential Power Analysis”，CRYPTO'99 を参照.

- 可能な対策

本論文では，T-DES と AES に対する DPA 対策方法を提案している.

＜DES に対する対策＞

DES の S-box 入力が M(メッセージ)⊕ K(拡大鍵)⊕ R(乱数)となっている場合，乱数が XOR された状態で処理すると，期待値に復元するのが難しくなる．しかしながら，DES の S-box は 6 ビット入力，4 ビット出力のため，乱数に応じて少ない RAM 領域で，S-box を再構築することが可能である．図 1 に文献における DES の S-box の構築法を示す.

再構築された S-box はデフォルトの S-box(DES で定義されている S-box)に対して⊕ R 分だけずれたものとなっている．このため，M⊕ K⊕ R をテーブル参照した場合，デフォルトの S-box で M⊕ K を参照したものと同じ値となる．これにより非線形部に乱数値を用いたまま処理できるため，サイドチャネル攻撃に対しての効果が期待される.

＜AES に対する対策＞

AES も DES と同様の手法の適用が考えられるが，この場合少なくとも 256 バイトの RAM 領域が必要となる．よって，メモリ領域の制約が厳しいアプリケーションでは適用が困難になる．そこで，提案されている手法は S-box の特徴を利用して，再構築をせずに非線形部に乱数の要素を用いたまま処理可能としている. 図 2 にその手法の概要を示す. AES の S-box がガロア拡大体上の逆関数を用いて構成されているため，$(M \otimes R)^{-1} = M^{-1} \otimes R^{-1}$ が成り立つ．よってメッセージに対して乱数値を乗じたデータであれば $M^{-1} \otimes R^{-1} \otimes R = M^{-1}$ の処理で復元可能となる. 提案の手法では, さらに乱数値を S-box の入力直前と直後に XOR することで強度を高めようと試みている

＜対策の効果 （提案者らの主張）>

SPA

- 攻撃者がデータパスへの SPA によって得られる情報はマスクされた鍵情報のハミング重みだけである.

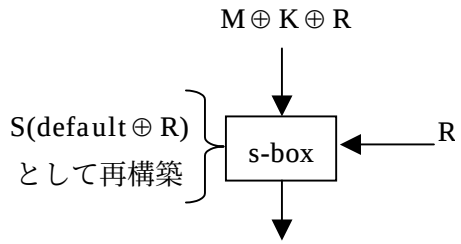


図 1　提案の DES　S-box

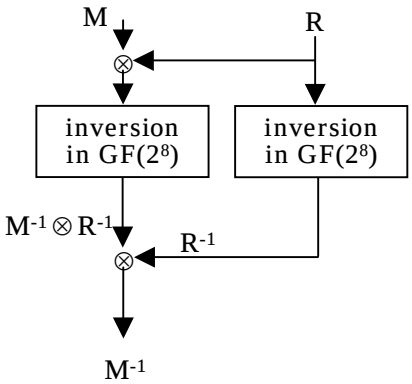


図 2　提案の AES S-box

- DES の場合，拡大鍵生成はラウンド毎に処理する必要がある．この場合，拡大鍵生成部への攻撃によって攻撃者が得られる情報は各ラウンドのハミング重みだけである．
- 毎回乱数を変えた場合，1 回の XOR，Load，Store 命令で正確なデータを導出することはできない．
- 高次の電力差分攻撃に備えるため，XOR，Load，Store 命令はランダム化したほうがより良い．

DPA

- データバス中で処理されるデータは必ず乱数値を含んだ値になっているため，中間値を予測して攻撃する DPA に対しては耐性を持つ．
- 但し，マスク値として 0ｘ00 や 0ｘFF は不適切である．
- 高次の DPA に対しては，処理する S-box の場所をランダムにすることで，耐性を高められる可能性がある．

- 他の文献との関係

Elena Trichana, Domenico De Seta, Lucia Germani “Simplified Adaptive Multiplicative Masking for AES and its Securized Implementation” CHES2002

原文を応用．　提案手法では $A+X$ を $A*X$ に変形した後，$A^{-1}*X^{-1}$ を得て $A^{-1}+X$ に変形している．S-box の表引きの際に，A の値が 0 であると，X の値に関わらず 0→0 への写像になってしまう為，後で+1 加算する代わりに S-box にあらかじめ+1 を入れ込む方法や，AES の計算前に S-box 表に乱数を XOR しておく方法なども提案．

Jovan Dj.Golic, Christophe Tymen , “Multiplicative Masking and Power Analysis of AES”　CHES2002

原文の応用．差分電力解析に対抗するため乗算マスキングを改良し，また計算量を変化さ

せることでセキュリティレベルをコントロールできることを示している.

備考　：　この論文で提案されている adapted masking method はメモリ領域を少なく実装できるため，現在この改良が盛んに研究されている．現時点では乱数との乗算時に DPA で攻撃可能なことが知られており，改良案が研究されている.

5.5. 公開鍵暗号系に対する電力解析攻撃

5.5.1. Power Analysis Attacks of Modular Exponentiation in Smartcards(Messerges, Dabbish and Sloan)

- 文献情報

発行年	1999 年
文献名	CHES '99
タイトル	Power Analysis Attacks of Modular Exponentiation in Smartcards
著者	T. S. Messerges, E. A. Dabbish, R. H. Sloan

- 攻撃対象

指数剰余演算を実装したスマートカード

- 攻撃の原理・前提

スマートカードの指数剰余演算は、モンゴメリ乗算器を用いたバイナリ法(Square-and-multiply)を用いているものとする。また、指数剰余演算回路に対し、カードメモリ上のソフトウェアプログラムを用いてアクセスできるものとする。また、このソフトウェアは、ISO7816 スマートカードプロトコルを用いており、標準的な内部認証（Inertnal Authentication）コマンドに類するコマンドをサポートしているものとする。

- 攻撃方法

1 単純な相関関係(correlation)を用いる

乗算処理時の電力信号 $S_m[j]$と、指数剰余時の電力信号 $S_e[j]$との相互相関

$$S_c[j] = \sum_{t=0}^{W} S_m[t] S_e[j+t]$$

をとる。ここで W は乗算処理時の電力信号サンプル数である。このとき、相互相関 $S_c[j]$はべき乗剰余時の乗算処理である自乗算と乗算の部分にピークが現れる実験結果が示されている。しかし、この方法では、自乗算と乗算の区別がつかないため有効な攻撃とはならない。

2 Single-Exponent, Multiple-Data(SEMD)Attack

この攻撃の前提条件は、スマートカードが、２つの指数（プライベート鍵と公開鍵）に対し任意の数の乱数を処理できることである。このような状況は、攻撃対象のスマートカードが ISO7816 をサポートしているとき起こりうる。つまり、自分のプライベート鍵を使用する通常の認証コマンド"Internal authentication"のほかに、特定のカードリーダの公開鍵を使った認証"external authentication"をサポートしている場合である。また、このカー

ドの公開鍵を攻撃者が知っていることは必要である。

この攻撃は、既知の指数の電力信号を未知のそれを比較し、指数のビット値が予想できるとしたものである。具体的には、ランダムな平文を L 個用意し、それを秘密鍵で処理した時の電力信号 $S_i[j]$と、既知の指数で処理した時の電力信号 $P_i[j]$を測定する。それぞれの平均をとりその差分

$$D[j]=\frac{1}{L}\sum_{i=1}^{L}S_i[j]-\frac{1}{L}\sum_{i=1}^{L}P_i[j]=\bar{S}[j]-\bar{P}[j]$$

を計算する。演算するタイミングは同じとしている。このとき D[j]=0 ならば j における乗算が同じであり、そうでなければ、j における演算が異なるといえる。

この攻撃が有効なことを 64 ビットの指数剰余演算の実験で確認している。この場合、20000 個の電力信号で解析が可能となったと報告されている。

3　Type2: Multiple-Exponent, Single-Data(MESD)Attack

この攻撃の前提条件は、攻撃対象のスマートカードに任意の指数を指定して指数剰余計算が行えることである。攻撃者は、この指数の値を攻撃者は知っていても知らなくてもよい。このような状況は、起こりうる。なぜなら一般的にスマートカードは、指数を変更できるようになっている場合があるからである。このアルゴリズムは、図１に示されている。あるメッセージをプライベート鍵 e で指数剰余した電力信号を S_M としている。

M=任意の値、e_g=0
S_M[j]を集める
for (i=n-1 to 0)
{　(e_g の i 番目のビットが 1)であると予想した　S_1[j]をあつめよ
　(e_g の i 番目のビットが 0)であると予想した　S_0[j]をあつめよ
　　2 つの DPA バイアス信号を計算する
　　$D_1[j]= S_M[j]- S_1[j]$　および　$D_0[j]= S_M[j]- S_0[j]$
　どちらの予想がただしいか、DPA の結果から決めよ
　e_g を更新する}
e_g は、e（秘密の指数）と等しい

図１　MESD アルゴリズム

(i-1)番目まで全てわかっているとき、i 番目のビットを攻撃する場合を考える。(i-1)番目までが既知の値で、i 番目が 0 の指数と 1 の指数を作成し、あるデータに対してその電力信号 $S_0[j]$, $S_1[j]$を測定する。同様に同じデータで攻撃対象のカードの電力信号 $S_M[j]$も測定する。次に $S_M[j]$と電力信号 $S_0[j]$, $S_1[j]$との差分 $D_0[j]$, $D_1[j]$を計算する。この差分 $D_0[j]$, $D_1[j]$をグラフ化すると、正しい方の差分曲線のグラフは誤りのものと比較してゼロに近い値と

なる。これによりi番目のビットの値を決定する。同様の方法で、i+1番目以降も計算できる。この方法では1ビットあたり200回の冪乗剰余で鍵がわかる。

4　Type3: Zero-Exponent, Multiple-Data(ZEMD)Attack

攻撃者が多くのランダムなメッセージに対する秘密の指数を用いた指数剰余演算を行うことができる。ただし、指数に関する予備知識はないものとする。また、攻撃対象のスマートカードのアルゴリズムと法Nを知っているものとする。

具体的な攻撃方法は、図2に示す。この方法は、ランダムな平文を L 個用意し、それをプライベート鍵で処理した時の電力信号 Si[j]を測定する。一方で、同じアルゴリズムがシミュレート出来る環境を用意する。(i-1)番目まで全てわかっているとき、i番目のビットを攻撃する場合を考える。(i-1)番目までが既知の値で、i 番目が 1 の指数を作成し、i 番目の途中結果をシミュレートする。そのシミュレート結果のHamming重みが閾値highより大きいもの電力曲線を $S_{high}[j]$、閾値より小さいものの電力曲線を $S_{low}[j]$に分類する。そして、

$$D[j] = \overline{S}_{high}[j] - \overline{S}_{low}[j]$$

を計算する。実際にi番目が1の場合、差分d[j]のグラフにはピークが立ち、そうでない場合は、差分d[j]のグラフには大きなピークは現れない。それによりi番目の値を特定する。この方法では1ビットあたり100回の指数剰余で鍵がわかる。

```
eg =0
for (i= n-1 to 0)
    {(eg の i 番目のビットは 1)と予想する
     for (k=1 to L)
       {ランダム値 M を選択
          M^eg mod N の i 番目の処理をシミュレートする
        if(乗算結果が高いハミング重みを持つ)
          スマートカードを動かして、電力信号 S[j]をあつめる
           S[j]を S̄high[j] の集合に加える
        if(乗算結果が低いハミング重みを持つ)
          スマートカードを動かして、電力信号 S[j]をあつめる
           S[j]を S̄low[j] の集合に加える}
       電力信号の平均をとり、DPA バイアス信号を計算する
          D[j] = S̄high[j] − S̄low[j]
       if(DPA バイアス信号がスパイクをもつ)
          予想は、正しい：eg の i 番目のビットを 1 にセット
    else
        予想は、誤り：eg の i 番目のビットは、0 にセット}
  eg は、e（秘密の指数）に等しい
```

図2　ZEMD アルゴリズム

5　攻撃法のまとめ

攻撃方法をまとめると下表のとおり

攻撃名	攻撃に必要な指数計算数	攻撃の仮定
SEMD	20000	指数１つを知っている
MESD	200	べき指数を選択できる
ZEMD	200	処理アルゴリズムと剰余を知っている

- 可能な対策

タイミングアタックの多くの対策を用いることができる。４つの方法が示されている。乱数 v_i とし、$v_f=(v_i^{-1})^e \bmod N$ とする。ここで、N=pq、 $\phi(N)=(p-1)(q-1)$で、p,q は RSA 暗号で用いられる素数である。対策例として下記が挙げられている。

1. メッセージのブラインド化　$\underline{M} = (v_i M) \bmod N$
2. 指数のブラインド化　$\underline{e} = e + r\,\phi(N)$
3. 指数剰余演算　$\underline{C} = (\underline{M}^e) \bmod N$
4. 逆変換　$C = (v_f S) \bmod N$　　但し、$v_f = (v_i^{-1})^e \bmod N$

5.5.2. Further Results and Considerations on Side Channel Attacks on RSA(Klima and Rosa)

- 文献情報

発行年	2002 年
文献名	CHES 2002
タイトル	Further Results and Considerations Side Channel Attacks on RSA
著者	V.Klima, T.Rosa

- 攻撃対象

RSA 暗号を実装した（32 ビット）プロセッサ

- 攻撃の原理・前提

攻撃方法にあわせて記述

- 攻撃方法

1　RSA-OAEP へのサイドチャネル攻撃

ＲＳＡ-ＯＡＥＰの復号処理において、暗号文を復号し、OAEP の復号処理する。その中にMGF処理､すなわち復号文の一部をハッシュ関数SHA-1を用いて処理する部分がある。OAEP の仕様により SHA-1 入力は、つねにパディング処理されていることが分かる。パディングデータは、常に定数であるため、SHA-1 の処理を考えると固定値と復号文のメッセ

ージの下位３ワード（32 ビット）が XOR されることが分かる。サイドチャネル攻撃を用いてこの下位３ワードのハミング重みを得ることができる。

さらに、暗号文に公開鍵 e としたとき、暗号文 c に対して $c'=c*2^{-e} \bmod N$ の処理を行った暗号文を復号処理する。このとき、c'の復号データは、c の復号データに比べ mod N 上で 1 ビット右シフトした値となる。このとき、上記で得たハミング重みがシフトされた場合の変化を考えると、復号した平文の最下位ビットが高い確率で得られることが分かる。最下位ビットが得られれば、文献 11 で述べられた方法を用いて RSA の平文が得られる。

2　署名オラクルに対する復号処理オラクルを署名オラクルとして用いる攻撃

もし、攻撃者が PKCS#1 v1.5 あるいは v2.1 に対して Bleichbacher や Manger の攻撃を用いることができるのなら、同じ RSA のプライベート鍵を用いて偽の署名を作成できることが示されている。SSL では、サーバの公開鍵証明書で暗号化あるいは署名を行うことがあるので、これらの攻撃は実際的である。

Manger の攻撃では PKCS#1 v2.1 で RSA の最上位バイトが固定値になることを利用している。復号処理を行い想定される固定値なら正しい、そうでなければ否を知らせるオラクルを PIO_{MAB}（Partial information oracle）と呼び、復号するオラクルを$WIO(c)=c^d \bmod N$(Whole information oracle)と呼ぶ。

攻撃法は、先ず、偽署名を作成したいメッセージを c とする。n より小さい乱数 r=r1, r2, …を生成し、$c'=c*r^e \bmod N$ を計算し、PIO_{MAB}が正を返すまで繰り返す。最上位バイトが固定値になればいいので 1/256 の確率で成功する。成功した情報を WIO で復号する。つまり、m'=WIO(c')。このとき、$m=m'*r^{-1} \bmod N$ を計算すれば、ｃに対する正しい署名ｍが得られる。Bleichbacher の攻撃でも同様のことができる。

3　RSA-KEM への故障利用サイドチャネル攻撃

RSA-KEM は、メッセージ M を共通鍵暗号の鍵 r で暗号化した暗号文を C1、その鍵 r を公開鍵 e,n で暗号化 $y(=r^e \bmod n)$としたとき、暗号文 Ciphertext= y||C1 とするもの。ここで、RSA 暗号に限定した確認オラクル RSA-CO を定義する。これは、Ciphertext の復号を行う場合に、C０をプライベート鍵 d で復号し鍵 K と等しくなるか比較する。同じ場合は、常に、正しいと出力するものとする。

2 種類の故障利用攻撃を述べる。

・　プライベート鍵ｄのビットエラーを利用した攻撃

攻撃者が、復号鍵ｄの第 i ビットを d(i)を反転した鍵を d'を生成できるとする。また、受信者がこのことに気付かないとする。このときと $d'=d+2^i$ あるいは、$d'=d-2^i$ と表せる。ここで、$I=2^i \pmod n$、$\alpha=y^I \pmod n$、$\alpha \times \alpha^{-1}=1 \pmod n$、及び $r=y^{d'} \pmod n$ とするとｄ(i)=0 の場合 $r=(y^d \times \alpha \pmod n)$となり、ｄ(i)=1 の場合 $r=(y^d \times \alpha^{-1} \pmod n)$となる。

この性質を使って任意の x(０<x<n)を生成し、$y=x^e \pmod n$（e は公開鍵）を計算し、さらにｒ＝x* α(mod n)を計算して、誤りを発生した d'について RSA-CO の結果を見る。そして結果正しければ d(i)=0 とし、さもなくば d(i)=1 とする。このとき、RSA-CO では、ｙをd'で復号し、ｒと比較処理を行い、等しければ正しい答えを返し、等しくなければ誤りを返す。

これをいろいろな復号鍵の場所で繰り返せばすべての鍵が分かるというもの。

・ トロイの木馬攻撃の利用

RSA-KEMで公開鍵の一部である剰余数ｎの変更をしてもなんらアラームが出ない場合、プライベート鍵を取り出すことができることが示されている。すなわち、n を素数 $n'=t\times 2^s+1$（ｔは小さな素数）と置き換える。この場合、RSA 暗号の復号処理 $r=g^d \bmod n$ は、離散対数問題となり、n ’が上記のような形式の場合 Pohlig-Hellman のアルゴリズム（PH 法）で解けることが分かっている。実際は、復号結果は、オラクルより出力されないため。本オラクルを用いた PH 法によりプライベート鍵ｄを解くアルゴリズムを示している。詳細は、本文を参照。

・ その他の故障利用攻撃

本論文では、プライベート鍵ｄと剰余数ｎの変更による攻撃を述べたが、他の RSA パラメータによる攻撃も紹介されている。

4 ＲＳＡ法への攻撃の比較

	PKCS#1 v1.5	RESAES-OAEP	RSA-KEM
公開攻撃	可能	可能	可能
ｻｲﾄﾞﾁｬﾈﾙ攻撃	平文は PKCS#1 v1.5 に準拠しているか？	・平文の MSB がゼロか？ ・処理データのハミング重み	故障利用攻撃
攻撃により得られる情報	平文	平文	ﾌﾟﾗｲﾍﾞｰﾄ鍵

- 可能な対策

電力利用攻撃の対策が必要である。故障利用攻撃に対しては、適切なパディングを使用すること。暗号に使う鍵やパラメータの完全性のチェックを処理毎に行うこと。誤りを通知するメッセージの範囲を最小にすること。可能ならば故障利用攻撃の検出や訂正が可能なプラットフォームで演算すること。また、強力な対策としては、RSA 復号したものを再度暗号化し、暗号文に戻るかどうかチェックすること。これは、本論文の攻撃の有力な対策となっている。

- 他の文献との関係

本論文には、多くの関連論文が引用されている。それらを参照のこと。

5.5.3. Resistance Against Differential Power Analysis for Elliptic Curbe Cryptosystems (Coron)

- 文献情報

発行年	1999 年
文献名	CHES '99
タイトル	Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems
著者	J.-S. Coron

- 攻撃対象

スマートカードなどのデバイスに格納した楕円曲線暗号の秘密鍵

概要： SPA 対策を施した楕円曲線上のスカラー倍アルゴリズムに対して DPA 攻撃を適用する方法を提案している．スカラー値の先頭ビットから 1 ビットずつ DPA による解析を行うことで，スカラー値全体を導出することが可能である．

- 攻撃の原理・前提

前提：

・耐 SPA の double-add アルゴリズム（アルゴリズム 1'）を使用していること

・4P の特定のビット s_i が 0 が 1 かで消費電力が異なること

・アルゴリズム 1'の各ステップが常に同じタイミングで実行されること

スカラー倍演算 Q=dP を計算する耐 SPA アルゴリズムを以下に示す．ここで，d のバイナリ表現を$(d_{l-1},...,d_0)$と表記する．

アルゴリズム 1'

```
input P
Q[0] ← P
for i from l-2 to 0 do
    Q[0] ← 2Q[0]
    Q[1] ← Q[0]+P
    Q[0] ← Q[di]
output Q
```

原理：

アルゴリズム 1'に対して，d_{l-2} を解析する攻撃方法を示す．この攻撃方法では，電力消費と 4P の特定のビットとの関連を計算することによってビット d_{l-2} を復元する．$d_{l-2}=0$ ならば，アルゴリズム 1'中で 4P が計算されるため，電力消費と 4P の特定のビットを関連付けることができる．一方，$d_{l-2}=1$ ならば，アルゴリズム 1'中で 4P は計算されず，4P との関連は観測されない．このことから，4P が計算された場合には平均電力消費に統計的な特徴が出ることを利用して d_{l-2} を解析する．d の続くビットも同様の方法を再帰的に適用することで判別できる．

アルゴリズム 1 'を k 回実行する, すなわち個別の $P_1, P_2, \ldots, P_k$ から $Q_1=dP_1, Q_2=dP_2, \ldots, Q_k=dP_k$ を計算する．$C_i(t)$をアルゴリズムの第 i（$1<i<k$）回目の実行に関連付けた電力消費と定義する．s_i（$1<i<k$）を 4P のバイナリ表現中の特定のビットであると定義する．$C_i(t)$ と s_i の間の関係を示す関数 g(t)は次式のようになる．

$g(t)=< C_i(t) >_{i=1,2,...,k \mid s_i=1} - < C_i(t) >_{i=1,2,...,k \mid s_i=0}$

ポイント $4P_i$ が時刻 $t=t_1$ で計算されているときには，電力消費 $C_i(t_1)$は特定のビット s_i に関連付けることができる．したがって，$s_i=1$ の場合と $s_i=0$ の場合で電力消費の平均が異なる．このため，関数 g(t)は時刻 $t=t_1$ でピークを示す．逆に，ポイント $4P_i$ が時刻 $t=t_1$ で計算されていないときには，s_i と電力消費 $C_i(t_1)$には関連がない．したがって，$s_i=1$ の場合と $s_i=0$ の場合で電力消費の平均に有意な差がない．このため，時刻 $t=t_1$ で関数 g(t)にピークは観測されない．

- 攻撃方法

推定する．なお，ECDSA では固定の指数ではなくランダムな指数によってスカラー倍演算が行われるため，この攻撃方法は使えない．

0 節で示した攻撃をスカラー倍演算アルゴリズムに適用できるように拡張する．スカラー倍演算ではポイント P を次のような順序で計算する．

$a_0P = P \rightarrow a_1P \rightarrow a_2P \rightarrow \ldots \rightarrow a_rP = dP$

この攻撃は $a_0=1$ から始めて $a_r=d$ まで a_i を連続して推測することによって行う．ステップ i において，$0 \leqq k \leqq j < i$ なる $a_i'=\pm a_j \pm a_k$ のすべての組み合わせ A_i を考える．ここで，$a_i' \in A_i$ によって，ポイント $a_i'P$ と電力消費の間の関係を示す関数 g(t)を計算する．もし g(t)にピークが観測されれば, デバイスによってポイント $a_i'P$ が計算されたことを示しており，$a_i=a_i'$が成り立つ．このように実際に $O(r^2)$の時間で $d=a_r$ が復元できる．

- 可能な対策

DPA への対策を３つ提示する．これらの対策は，Q=dP を計算する際に乱数を導入する

のが基本的な考えである．

対策１：秘密指数のランダム化

εを曲線上のポイントの数とする．Q=dP の計算を以下のアルゴリズムで行う．この対策法では，d'をアルゴリズムの実行ごとに変化させる必要がある．

(1) サイズ n ビットの乱数を選ぶ．例えば，n=20 ビットの乱数を選択できる．
(2) d'=d+k.# εを計算する．
(3) ポイント Q=d'P を計算する．# εP=O から Q=dP が得られる．

対策２：P のブラインド化

この対策法は Chaum による RSA ブラインド署名に似ている．倍算するポイント P を秘密のランダムなポイント R と加算することで“ブラインド”にする．ポイント d(R+P)から S=dR を引くことによって Q=dP を得る．ポイント R と S はカード内にあらかじめ格納しておくことができる．例えば b をランダムなビットとして，計算ごとに R←(-1)^{b}2R，S←(-1)^{b}2S のように更新する．

対策３：射影座標のランダム化

$$(X,Y,Z)=(\lambda X,\ \lambda Y,\ \lambda Z) \qquad \text{(式 1)}$$

この対策法では，ポイント P=(X,Y,Z)の射影座標表現をランダム化する．Q=dP の新しい計算の前に P の射影座標をランダムな λを使った（式１）によってランダム化する．

- 他の文献との関係

[1] P. Kocher, J. Jaffe, B. Jun, "Introduction to Differential Power Analysis and Related Attacks", http://www.cryptography.com/dpa/technical/index.html, 1998

本論文の楕円曲線暗号に対する DPA は，この論文で提案した DPA を基にしている．実際にスマートカード上の DES に対して 1000 回の暗号処理を観察することにより，秘密鍵の導出に成功している．

[2] Okeya,K., Sakurai,K., Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack, Progress in Cryptology-INDOCRYPT 2000, LNCS1977, (2000), 178-190

本論文で示した DPA 対策の要件を含め, DPA を含むサイドチャネルアタックを防ぐ要件として以下の２つを提案している.

- 秘密情報と計算実行手順とが独立であること
- 計算対象の値がランダム化されていること

また，この２つの要件を基に本論文の３つの対策法に対して考察を行っている.

[3] 桶屋 勝幸，宮崎 邦彦，櫻井 幸一，サイドチャネル攻撃を防ぐモンゴメリ型楕円曲線上の高速なスカラー倍計算方法, To appear in Computer Security Symposium 2001 (CSS2001)

本論文で提示した対策法とは別の対策法として，モンゴメリ型楕円曲線におけるランダム化射影座標を用いたスカラー倍演算アルゴリズムを提案している.

[4] Joye,M., Quisquater,J.J., Hessian elliptic curves and side-channel attacks, Cryptographic Hardware and Embedded Systems (CHES’01), (2001), pp.412-420

本論文で提示した対策法とは別の対策法として，ヘジアン型の楕円曲線を用いて加算と２倍算の演算公式を同一にするスカラー倍計算方法を提案している.

[5] Liardet,P.Y., Smart,N.P., Preventing SPA/DPA in ECC systems using the Jacobi form, Cryptographic Hardware and Embedded Systems (CHES’01), (2001), pp.401-411

本論文で提示した対策法とは別の対策法として，ヤコビ型の楕円曲線を用いて加算と２倍算の演算公式を同一にするスカラー倍計算方法を提案している.

[6] （株）日立製作所，自己評価書 OK-ECDSA, http://www.ipa.go.jp/security/enc/CRYPTREC/fy14/cryptrec20021128_endedeval.html, 2001

本論文の対策法を含め, DPA を含むサイドチャネルアタックに対する既存の対策法に対する考察が含まれる.

5.5.4. Weierstra Elliptic Curves and Side-Channel Attacks (Brier and Joye)

- 文献情報

発行年	2002 年
文献名	PKC '2002
タイトル	Weierstrass Elliptic Curves and Side-Channel Attacks
著者	Eric Brier, Marc Joye

- 攻撃対象

暗号モジュールに格納した楕円曲線暗号の秘密鍵

概要：楕円曲線暗号の SPA 対策として，パラメータ変換やモンゴメリバイナリ法を用いる方法があるが，これらは適用できる楕円曲線が限られているという問題があった．本文献では，モンゴメリバイナリ法を一般的に用いられるワイエルシュトラウス形の楕円曲線に適用することで，すべての楕円曲線に SPA 対策を適用可能としている．

- 攻撃の原理・前提

楕円曲線暗号のサイドチャネルアタックに対する特性は以下のとおりである．

- SPA に弱い

加算と 2 倍算の処理が異なるので，これを解析すれば鍵がわかる．

- DPA に強い

毎回異なる乱数を用いるため．

- 攻撃方法

楕円曲線上の点のスカラー倍演算を double-and-add アルゴリズムで実行するときに，simple side-channel analysis を行う．電力や電磁波の解析により，暗号モジュールが 2 倍算の次に加算を連続して行っていることを検出した場合，スカラー値のそのとき処理中のビットは 1 である．

ただし，本論文は攻撃手法を提案するものではない．

- 可能な対策

(1) ダミーの演算を実行する．

例： double-and-add-always アルゴリズム

問題点：処理時間が増える

(2) 楕円曲線のパラメータ変換を用いる．

例：　　ヤコビ形式，ヘシアン形式

問題点：適用できる楕円曲線が限られている．

(3) 元々条件を満たしているアルゴリズムを用いる．

例：　　Montgomery's binary technique の適用

問題点：素数体でのアルゴリズムは，モンゴメリパラメータ表示（オーダ 2 の楕円曲線）に限定

上記対策(2),(3)を汎用化し通常の Weierstrass parametarization に適用可能とする．

以下に，楕円曲線状の点の k 倍算を行うモンゴメリ法を示す．x(P)は点 P の x 座標を示す．モンゴメリ法は P-Q がわかっている場合に，P+Q が x 座標のみから計算できることに基づいている．

```
Input:    P, k = (k_{l-1}, ⋯, k_0)_2
Output:   x(kP)
  1. R_0 = P; R_1 = 2P
  2. for i = l-2 downto 0 do
  3.       if ( k_i = 0 ) then
  4.                x(R_1) ← x(R_0+R_1); x(R_0) ← x(2R_0)
  5.       else [ if ( k_i = 1 ) ]
  6.                x(R_0) ← x(R_0+R_1); x(R_1) ← x(2R_1)
  return ( x(R_0) )
```

モンゴメリの研究は，$by^2=x^3+ax^2+x$ の楕円曲線への適用に限定しているが，本文献では x(P+Q)と x(2P)の演算に以下の式を用いることで, 一般的な楕円曲線に適用可能としている．

楕円曲線が $y^2=x^3+ax+b$ で与えられ，P－Q=(x, y)であることがわかっているとき，

$$x(P+Q)=\frac{-4b(x_1+x_2)+(x_1x_2-a)^2}{x(x_1-x_2)^2}$$

$$x(2P)=\frac{(x_1{}^2-a)^2-8bx_1}{4(x_1{}^3+ax_1+b)}$$

楕円曲線が $y^2=x^3+ax+b$ で与えられ，$P=(x_1, y_1)$，$Q=(x_2, y_2)$，P－Q=(x, y)のとき，

$$y(P)=y_1=\frac{2b+(a+xx_1)(x+x_1)-x_2(x-x_1)^2}{2y}$$

また，$x_i=X_i/Z_i$, $y_i=Y_i/Z_i$ となる射影空間(X, Y, Z)上では，上式は以下のようになる．

$$X(P+Q)=-4bZ_1Z_2(X_1Z_2(X_1Z_2+X_2Z_1)+(X_1X_2-aZ_1Z_2)^2$$

$$Z(P+Q) = x \cdot (X_1Z_2 - X_2Z_1)^2$$
$$X(2P) = (X_1^2 - aZ_1^2)2 - 8bX_1Z_1^3$$
$$Z(2P) = 4Z_1(X_1^3 + aX_1Z_1^2 + bZ_1^3)$$

文献に記載の証明は省略した.

- 他の文献との関係

(1) 攻撃法の提案

[1] E.Oswald: Enhancing Simple Power-Analysis Attacks on Elliptic Curve Cryptosystems, CHES2002

SPA を強化した解析手法を提案. 一時的な鍵を用いることで SPA 対策を施した楕円暗号処理を解析可能.

[2] K.Itoh, T.Izu: Address-bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA, CHES2002

レジスタのアドレスを利用する DPA の変形方式. データへの DPA 対策を施した実装に対しても攻撃可能.

(2) 対策の提案

[3] J.S. Coron: Resistance against differential power analysis for clliptic curve cryptosystems, CHES'99, pp.292-302, Springer-Verlag, 1999

ダミーの演算を導入して SPA を防ぐ, double-and-add-always 方式の提案.

[4] P.Y. Liardet and N.P. Smart: Preventing SPA/DPA in ECC systems using the Hacobi form, CHES2001, pp401-411, Springer-Verlag, 2001

楕円曲線をヤコビ形式に変換して演算することでサイドチャネルアタックを防ぐ.

[5] M. Joye and J.J. Quisquater, Hessian elliptic curves and side-channel attacks, CHES2001, Springer-Verlag, 2001

楕円曲線をヘシアン形式に変換して演算することでサイドチャネルアタックを防ぐ.

[6] J. Lopez and R. Dahab: Fast multiplication on elliptic curves over GF(2^m) without precomuputation, CHES'99, pp.316-327, Springer-Verlag, 1999

モンゴメリ演算を用いて楕円曲線暗号へのサイドチャネルアタックを防ぐ.

[7] K. Okeya and K. Sakurai: Power Analysis breaks elliptic curve cryptosystems even secure against the timing attack, INDOCRYPT2000, pp.178-190, Springer-Verlag, 2000

モンゴメリ演算を用いて楕円曲線暗号へのサイドチャネルアタックを防ぐ方式.

[8] E.Trichina, A.Bellezza: Implementation of Elliptic Curve Cryptography with Built-in Counter Measures ageinst Side Channel Attacks, CHES2002

事前計算テーブルを利用した，非決定的な楕円曲線上の点の累乗を行うことで，サイドチャネルアタックを回避.

[9] M.Ciet, J.J.Quisquater, F.Sica: Preventing Differential Analysis in GLV Elliptic Curve Scalar Multiplication, CHES2002

k をランダム化して，スカラー倍演算を DA から保護，かつ GLV 楕円曲線演算方式の高速演算のメリットを享受.

[10] J.C.Ha, S.J.Moon: Randomized Signed-Scalar Multiplication of ECC to resist Power Attacks, CHES2002

スカラー倍演算をランダム化して SPA を防止．通常のバイナリ法と比べて演算量が増えない.

(3) その他

[11] C.Gebotys, R.Gebotys: Secure Elliptic Curve Implementations: An Analysis of Resistance to Power-Attacks in a DSP Processor, CHES2002

実際の暗号チップを解析して，セキュリティ対策の実装とコードサイズ，実装速度のトレードオフを評価.

5.6. **アタックの拡張**

5.6.1. Using Second-Order Power Analysis to Attack DPA Resistant Software (Messerges)

- 文献情報

発行年	2000 年
文献名	CHESS 2000
タイトル	Using Second-Order Power Analysis to Attack DPA Resistant Software
著者	T. S. Messerges

- 攻撃対象

ソフトウェアで暗号処理を行っているスマートカード

- 攻撃の原理・前提

・n 次 DPA の定義：

n 次 DPA 攻撃は、あるアルゴリズムの実行中に計算されるｎ個の異なった中間値に対応する、電力消費曲線中の n 個の異なったサンプル値を利用する。

・健全の定義：

あるアルゴリズムの秘密鍵に対する DPA 攻撃が健全(sound)であるとは、ある攻撃者が秘密鍵の全てビット値を学ぶために電力消費情報を使うことが理論的に可能であること。

一般的に健全な攻撃は実用的であることも、そうでないときもある。本論文では、１次の DPA 攻撃と２次の DPA 攻撃、それぞれの攻撃が健全であることを確認し、実験で実用性を確認している。

・電力漏洩モデル（Power Leakage Model)の仮定：

本論部では、プロセッサは、処理しているデータのハミング重みに関する情報がもれる。ハミング重みの小さいデータより、大きいデータの方がより多くの電力を消費し、その関係は、ハミング重みに関して線形である。

・ある時刻 j における電力消費 P[j]

P[j］は、下記のように書かれる

P[j］= ε・ d[j] + L + n

ここで、d[j]：時刻 j における中間データ結果：

ε：ハミング重みが１増加したときの電力の増加分

L：電力の定数部分：L

n：ノイズ

ｎは、平均０と仮定されている。

・攻撃対象の処理ルーチン例

下記に示すように W1 と W2 の２つの例が示されている。W2 は、１次 DPA 対策が施さ

れている。

```
W1 {PTI}
{
    A:Result=PTI  (XOR)  SecretKey
    ・・・
    other operations
    ・・・
    return CTO
}
```

```
W2(PTI)
{
    B:RandomMask = rand()
      mPTI = PTI (XOR) RandomMask
    C:Result = mPTI (XOR) SecretKey
    ・・・
   other operations ・・・
   return CTO
}
```

- 攻撃方法

1　1 次のスマートカード DPA 攻撃例

命題１：　W1 アルゴリズムが N ビットのプロセッサで用いられていて、電力消費とハミング重みに線形関係のある場合は、下記の 1 次の DPA 攻撃は健全である

1.Repeat　for i equal 0 through N-1 {
2. Repeat for b = 0 to 1 {
3. 平均電力信号　Ab[j]の計算を下記を繰り返すことで行う{
4. PTI 入力の i 番目のビットを b にセットする
5. PTI 入力の残りのビットをランダムな値にセットする
6. アルゴリズムの電力信号を集める}}
7. DPA バイアス信号 T[j]=A0[j]－A1[j]を計算
8. T[j]は、i 番目の秘密鍵ビットが１ならば正のスパイクが現れ、i 番目の秘密鍵ビットが 0 ならば負のスパイクが表れる。

上記攻撃が可能なことが、上記仮定のもとで示されている。

2　2 次の DPA の攻撃例

命題２：　W2 アルゴリズムが N ビットのプロセッサで用いられていて、電力消費とハミング重みに線形関係のある場合は、下記の 2 次の DPA 攻撃は健全である

1.Repeat　for i equal 0 through N-1 {
2. Repeat for b = 0 to 1 {
3. 平均統計値　Sb　=｜Pb　－　Pc |の計算を下記を繰り返すことで行う{
4. PTI 入力の i 番目のビットを b にセットする
5. PTI 入力の残りのビットをランダムな値にセットする
6. アルゴリズムの B 行と C 行の瞬間電力消費量を集める、

これらをそれぞれ Pb，及び Pc と呼ぶ。}}

7. DPA バイアス信号 T=S0－S1 を計算
8. もし、T＞０ならば、i 番目の秘密鍵ビットは１、そうでなければ 0 である。

W2 アルゴリズムは、1 次の DPA 攻撃を避けるために乱数加算によるホワイトニングを行っているが、本攻撃により攻撃可能なことが示されている。

3 実験結果

対象スマートカード ST16 である。このカードは、EPROM が搭載されており、外部よりプログラムが書き込める。一次の DPA 攻撃のためには、実装の設計情報は不要だが、2 次の DPA 攻撃には、どの時点で B 行と C 行の処理が行われるかという情報が必要となる。

スマートカードの入力周波数 3.57MHz、サンプリング周波数:1GHz で攻撃実験を行った。

1 次の DPA 攻撃は、50 個の電力信号があれば正しい鍵が求まる。2 次のものは、たいていのビットは 50 個以下で求まるが 2500 以上必要なビットがあった。

これらの結果は、実装方法、実装するスマートカードにより異なってくる。

4 最適な攻撃

さらに本論分では、2 次の DPA 攻撃が古典的な決定問題の完全な例になっていることを示している。つまり、ノイズの多い電力消費データから攻撃者は、鍵ビットがゼロか１かを決定する問題である。最適な決定は、誤り確率が最小であればよい。下記の定理が証明されている

定理：N 個のベクトル（b_k、c_k）を用いた最適な 2 次 DPA 攻撃は、下記の決定問題に帰着できる。ここで、各ベクトルは独立で、かつ b_k と c_k は、結合正規ランダム変数と仮定されている。

$$\prod_{k=0}^{N-1}\cosh(b_k+c_k) \quad \begin{matrix}\leq \\ > \end{matrix} \quad \prod_{k=0}^{N-1}\cosh(b_k-c_k)$$

ここで、｜b_k-c_k｜>>1 のとき、命題２の攻撃は、最適な決定問題をよく近似している。つまり、｜b_k-c_k｜>>1 のとき、

$$\prod_{k=0}^{N-1}\cosh(b_k+c_k) \quad \propto \quad \sum_{k=0}^{N-1}|b_k-c_k|$$

からわかる。実際、実験結果からも確認できた。

- 可能な対策

長期的には、秘密情報の漏れないハードウェアを開発すること。短期的には、様々な一次の DPA 対策は、高次の DPA 対策の助けになる。たとえば、攻撃者が予想し対策できな

いランダムな時間遅延を加える等である。実装の詳細を秘密にすることは高次 DPA に対して非常に効果的である。Chari et al が提案している秘密分割方式も有効な方法の１つである。

- 他の文献との関係

長期的には情報のもれないハードウェアは、文献 13,14 に紹介されている、文献 15 での統計テストは、そのようなハードを評価するのに用いられる。

5.6.2. The EM side-channel(s)(Agrawal, Archambeault, Rao and Rohatgi)

- 文献情報

発行年	2002 年
文献名	CHES '2002
タイトル	The EM Side-Channel(s)
著者	Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi

- 攻撃対象

CMOS を用いた電子回路全般（IC カード，暗号モジュール）

暗号モジュールから出力される電磁波を測定する電磁波解析攻撃において，電磁波の故意でない放射(unintentional emanations) の解析を提案している．また，電磁波解析と電力解析を比較し，いくつかの点で電磁波解析の方が優れていることを示している．

- 攻撃の原理・前提

CMOS デバイスは内部のロジック状態が変化したときのみ"方形波"が流れる．これにより発生する電磁波を測定する．

電力による解析が一般的だが，回路の適当な部分をプローブで測定する必要があるため，現実には実践は困難．電磁波は様々な場所で測定できるので，IC カードの裏側など様々な場所で測定できる．

電磁波の放射には大きく分けて以下の 2 種類がある．

(1) 直接放射（Direct Emanations）

故意的な(intentional)電流の流れの結果として放射され，広い周波数帯で観測可能である．測定対象近くの狭いエリアの電磁波だけを計測する．複雑な回路の計測をする場合には，小型のフィールドプローブ(tiny field probe)を信号減の間近に設置することで，干渉を最小限に抑える必要がある．これは，良い結果を得るためにはチップのパッケージをはがす必要があることを意味する．また，慎重にフィールドプローブを設置しても，ごく近い場所

のソースからの干渉を消すことは不可能である．

(2) 故意でない放射（Unintentional Emanations）

CMOS デバイスの小型化と複雑化により，ごく近い場所を流れる電気信号や電磁波の結合(coupling)が起こる．このとき放射は搬送波の変調という形で現れる．強力な搬送波の一つはどこでも測定されるクロックシグナルである．搬送波の変調は，振幅変調，角度変調などからなる．これらを復調することで，目的のデータ信号を得ることが可能である．

また，変調された搬送波が，直接放出よりもうまく伝播する場合がある．これによりデバイスへの進入が不要になり，離れた場所からですら攻撃が可能となる．

- 攻撃方法

電磁波は多くの場合，輻射(radiation)と伝導(conduction)の組み合わせにより伝播する．そのため，2 種類のセンサが必要となる．

輻射(radiation)を取得するには, ニアフィールドプローブ(near field probe)を可能な限りデバイスの近くに設置する方法が最適であるが，通常のアンテナで少し離れた場所で測定可能な放射(emanation)もある．本文献の実験では，最も効果的なニアフィールドプローブは銀や銅など伝導率の高い金属板に同軸ケーブルをつけたものとしている．離れた場所からは，双円錐形の対数周期ワイドバンドアンテナと手作りのナローバンドで高利得な八木アンテナを使用している．さらにフィルタを用いて，必要な信号を抜き取る．

伝導による放射(conductive emanation)はすべての導電部にかすかな電流として現れる．この放射(emanation)を取得するには電流プローブ(current probe)が必要である．さらにレシーバと復調器が必要である．取得した信号を解析するためには，デジタルスコープやサンプリングカードを利用する．スペクトラムアナライザは搬送波と情報を含む可能性がある信号を区別するために有用である．

取得した電磁波の信号に対して, 電力解析の場合と同じように, 単純解析 SEMA (Simple Electromagnetic Attack) や，差分解析 DEMA (Differential Electromagnetic Attack)適用することで，デバイスの動作を解析する．

- 可能な対策

signal strength reduction

(1) 想定外の放射を減らすように回路を再設計する．

(2) シールドや物理的に守られたエリアを用いる．

signal information reduction

(1) ランダム化

(2) 頻繁な鍵更新

- 他の文献との関係

[1] Karine Gandolfi, Christophe Mourtel, and Francis Olivier: Electromagnetic Analysis: Concrete Results, CHES2001

ハードウェアによる保護を施したCMOSチップに対して, 実際に電磁波解析を行い, DES, alleged COMP128, RSA の鍵を導出している.

電力解析と比較し，電磁波解析のほうが効果的な解析が可能としている.

5.6.3. Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies (Shamir)

- 文献情報

発行年	2000 年
文献名	CHES 2002, LNCS 1965, pp.71-77
タイトル	Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies
著者	Adi Shamir

- 攻撃対象

スマートカード

- 攻撃の原理・前提

チップが取り出され、変更されチップ表面に直接アクセスし、回路を観察、変更、干渉する、活性攻撃に対して、タイミング・グリッジ信号・電力分析などの侵入攻撃が存在する。電力分析は実装が容易であり、避けることが困難である。これは、詳細な電力消費カーブを観察することに基づく。

- 攻撃方法

単純電力分析は（SPA: Simple Power Analysis）は、消費電力の観察によって、クロックサイクルにおける命令の識別とメモリへの R/W するデータワードのハミングウェイトに関する統計的情報を獲得する。

差分電力分析（DPA：Differential Power Analysis）は複数の異なる入力による複数の実行で記録された電力消費を対象とする。

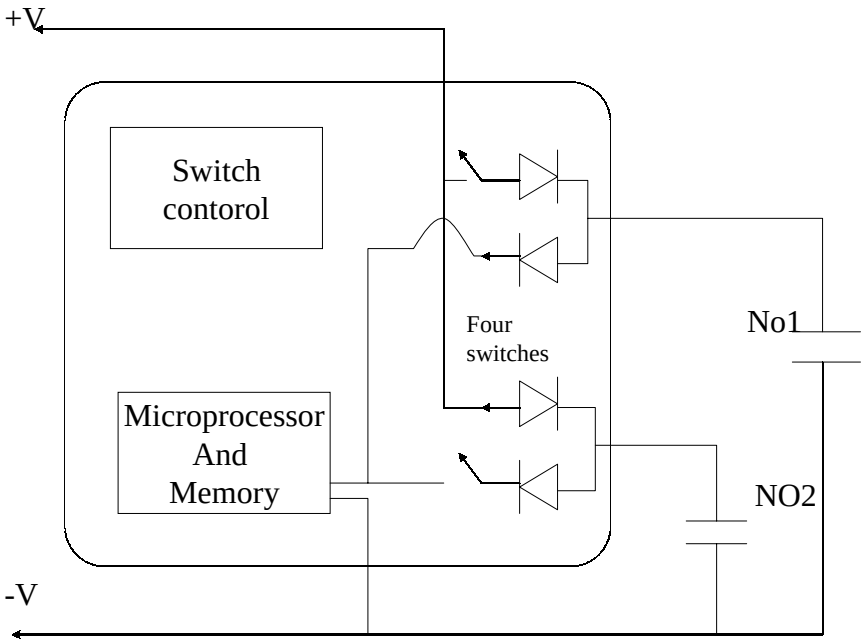
- 可能な対策

電力消費を一定にするための方策がとられた。物理的な設計が変更されたり、電力入力にコンデサを追加したが充分な平準化を得られなかった。また、ソフトウェア乱数を含む HW

乱数信号なども提案されたが、限定的な対策でしかない。また、内部バッテリや充電バッテリを使用する案もあるが、スマートカードの物理的な制約のため困難である。

ここでは２つのコンデンサと４つのスイッチによる方法を提案する。（図）

1. No1 コンデンサを外部電力から切断
2. No.1 コンデンサをチップに接続
3. No.2 コンデンサをチップから切断
4. NO2 コンデンサを外部パワーに接続



この方法では、チップは常にひとつのコンデンサによって電力供給されているが、外部電力は内部のチップに直接接続しない。供給された電流は統一され予測可能である。電力分析攻撃から逃れるため、チップから切断し（３）、外部パワーに接続（4）する前に外部より観察不可能な方法でコンデンサを放電する要素を追加する。

- 他の文献との関係

電力分析攻撃について、Kocher らの論文を元にしている。

P.Kocher J.Jaffe, and B.Jun, Introduction to Different Power Analysis and Related Attacks

参考文献

[1] 松本 勉, “耐タンパー技術： 物理と論理のはざま,” 電子情報通信学会基礎・境界ソサイエティ大会予稿集, pp.296-297, 1997.

[2] 竹田 忠雄, “IC カードの第四の性能指標：耐タンパー,” 電子情報通信学会基礎・境界ソサイエティ大会予稿集, pp.298-299, 1997.

[3] 村松 晃, “電子マネーの安全性と耐タンパー技術,” 電子情報通信学会基礎・境界ソサイエティ大会予稿集, pp.300-301, 1997.

[4] 村山 隆徳, “ソフトウェアの耐タンパー化技術,” 電子情報通信学会基礎・境界ソサイエティ大会予稿集, pp.302-303, 1997.

[5] D. Aucsmith, “Tamper Resistant Software: An Implementation,” Proc. of the First International Information hiding Workshop (IHW'96), Vol. 1174, pp. 317-333, 1997.

[6] S. Burnett and S. Paine, “暗号化, ”RSA セキュリティオフィシャルガイド, 翔泳社, 2002

[7] 矢野経済研究所, “2002 年版 IC カード市場白書～無線免許制撤廃で急速に市場は拡大する～,” 矢野経済研究所, 2002.

[8] 総務省情報通信政策局情報流通振興課, “電子認証ビジネス市場規模調査の結果,” <http://www.soumu.go.jp/s-news/2002/020412_2.htm>

付録１：海外における暗号モジュール評価実態調査

IPA「CC の MR 加盟国における暗号モジュール評価の実態調査」より

別ファイル

No	大項目	中項目	アメリカ/カナダ	イギリス
1	組織概要	a.政府機関の名称	・アメリカ：NIST(National Institute of Standards and Technology) ・カナダ：CSE(The Communications Security Establishment)	CESG (Communications-Electoronics Security Group)
		b.組織上の位置付け	・NIST：米国商務省傘下 ・CSE：カナダ国防省傘下	・政府による暗号の正式使用のための政府支援国家技術局。 ・情報ｾｷｭﾘﾃｨ（INFOSEC)のための技術局。
		c.機関の主な役割	CMVPの運用により、以下を目指す。 ・米国/ｶﾅﾀﾞの利用者に対し、信頼できる製品を供給する。 ・暗号ﾓｼﾞｭｰﾙ製品ﾍﾞﾝﾀﾞは共通の標準/認定ﾌﾟﾛｾｽを獲得し、大きな市場を創造する。 ・それぞれの連邦政府機関に認定製品の利用を勧めることにより連邦政府の情報ｾｷｭﾘﾃｨを確立する。	・政府が使用する暗号製品の開発/認定 -CESGの運用ﾌﾟﾛｸﾞﾗﾑにCESG支援ｽｷｰﾑ(CAPS：企業の会員制組織）があり、CAPSﾒﾝﾊﾞｰは、CESGが開発した暗号ｱﾙｺﾞﾘｽﾞﾑの自社製品への組込みおよびCESGへの評価依頼が可能となる。 -評価の結果、認定されると英国政府調達製品として公表される。
		d.規模	不明	情報入手ができなかったため、不明。
2	政府標準暗号の有無および選定/評価基準	a.政府標準暗号の有無	あり	あり
		b.a.にて「あり」の場合、その概要	(米国、カナダ共通) FIPS 46-3(DES, TripleDES) FIPS 186-2(DSS) FIPS 180-1(SHS) FIPS 185(Skipjack) FIPS 197(AES) (上記に加え、カナダのみ) CAST-128	リスト非公開のため、不明。 ・以下はCESGで開発・標準化された暗号例。 -実用的なID-PKC(Identifier-based public key cryptography)を提案（Cliff Cocks, 1998年)。 -次世代の音声/ﾃﾞｰﾀ暗号化(NGVDC)を取組中。
		c.a.にて「あり」の場合、標準化の選定/評価基準	FIPS 46-1,197は、要求仕様を公開し，公募。応募を評価し，選定。最終的選定基準は明らかではない。FIPS 46-2からFIPS 46-2/-3への変更はNISTが実施。 FIPS 186-1/-2、180-1は、NISTが作成。FIPS 185は、NSA（国家安全保障局)が作成。	CAPSでは、製品用途に応じて以下の3段階の保証ﾚﾍﾞﾙがある。 ・ﾍﾞｰｽﾗｲﾝ -用途：ｲﾝﾀｰﾈｯﾄ上でどの地域からでもある限定された情報を送ることを目的。 -搭載暗号条件：CESG設計暗号/ﾊﾟﾌﾞﾘｯｸな暗号 ・ｴﾝﾊﾝｽﾄﾞ -用途：confidential/secret対象の情報保護を目的。 -搭載暗号条件：CESG設計暗号 ・ﾊｲｸﾞﾚｰﾄﾞ -用途：secret/secret以上対象の情報保護を目的。CAPSの認証範囲外。
		d.a.にて「なし」の場合、標準暗号の今後の計画の有無	---	調査会社を通じた調査時点では，「国家情報戦略に関連するので回答しない。」との拒否にあった． しかし、2002年3月のCMVP2002（米NIST主催)では、”sensitive”であるが、”unclassified”である情報（いわゆる、一般秘に相当する情報）を扱う暗号モジュールの評価に対して、FIPS 140-2の評価を行うとの意思表明がなされた。
		e.現在選考中のISO/IEC JTC1 SC27 WD18033の扱い	---	情報入手ができなかったため、不明。
3	暗号モジュールの実装評価基準・制度の現況	a.実施評価基準の内容	FIPS 140-1/-2　に準拠。	実装基準は、ITSECおよびCCに準拠。
		b.実装評価の実施体制	NIST/CSEはNVLAPに基づき民間の研究機関を評価機関として認定し、それらの機関がﾍﾞﾝﾀﾞの製品等の評価を行う。 ＜認定評価機関：6機関＞ -Atlan Laboratories -CEAL：a CygnaCom Solutions Laboratory -COACT Inc. CAFE Laboratory -DOMUS IT Security Laboratory -EWA-Canada LTD, IT Security Evaluation Facility -InfoGard Laboratories, Inc	CESGおよび以下の民間評価機関(CLEF)にて実施。 ＜民間評価機関：5機関＞ -CMG -EDS Ltd. -IBM Global Service -Logica UK Ltd. -Syntegra
		c.実施評価の実施手順	・CMVPにおける認定ﾌﾛｰに従う。 1)ﾍﾞﾝﾀﾞによる製品の申請（認定機関はﾍﾞﾝﾀﾞが選択) 2a)NIST/CSEによるｶﾞｲﾀﾞﾝｽの提示 2)評価機関によるﾃｽﾄの実施 3)評価機関によるﾚﾎﾟｰﾄの作成 4)NISTとCSEへのﾚﾎﾟｰﾄの送付 5)ﾍﾞﾝﾀﾞへの認定証の交付 6)認定ﾓｼﾞｭｰﾙﾘｽﾄへの追加	・一般市場向け暗号の実装評価の場合、正規のITSECまたはCCの評価基準に従う。 ・開発者は以下の規定に従い、作業を行う。 UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME -UK Scheme Publication No.4 Developer's Guide Part Ⅰ / Ⅱ /Ⅲ
		d.実施評価の実績・具体例	・2001年1月23日現在、200の製品が認定を受けている。 ＜ｾｷｭﾘﾃｨﾚﾍﾞﾙによる内訳＞ -ﾚﾍﾞﾙ1：54製品（ﾊｰﾄﾞ23，ﾌｧｰﾑ1，ｿﾌﾄ30) -ﾚﾍﾞﾙ2：91製品（ﾊｰﾄﾞ83，ﾌｧｰﾑ0，ｿﾌﾄ8) -ﾚﾍﾞﾙ3：48製品（ﾊｰﾄﾞ46，ﾌｧｰﾑ2，ｿﾌﾄ0) -ﾚﾍﾞﾙ4：7製品（ﾊｰﾄﾞ7，ﾌｧｰﾑ0，ｿﾌﾄ0)	専門企業と共同し、以下の製品を提供。 -ED20M(Baltimore Technologies) -CS Authenticate(Crypto Solutions) -Flagstone(TM) (Stonewood Electronics Limited)
4	政府調達一般暗号製品の評価実態	a.各国の標準暗号プロトコル	不明	製品ﾚﾍﾞﾙで評価を実施しているため、暗号ﾌﾟﾛﾄｺﾙを使用するかどうかは製品に依存する。
		b.製品評価基準	FIPS 140-1/-2に準拠	・CC for Information Technology Security Evaluation (ISO/IEC Standard 15408) ・既存のﾖｰﾛｯﾊﾟITSECとUS TCSEC、ｶﾅﾀﾞCTCPE Cの提携・開発の国際的活動 ・標準SFRのCCｶﾀﾛｸﾞがPPの開発に使用され、かつST開発の方法として使用される。 ・EAL4以下のCC認証がｶﾅﾀﾞ、ﾃﾞﾝﾏｰｸ、ﾌﾗﾝｽ、ｲｷﾞﾘｽ、ｱﾒﾘｶにより相互認証されている。
		c.製品評価の実施体制	政府調達製品には、CMVPによる認定を義務付け。	・UKAS(UK Accrediation Service) DTIからのﾗｲｾﾝｽを受けた認証機関・検査/検定研究所 ・UK CB(Certification Body) CESG内で独立した組織で、1990年からDTIによるｻﾎﾟｰﾄを受け、UKASからの認定を受けている。 ・CLEF(Commercial Evaluation Facility) CBから認定されたｾｷｭﾘﾃｨ評価機関で、UKASから定期的な査察を受けている。
		d.製品評価の実施手順	DTR(Derived Test Requirement)に従い、FIPS140-1/-2に適合しているかどうかの評価を行う。	・政府向けの暗号製品は、CAPSｽｷｰﾑで評価。 ・正規のITSECまたはCCの評価基準に従う。 ・開発者は以下の規定に従い、作業を行う。 UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME -UK Scheme Publication No.4 Developer's Guide Part Ⅰ / Ⅱ /Ⅲ
		e.製品評価の実績・具体例	3.d.に同じ。	・CESGが政府に提供している一般暗号製品：BRENT ・CESGと専門企業が共同で政府に提供している製品 -ﾃﾞｰﾀ暗号化関連：10製品 -通信ｾｷｭﾘﾃｨ：11製品 -ｱｸｾｽｺﾝﾄﾛｰﾙ：5製品 -その他：3製品 -ﾊﾟｽﾜｰﾄﾞを使うﾊﾟｯｹｰｼﾞ：20製品

フランス	ドイツ	オーストラリア
DCSSI (Direction Centrale de la Securite des Systemes d'Information)	BSI (Bundesamt fur Sicheit in der Informationstechnic)	DSD (Defense Signals Directorates)
・2001年7月31日ﾌﾗﾝｽ政府令によって設立。 ・国防総務事務局（SGDN)の権限下。	・1991年に設立。ITと暗号分野の政府機関。 ・連邦内務省の管轄下にある連邦上級庁。	・ｺﾝﾋﾟｭｰﾀ/情報ｾｷｭﾘﾃｨに対する警告を発動する国家機関。 ・ｵｰｽﾄﾗﾘｱ国防総省内にある。
・情報ｾｷｭﾘﾃｨ政策の開発と実装における政府機関への支援。 ・以下の3部門で構成されている。 -規制部門：DCSSIの規制作成・実行、および認証ｻｰﾋﾞｽ -運営部門：通信/情報のｾｷｭﾘﾃｨにおける政府の活動支援 -科学技術部門：情報技術/通信ｾｷｭﾘﾃｨ/暗号分野での技術支援	・政府のITｼｽﾃﾑ維持支援（CERTﾌﾟﾛｸﾞﾗﾑ等の支援）。 ・電子署名/ｾｷｭﾘﾃｨ製品の分野における商用暗号ﾌﾟﾛｼﾞｪｸﾄの評価・認証の提供。	・海外の秘密情報(Sigintなど）の収集と普及。 ・政府およびその防御力に対し、情報ｾｷｭﾘﾃｨ製品/ｻｰﾋﾞｽを供給。 ・AISEP（ｵｰｽﾄﾗﾘｱ情報ｾｷｭﾘﾃｨ評価制度）の運営管理。
情報入手ができなかったため、不明。	職員数：約350名	職員数：約60名（うちAISEP担当者は6名）
なし	あり	あり (ただし、各省庁が使用し、国家安全保障には関わらないﾚﾍﾞﾙのもの)
---	・RSA - RSA：PKCS#1 v1.5 - 乱数を使ったISO/IEC9796-2に準拠したDSI ・DSA ・楕円曲線暗号を利用したDSA - EC-DSA - EC-KDSA, EC-GDSA - ﾅｲﾊﾞｰｸﾆ=ﾘｭｯﾍﾟﾙ署名	標準暗号は、ACSI33に定義されている。 -ﾃﾞｼﾞﾀﾙ署名標準 推奨：少なくとも1024ﾋﾞｯﾄのDSA + SHA-1 受容：少なくとも1024ﾋﾞｯﾄのRSA + MD5 -暗号化ｱﾙｺﾞﾘｽﾞﾑ標準 少なくとも56ﾋﾞｯﾄ鍵長のDEA -ｾｯｼｮﾝ鍵標準 推奨：1024ﾋﾞｯﾄ以上のRSAまたはDHﾌﾟﾛﾄｺﾙ -ｷｰﾘｶﾊﾞﾘ ・DSDの評価済み製品ﾘｽﾄ、EPLにﾘｽﾄされた暗号製品は、実用的である限り、鍵/ﾃﾞｰﾀのﾘｶﾊﾞﾘ方法を提供しなければならない。 ・評価時には、ｷｰﾘｶﾊﾞﾘ機能に関する技術情報をDSDに提出要。
---	・CC/ITSECﾌﾚｰﾑﾜｰｸのみに準拠。 （FIPS-140には準拠していない） ・BSIおよび民間ﾗﾎﾞ(T-Systems ISS, TUViTなど）で評価実施。 ・電子署名の利用には、 BSI認証+GPTM(ﾄﾞｲﾂ連邦郵便電気通信省）認可が必要。	・市場でもっとも広く受入れられており、安全性に問題がないことが実証されている暗号を選定し、それを評価して政府の標準暗号として採用。（ｺｽﾄ効率/市場で使用されないﾘｽｸ低減のﾒﾘｯﾄあり） ・多大な時間/労力/資源がかかるため、DSD独自で標準暗号選定のための評価は実施しない。
明確な計画なし。 ~~（FIPS-140を採択する見込み？）~~ 但し，FIPS 140-1/-2には、興味を持っており，検討中。	---	標準暗号はあるが、今後も市場で受入れられている暗号を選定して標準暗号ﾘｽﾄに加えていく予定。
情報入手ができなかったため、不明。	情報入手できなかったため、不明。	ｲﾝﾀﾋﾞｭｰ対象者から特に意識した話がなかったことから、対応していないと思われる。
・CMVP/CAPSのような民間評価機関による評価ｼｽﾃﾑなし。 ・政府が政府/民間で使用される暗号化ﾓｼﾞｭｰﾙの認証を提供。	・電子署名に関する規定(2001/5/21付けで出された） - 電子署名とその改変方法に関する一般条件 (Uber Rahmenbedingungen fur Rahmenbedingungen fur electronische Signaturen und zur Anderung weiterer Vorschriften) ・ｽﾏｰﾄｶｰﾄﾞに関する規定 - 電子署名の機能/ｱﾌﾟﾘｹｰｼｮﾝを備えたｽﾏｰﾄｶｰﾄﾞのｲﾝﾀｰﾌｪｰｽ仕様(DIN NI-17.4およびV66291-1/4,DIN SIG-V)	未公開のため、不明。 （ＡＩＳＥＦの評価機関にも未公開。）
・米国のCMVPに相当するﾌﾟﾛｸﾞﾗﾑなし。 ・政府は、民間評価機関の認可要件の修正を検討中。 ・評価機関許可が想定される民間評価組織（7つ） -現在、DCSSIと共に評価活動中の組織（4つ） AQL/CEACI/SERMA/CEA -現在、評価機関の許可申請中の組織（3つ） Ernst&Young eLabel/Algoriel/Oppida	・ITSEC/CCに基づき、民間企業による認証作業を許可。 - BSIの認可企業：7社 - TUV InformationstechniK GmbHの認可企業：10社 ・ITSECの相互認証 - 12加盟国（ﾌｨﾝﾗﾝﾄﾞ、ﾌﾗﾝｽ、ﾄﾞｲﾂ、ｷﾞﾘｼｬ、ｲﾀﾘｱ、ｵﾗﾝﾀﾞ、ﾉﾙｳｪｰ、ﾎﾟﾙﾄｶﾞﾙ、ｽﾍﾟｲﾝ、ｽｳｪｰﾃﾞﾝ、ｽｲｽ、ｲｷﾞﾘｽ） - 認証ﾚﾍﾞﾙ：EAL7 ・CCの相互認証 - 8加盟国（ｶﾅﾀﾞ、ﾌﾗﾝｽ、ﾄﾞｲﾂ、ｲｷﾞﾘｽ、ｱﾒﾘｶ、ｵｰｽﾄﾗﾘｱ、ﾆｭｰｼﾞｰﾗﾝﾄﾞ）：2000年末時点 - 認証ﾚﾍﾞﾙ：EAL4 ※上記取り決めを修正した規約には、さらに7ヶ国(ﾌｨﾝﾗﾝﾄﾞ、ｷﾞﾘｼｬ、ｲﾀﾘｱ、ｵﾗﾝﾀﾞ、ﾉﾙｳｪｰ、ｽﾍﾟｲﾝ）が加盟。	暗号機能については、ｱﾙｺﾞﾘｽﾞﾑも実装ﾚﾍﾞﾙもＤＳＤのCryptographic Evaluation and Export Control と呼ばれる部署で行われている。
・同じｾｷｭﾘﾃｨﾚﾍﾞﾙにあるべき暗号ﾓｼﾞｭｰﾙとﾒｶﾆｽﾞﾑの強度に関する一般的なｶﾞｲﾄﾞﾗｲﾝのみ。 ・扱う製品/ｾｷｭﾘﾃｨﾚﾍﾞﾙによって評価機関が分類されている。	情報入手ができなかったため、不明。	公表されていないため、不明。 （実施手順はDSD独自）
・政府は評価自体は行っていないが、認証を行っている。 -機密部分は政府、機密部分以外は民間評価機関が認証を実施。 -政府は暗号の評価を指揮しているが、暗号の完全さをﾁｪｯｸするための基本的ﾒｶﾆｽﾞﾑのﾚﾍﾞﾙにとどまっている。 ・年間のITｾｷｭﾘﾃｨ証明数（暗号ﾓｼﾞｭｰﾙ認証を含む） -年5～7件から年約25件まで増加している。	・国内および相互認証による他国の例あり。 ただし、以下の例で暗号実装評価の実施は不明。 ー認証ﾚﾍﾞﾙ：EAL5+ の製品例 Smart Card Controller P8WE6017V11 ；Philips製 ー認証ﾚﾍﾞﾙ：E4 の製品例 aSetcad 202 Software Version 1.43(Smartcard Reader Operating System) ；Setec Oy製 ー認証ﾚﾍﾞﾙ：E3/high の製品例 KITAS 2171 Firmware(Motion Sensor) ；Mannesmann VDO AG製	・ｽﾏｰﾄｶｰﾄﾞOS：MULTOS version4.02(Keycorp Ltd.製） -評価担当 ・OS(ｿﾌﾄ)部分：CMG(AISEF評価機関の一つ) ・ﾊｰﾄﾞ部分：Mondex International ・暗号部分：DSD -評価期間：2年半(1998.1～2000.5) MULTOSの開発と平行して実施。 -認定：2000年7月にAISEP認定
情報入手ができなかったため、不明。	情報入手ができなかったため、不明。	製品ﾚﾍﾞﾙで評価を実施しているため、各製品が、暗号ﾌﾟﾛﾄｺﾙを使用するかどうかは認定した製品ﾘｽﾄを参照。
情報入手ができなかったため、不明。	情報入手ができなかったため、不明。	・商用製品および商用ｼｽﾃﾑが納品前にDSDによって評価され認証されることが必須。 ・暗号製品は、政府関係機関での利用に適合するかどうかに関し、DSDによるﾚﾋﾞｭｰを受ける必要がある。 ・政府で利用される製品選択の評価基準はDSDのEPLにある。
情報入手ができなかったため、不明。	情報入手ができなかったため、不明。	政府機関で利用される商用暗号製品はAISEPに基づき評価されなければならない。
情報入手ができなかったため、不明。	情報入手ができなかったため、不明。	・実際の製品評価の実施手順に関する詳細情報は未公開。 -製品の暗号機能の妥当性確認 DSD, Information Security Group, Cryptographic Evaluation Sectionによって行われる。 -製品の検査/評価 AISEFによって行われる。
情報入手ができなかったため、不明。	情報入手ができなかったため、不明。	暗号および非暗号製品を含むITSEC/CCの認証製品ﾘｽﾄあり。 -ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ製品：34件 -公開鍵技術：8件 -ｽﾏｰﾄｶｰﾄﾞ技術：2件 -OS：11件 -PCｾｷｭﾘﾃｨ製品：14件 -ﾊﾞｲｵ認証技術：1件 -ﾎｽﾄｾｷｭﾘﾃｨﾓｼﾞｭｰﾙ：1件 -その他製品：10件

ニュージーランド
GCSB (Government Communications Security Bureau)
・ﾆｭｰｼﾞｰﾗﾝﾄﾞ政府下にあるｾｷｭﾘﾃｨ対策機関。 -1996年からｵｰｽﾄﾗﾘｱDSD運営のAISEPに参加。情報・ITｻｰﾋﾞｽに関する暗号などの評価認証を実施。 -外部のｻｲﾊﾞｰ脅威からｲﾝﾌﾗを保護するため、2002年4月にCCIPをGCSB内に設置すると発表。
・ﾆｭｰｼﾞｰﾗﾝﾄﾞの海外情報(SIGINT)要件の収集および報告を通じて重要情報の提供を行う。 ・ﾆｭｰｼﾞｰﾗﾝﾄﾞ政府の省庁および政府機関に対して、情報ｼｽﾃﾑｾｷｭﾘﾃｨ(INFOSEC)を提供することを通じて公的情報の完全性、可用性および機密性を保証する。
職員数：約220名 予算：2千万ドル
あり (ただし、ﾆｭｰｼﾞﾗﾝﾄﾞ独自の暗号評価ｱﾙｺﾞﾘｽﾞﾑはなく、ｵｰｽﾄﾗﾘｱとのAISEPに依存している。)
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
ﾆｭｰｼﾞﾗﾝﾄﾞ独自の評価ﾌﾟﾛｸﾞﾗﾑについては、今後の運営可能性は当面ない。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。
・ｵｰｽﾄﾗﾘｱのDSDの内容を参照のこと。

付録２：耐タンパー技術関連資料

- 細川 勉, 宮内 宏, 木村 道弘, “鍵管理装置 CK-Guard,” NEC 技法, Vol.51, No.9, pp.146-149, 1998.
- 熊山 治良, 福澤 寧子, 花田 晋一, 佐藤 義人, “ノンストップ自動車料金収受システム,” 日立評論, Vol.83, N0.6, pp.39-42, 2001.
- 宝木 和夫, 荒井 孝雄, 中田 邦彦, 原 秀幸, 山田 徹, “暗号機能付きシステム LSI とその応用,” 日立評論, Vol.81, N0.10, pp.21-24, 1999.
- 堀江 武, 川村 巧, 山本 勝之, 福澤 寧子, “ETC（有料道路自動料金収受）システムを支えるセキュリティシステム,” 日立評論, Vol.82, N0.3, pp.15-18, 2000.
- 中田 邦彦, 北川 信男, 長崎 信孝, “IC カードを支える半導体技術,” 日立評論, Vol.80, N0.4, pp.51-54, 1998.
- 兼平 晃, 三宅 順, 戸塚 隆, “ユビキタス情報社会のセキュリティを支える「PIN セキュアマルティメディアカード」,” 日立評論, Vol.84, N0.10, pp.29-32, 2002.
- 笛木 俊介, “FRAM 搭載商品のセキュリティ設計,” FUJITSU, Vol.53. No.2, pp.110-115, 2002.
- 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 調査報告書,” 2000. http://www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/report/SmartCard/
- 吉松 健三, 川村 信一, “IC カード技術と情報セキュリティ,” 東芝レビュー Vol.52, No.2, pp.14-17, 1997.
- 上野 秀樹, 鈴木 勝宜, “ETC システムにおけるセキュリティ,” 東芝レビュー Vol.56, No.7, pp.14-17, 2001.

付録３：調査対象論文リスト

1. 侵入型解析法

- [AK] R. Anderson, M. Kuhn “Tamper Resistance – a Cautionary Note”-----*2nd USENIX Workshop on Electronic Commerce, 1996*

- [AK97] R. Anderson, M. Kuhn, "Low Cost Attacks on Tamper Resistant Devices"
-----*Security Protocols, 5th International Workshop*, 1997.

- [HPS99] H. Handschuh, P. Paillier, J. Stern, "Probing Attacks on Tamper-Resistant Devices",
-----*Proceedings of CHES '99*

- [KK99] O. Kommerling, M. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors",
-----*USENIX Workshop on Smartcard Technology*, 1999.

2. 非侵入型解析法（サイドチャネル攻撃）

2.1 フォールト・ベース攻撃

- [BDL96] D. Boneh, R. A. DeMillo, and R. J. Lipton, "A New Breed of Crypto Attack on "Tamperproof" Tokens Cracks Even the Strongest RSA Code", 1996.

- [BDL97] D. Boneh, R. A. DeMillo, R. J. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults",
-----*Advances in Cryptology: Proceedings of Eurocrypt '97*

- [BS97] E. Biham, A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems"
-----*Advances in Cryptology: Proceedings of CRYPTO '97*

- [JQ97] M. Joye, J.-J. Quisquater, "Faulty RSA Encryption"
-----*UCL Report*, 1997

- [MS97] 盛合 志帆, "故障利用暗号攻撃によるブロック暗号の解読",
-----*Proceeding of SCIS '97*

- P. Paillier, “Evaluating Differential Fault Analysis of Unknown Cryptosystems”, PKC’99

- S.-M. Yen, S. Kim, S. Lim, and S. Moon, “RSA Speedup with Residue Number System Immune against Hardware Fault Cryptanalysis”, ICISC’01

- S.Skorobogatov and R.Anderson, “Optical fault induction attacks”, CHES2002

- E.Trichina, D.De Seta, L.Germani, “Simplified Adaptive Multiplicative Masking for AES and its Securized Implementation”, CHES2002

- S.Chari, J.R.Rao, P.Rohatgi, “Template Attacks”, CHES2002

- S.Agrawal, B.Archambeault, J.R.Rao, P.Rohatgi, “The EM side-channel(s)”, CHES2002

2.2 タイミング攻撃

- [Koc96] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", *CRYPTO '96*

- [DK+98] J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestre, J.-J. Quisquater, J.-L. Willems, "A Practical Implementation of the Timing Attack", *UCL Report*, 1998

- W. Schindler, “A Timing Attack against RSA with the Chinese Remainder Theorem” ----- *Proceedings of CHES '00*

- H. Handschuh and H. M. Heys, “A Timing Attack on RC5”, SAC’98

- K. Okeya, H. Kurumatani, and K. Sakurai, “Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications”, PKC’00

2.3 電力解析攻撃

2.3.1 共通鍵暗号系に対する電力解析攻撃

- P. Kocher, J. Jaffe, B. Jun, "Introduction to Differential Power Analysis and Related Attacks", 1998

- P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis", *CRYPTO '99*

- T. S. Messerges, E. A. Dabbish, R. H. Sloan, "Investigations of Power Analysis Attacks on Smartcards", *USENIX Workshop on Smartcard Technology*, 1999.

- E. Biham, A. Shamir, "Power Analysis of the Key Scheduling of the AES Candidates"

-----*Proceedings of the Second Advanced Encryption Standard Candidate Conference*, 1999.

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

- S. Chari, C. Jutla, J. Rao, P. Rohatgi, "Toward Sound Approaches to Counter Power Analysis Attacks" *CRYPTO '99*

- [GP99] L. Goubin, J. Patarin, "DES and Differential Power Analysis", *CHES '99*

- M.Akkar and C.Giraud, "An Implementation of DES and AES, Secure against Some Attacks", CHES'01

- Thomas S.Messerges, "Securing the AES Finialists Against Power Analysis Attacks", Fast Software Encryption, FSE 2000, pp.150-164.FSE2000

- J. S. Coron, L. Goubin, “On Boolean and Arithmetic Masking against Differential Power Analysis”

----- *Proceedings of CHES '00*

- L.Goubin, "A Sound Method for Switching between Boolean and Arithmetic Masking", CHES'01

- K. Itoh, M. Takenaka, and N. Torii, “DPA Countermeasure Based on the “Masking

Method"", ICISC'01

- J.Dj.Golic, C.Tymen, "Multiplicative Masking and Power Analysis of AES", CHES2002

2.3.2 公開鍵暗号系に対する電力解析攻撃

【ＲＳＡ関連】

- T. S. Messerges, E. A. Dabbish, R. H. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards", *CHES '99*

- G. Hachez and J.-J. Quisquater, "Montgomery Exponentiation with no Final Subtractions: Improved Results", CHES'00

- C.Clavier and M.Joye, "Universal exponentiation Algorithm: A First Step towards Provable SPA-Resgistance", CHES'01

- C.D.Walter, "Sliding Windows Succumbs to Big Mac Attack", CHES'01

- S.-M. Yen, S. Kim, S. Lim, and S. Moon, "A Countermeasure against One Physical Cryptanalysis May Benefit Another Attack", ICISC'01

- C. D. Walter and S. Thompson, "Distinguishing Exponent Digits by Observing Modular Subtractions", CT-RSA'01

- M. Joye, J.-J. Quisquater, S.-M. Yen, and M. Yung, "Observability Analysis ― Detecting When Improved Cryptosystems Fail ―", CT-RSA'02

- C. D. Walter, "Precise Bounds for Montgomery Modular Multiplication and Some Potentially Insecure RSA Moduli", CT-RSA'02

- C. D. Walter, "MIST: An Efficient, Randomized Exponentiation Algorithm for Resisting Power Analysis", CT-RSA'02

- R. Novak, "SPA-Based Adaptive Chosen-Ciphertext Attack on RSA

Implementation”, PKC’02

- W. Schindler, “Combined Timing and Power Attack”, PKC’02
- C.D.Walter, “Some Secyrity of the MIST Randomizing Exponential Algorithm”, CHES2002
- K.Itoh, J.Yajima, M.Takenaka, N.Torii, “DPA Countermeasure by improving the Window Method”, CHES2002
- B.den Boer, K.Lemke, G.Wiche, “A DPA Attack Against the Modular Reduction with a CRT Implementation of RSA”, CHES2002
- V.Klima, T.Rosa, “Further Results and Considerations on Side Channel Attacks on RSA”, CHES2002
- C.Aumueller, P.Bier, W.Fischer, P.Hofreiter, J.P.Seifert, “Fault attacks on RSA with CRT :Concrete Results and Practical Counter measures”, CHES2002

【楕円曲線暗号関連】

- [Cor99] J.-S. Coron, "Resistance Against Differential Power Analysis for Elliptic Curbe Cryptosystems", *CHES '99*
- M. A. Hasan, “Power Analysis Attacks and Algorithmic Approaches to their Countermeasures for Koblitz Curve Cryptosystems”, *CHES '00*
- E.Oswald and M.Aigner, "Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks", CHES'01
- M.Joye and C.Tymen, "Protections against Differential Analysis for Elliptic Curve Cryptography: An Algebraic Approach", CHES'01
- P.-Y.Liardet and N.P.Smart, "Preventing SPA/DPA in ECC Systems Using the

Jacobi Form", CHES'01

- M.Joye and J.-J.Qusiquater, "Hessian Elliptic Curves and Slide-Channel Attacks", CHES'01

- K. Okeya and K. Sakurai, “Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack”, Indocrypt'00

- K. Okeya, K. Miyazaki, and K. Sakurai, “A Fast Scalar Multiplication Method with Randomized Projective Coordinates on a Montgomery-Form Elliptic Curve Secure against Side Channel Attacks”, ICISC'01

- T. Izu and T. Takagi, “A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks”, PKC'02

- E. Brier and Marc Joye, “Weierstra Elliptic Curves and Side-Channel Attacks”, PKC'02

- E.Oswald, “Enhancing Simple Power-Analysis Attacks on Elliptic Curve Cryptosystems”, CHES2002

- E.Trichina, A.Bellezza, “Implementation of Elliptic Curve Cryptography with Built-in Counter Measures against Side Channel Attacks”, CHES2002

- C.Gebotys, R.Gebotys, ”Secure Elliptic Curve Implementations: An Analysis of Resistance to Power-Attacks in a DSP Processor”, CHES2002

- K.Itoh, T.Izu, “Address-bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA”, CHES2002

- M.Ciet, J-J.Quisquater, F.Sica, “Preventing Differential Analysis in GLV Elliptic Curve Scalar Multiplication”, CHES2002

- J.C.Ha, S.J.Moon, “Randomized Signed-Scalar Multiplication of ECC to Resist Power Attacks”, CHES2002

2.3.3 アタックの拡張

- R. Mayer-Sommer, “Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards”----- *Proceedings of CHES '00*

- [Fah99] P. N. Fahn, "IPA: A New Class of Power Attacks"-----*Proceedings of CHES' 99*

- T. S. Messerges, “Using Second-Order Power Analysis to Attack DPA Resistant Software”----- *Proceedings of CHES '00*

- Electromagnetic Attacks, CHES01

- M.-L. Akkar, R. Bevan, P. Dischamp, and D. Moyart, “Power Analysis, What Is Now Possible…”, Asiacrypt 2000

2.3.4 ハードウェア関連

- Shamir, ”Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies”----- *Proceedings of CHES '00*

- C. Clavier, J. S. Coron, N. Dabbous, “Differential Power Analysis in the Presence of Hardware Countermeasure”----- *Proceedings of CHES '00*

- E.Brier, H.Handschuh, and C.Tymen, "Fast Primitives for Internal Data Scrambling in Tamper Resistant Hardware", CHES'01

- D.May, H.L.Muller, and N.P.Smart, "Random Register Renaming to Foil DPA", CHES'01