CRYPTREC Report 2007

平成 20 年 3 月

独立行政法人 情報処理推進機構

独立行政法人 情報通信研究機構

「暗号モジュール委員会報告」

目次

はじめに

本報告書は、暗号技術検討会の下に設置された暗号モジュール委員会の 2007 年度活動報告である。

2000 年度から 3 年間に渡る暗号技術評価プロジェクト(CRYPTREC)の活動の成果として、2003 年 2 月に総務省と経済産業省から「電子政府推奨暗号リスト」が公表された。その後、CRYPTREC においては、暗号アルゴリズムそのものの安全性評価だけでなく、暗号化 LSI 等の暗号製品(暗号モジュール)の安全性を評価する必要性を認識し、暗号技術検討会の下に、独立行政法人 情報処理推進機構と通信･放送機構(現 独立行政法人 情報通信研究機構)が共同で運営する暗号モジュール委員会を設置し、暗号モジュールの安全性に関する要件の検討等を行っている。

本年度は、7 月に米国 NIST で改訂中の FIPS 140-3 の草案が公開されたことを受け、日本規格協会情報技術標準化研究センター(INSTAC)耐タンパー性技術標準化研究委員会と共同で FIPS 140-3 草案に対するコメントの検討を行った。このコメントは CRYPTREC 暗号モジュール委員会及び INSTAC の連名で NIST へ送付した。また、暗号モジュールに対するサイドチャネル攻撃などの暗号モジュールに対する攻撃法や対策の調査研究を、暗号モジュール委員会の傘下にある電力解析実験 WG にて実施し､将来のセキュリティ要件への適用の準備を進めた。本活動を契機として､わが国における暗号実装関連技術の研究が進展することを期待したい。

末筆ではあるが、本活動に様々な形でご協力いただいた委員の皆様、事務局および関係者の皆様に謝意を表する次第である。

2008 年 3 月

暗号モジュール委員会　委員長　松本　勉

本報告書の利用にあたって

本報告書は、一般的な情報セキュリティの基礎知識を有している読者を想定している。例えば､電子署名やGPKIを利用するシステムなど暗号関連の電子政府関連システムに関する業務の従事者などを想定している。ただし、暗号モジュールセキュリティ要件及び暗号モジュール試験要件、並びに運用ガイダンスを理解するためには、ある程度の暗号技術の実装経験があることが望ましい。

本報告書の第1章には暗号モジュール委員会の活動の背景と目的、第2章には暗号モジュール委員会の委員会開催状況、第3章には暗号モジュール委員会の活動内容と成果概要を記述した。

2006年度以前のCRYPTREC Reportは、下記URLで参照できる。

http://www.cryptrec.go.jp/report.html

本報告書に対するご意見、お問合せ等は、CRYPTREC事務局までご連絡していただけると幸いである。

【問合せ先】　info@cryptrec.go.jp

委員会構成

暗号モジュール委員会は、図１に示すように、総務省と経済産業省が共同で共催する暗号技術検討会の下に設置され、独立行政法人 情報処理推進機構（IPA）と独立行政法人 情報通信研究機構（NICT）が共同運営している。

暗号モジュール委員会では、ISO/IEC 等の国際標準の動向を注視しつつ、将来的に政府調達基準等として利用されることをも視野に入れながら、暗号モジュール評価基準及び試験基準の策定を行っている。また、電子政府推奨暗号の安全性及び信頼性確保のための、主として暗号実装関連技術等を対象とする調査・検討も行っている。

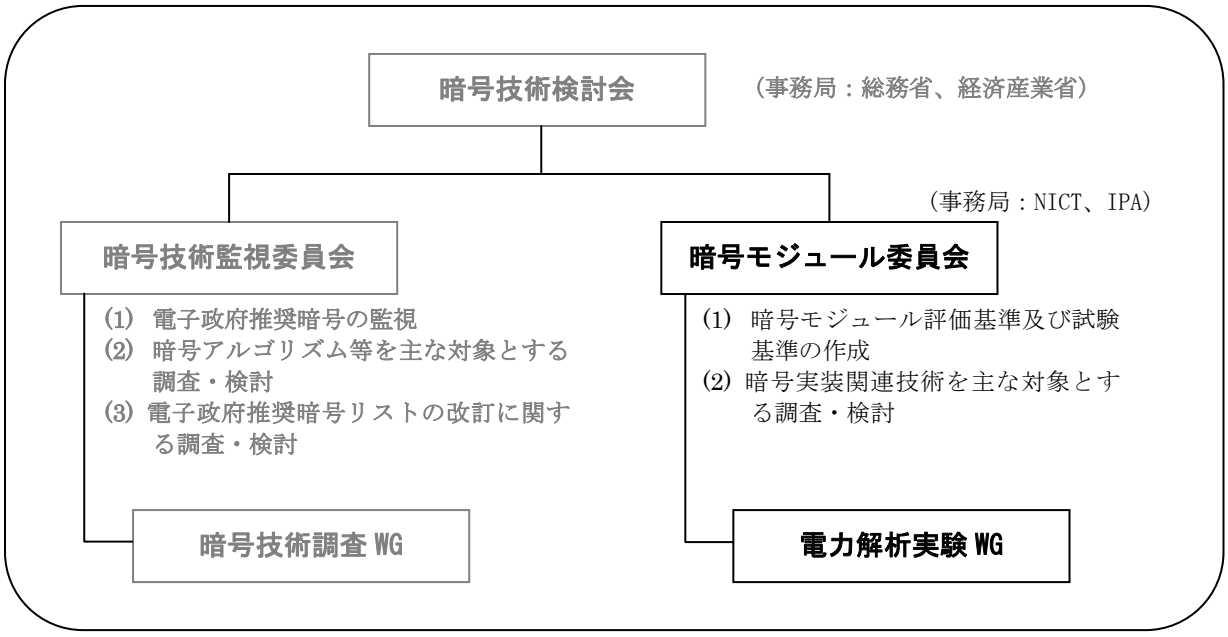

図１　2007 年度の CRYPTREC の体制

委員名簿

暗号モジュール委員会　(2008 年 3 月現在)

委員長	松本　勉	国立大学法人横浜国立大学 大学院　教授
委員	植村　泰佳	電子商取引安全技術研究組合　専務理事
委員	大須賀　勝美	NTT エレクトロニクス株式会社　主事
委員	太田　和夫	国立大学法人電気通信大学　教授
委員	福永　利徳	日本電信電話株式会社　研究主任
委員	亀田　繁	財団法人日本情報処理開発協会　センター長
委員	佐伯　稔	三菱電機株式会社　主席研究員
委員	佐藤　証	独立行政法人産業技術総合研究所　主任研究員
委員	高橋　芳夫	株式会社 NTT データ　シニアエキスパート
委員	角尾　幸保	日本電気株式会社　主席研究員
委員	栃窪　孝也	日本大学　専任講師
委員	鳥居　直哉	株式会社富士通研究所　部長
委員	古屋　聡一	株式会社日立製作所　研究員
委員	森岡　澄夫	日本電気株式会社　主任研究員
委員	横田　薫	松下電器産業株式会社　主任技師
委員	吉田　健一郎	財団法人日本品質保証機構

オブザーバ

氏原　正勝	警察庁	情報通信局
谷川　健	警察庁	情報通信局
伊東　信孝	警察大学校	警察情報通信研究センター
山本　寛繁	総務省	行政管理局
藤田　和重	総務省	情報通信政策局(2007 年 7 月まで)
能登　治	総務省	情報通信政策局(2007 年 7 月まで)
網野　尚子	総務省	情報通信政策局(2007 年 7 月まで)
荻原　直彦	総務省	情報通信政策局(2007 年 7 月より)
川崎　光博	総務省	情報通信政策局(2007 年 12 月まで)
増子　喬紀	総務省	情報通信政策局(2007 年 12 月より)
山崎　浩史	総務省	情報通信政策局(2007 年 7 月より)
東山　誠	外務省	大臣官房

山元　明裕　　外務省　大臣官房
森田　信輝　　経済産業省　産業技術環境局
小野塚　直人　経済産業省　商務情報政策局
太田　保光　　経済産業省　商務情報政策局（2007 年 5 月まで）
花田　高広　　経済産業省　商務情報政策局（2007 年 5 月より）
神藤　守　　防衛省　陸上幕僚監部
石川　正興　　防衛省　技術研究本部
武田　仁己　　防衛省　運用企画局
滝澤　修　　独立行政法人　情報通信研究機構
川村　信一　　財団法人日本規格協会
瀬戸　洋一　　財団法人日本規格協会
山中　正幸　　財団法人日本規格協会

事務局

独立行政法人　情報処理推進機構
　三角　育生（2007 年 6 月まで）
　山田　安秀（2007 年 6 月から）
　山岸　篤弘
　大久保　美也子
　伊東　徹
　鈴木　幸子

独立行政法人　情報通信研究機構
　篠田　陽一
　山村　明弘
　黒川　貴司
　金森　祥子

第１章　活動の背景と目的

1.1　CRYPTREC 活動の経緯

近年のインターネットの爆発的な普及と情報通信技術の飛躍的な発展により、社会・経済のネットワーク化が急速に進展している。電子商取引に代表されるように、オープンなネットワークを介して相手と直接対面することなく重要な情報をやり取りし、受発注や決済等を行うことが日常的になってきている。

また、政府の動きとしても、各種申請届出手続きや政府調達などの行政サービスを電子化する電子政府システムの構築が進められている。e-Japan 重点計画等で、電子政府システムにおける情報セキュリティの確保及びその基盤となる暗号技術の重要性が認識され、関連する施策が実行に移されている。

このような状況で、現在、様々な暗号技術が開発され、それを組み込んだ多くの製品が市場に提供されているが、全ての暗号技術の安全性が評価・確認されている訳ではない。電子政府システムの安全性を保つには、暗号技術を客観的に評価することが極めて重要である。

以上のような背景から、通商産業省（現経済産業省）からの委託を受けて、情報処理振興事業協会（現 独立行政法人 情報処理推進機構(IPA)）は電子政府で利用可能な暗号技術を安全性及び実装性能など技術的な面から評価することを目的とした暗号技術評価委員会を2000年5月に設置した。産学の最高水準の暗号専門家で構成されたこの委員会の設置により、わが国において本格的な暗号技術評価プロジェクトがスタートした。 翌年度には、委員会の共同事務局として通信・放送機構（現 独立行政法人 情報通信研究機構(NICT)）が参加した。

2001 年度には、経済産業省と総務省が共同で暗号技術検討会を設置し、暗号技術の利用に関する政策的な観点からの検討が開始された。暗号技術評価委員会と暗号技術検討会は、関係する省庁がオブザーバとして参加する等、政府横断的な活動であり、これらを総称して、CRYPTREC(CRYPTography Research and Evaluation Committees)と呼んでいる。

2000 年度から 2002 年度までの 3 年間に及ぶ CRYPTREC 活動で、電子政府システムで安心して利用できる暗号を選定するための客観的な評価が実施された。その結果、合計 29 方式の暗号技術が安全性及び実装性能に問題がないとされ、2003 年 2 月に総務省と経済産業省によって「電子政府推奨暗号リスト」が公開された。

2003 年度からは、電子政府の安全性及び信頼性を引き続き確保していくため、新しい体制に移行した。暗号技術検討会は存続とし、暗号技術検討会の下に「暗号技術監視委員会」及び「暗号モジュール委員会」を新設し、さらに、「暗号技術監視委員会」の下に「暗号技術調査 WG」を新設した。従来の暗号技術評価委員会は、暗号技術監視委員会に発展的に再編され、電子政府推奨暗号リストに掲載された暗号の安全性を監視する。従来の公開鍵暗号評価小委員会及び共通鍵評価小委員会は暗号技術調査 WG に再編され、監視委員会で必要と判断した個別テーマに関する調査を実施する。

2006 年度の 12 月からは、暗号モジュールへの実際の脅威となりつつあるサイドチャネル攻撃の一つである電力解析攻撃等について、実験を踏まえて脅威と対策を検討することにより、暗号モジュール製品の安全性を確保すると共に、FIPS（Federal Information Processing Standard） PUB 140-3 の試験要件作成に反映させることを目標として、「暗号モジュール委員会」の下に「電力解析実験 WG」を新設した。

この WG では、財団法人 日本規格協会 情報技術標準化センター（INSTAC） 耐タンパー性標準化調査研究委員会による、サイドチャネル攻撃耐性評価標準プラットフォーム仕様 INSTAC-8/-32 準拠のプラットフォーム（INSTAC-8, INSTAC-32）を用いた実験を行うことにより、電力解析に対する技術的な蓄積を実施してきた。

1.1.1 活動の総括

暗号モジュール委員会は、2003 年 3 月に策定された「電子政府推奨暗号リスト」に掲載された暗号技術を安全に使用するために、暗号機能を提供する暗号モジュールへの実装攻撃等の暗号実装関連技術を主な対象として調査及び検討を行うことを目的として設立された。

2003 年、2004 年の両年度にわたり、米国 NIST とカナダ CSE が運用している CMVP（暗号モジュール試験及び認証）制度の調査を行い、暗号モジュールに対するセキュリティ要件及び試験要件に対する研究を実施し、暗号モジュールに対するセキュリティ要件(案)及び試験要件（案）を作成した。

このセキュリティ要件等を検討する間、米国およびカナダが運用していた CMVP 制度における暗号モジュールに対するセキュリティ要件である FIPS（Federal Information Processing Standard）PUB 140-2 が、米国より、国際標準化機関である ISO（International Standard Organization）に、国際標準として提案され審議が始まったため、2004 年度からは、ISO/IEC JTC1 SC27/WG3 における標準化作業に対するコメント作成等の活動や 2006 年度に検討が開始された FISP 140-3 に対する検討作業を行ってきた。

また、米国/カナダにおける CMVP 制度のセキュリティ要件である FIPS PUB 140-2 の改訂への対応を考慮し、財団法人 日本規格協会 情報技術標準化センター（INSTAC）耐タンパー性標準化調査研究委員会と協調して、電力解析攻撃などのサイドチャネル攻撃の対策技術のセキュリティ要件や試験要件の研究を実施してきた。特に、暗号モジュール委員会と耐タンパー性標準化調査研究委員会とで検討した電力解析実験標準仕様（INSTAC-8/-32 仕様）に基づく標準基板を開発し、暗号モジュール委員会委員を中心に配布し、電力解析技術の蓄積を行った。

1.1.2 暗号モジュール委員会を取り巻く環境の変化

2003 年の暗号モジュール委員会の活動を開始した後、2004 年には、独立行政法人 情報通信研究機構が発足し、2005 年には、独立行政法人 産業技術総合研究所(AIST)の情

報セキュリティ研究センター(RCIS)が発足し、暗号モジュールの安全性評価に対する研究体制の充実がはかられた。さらに、2006 年には、ISO での暗号モジュールに対するセキュリティ要件の国際標準の成立を受け、独立行政法人 情報処理推進機構内に暗号モジュール試験及び認証の試験機関と認証機関を創設し、日本における暗号モジュールの試験及び認証制度(JCMVP)が創設された。

また、2006 年度に検討が開始された FIPS PUB 140-3 の作成作業は、2007 年 7 月に Draft が公開され、2007 年 10 月のコメント募集を経て、2008 年度中に FIPS PUB 140-3 が制定される見込みとなり、2008 年 5 月には、FIPS PUB 140-3 をベースとした暗号モジュールに対するセキュリティ要件の国際規格 ISO/IEC 19790 の改訂が提案される予定となっている。

このような環境の変化に合わせ、暗号モジュール委員会では FIPS PUB 140-3 草案へのコメント作成を行うとともに、暗号モジュールの安全性の確保と試験要件作成への反映を目標に電力解析実験 WG を組織し、サイドチャネル攻撃耐性評価標準プラットフォーム仕様 INSTAC-8/-32 準拠プラットフォーム（INSTAC-8, INSTAC-32）やその後継機種であるサイドチャネル攻撃実験用標準評価ボード（SASEBO）を用いて、電力解析に対する技術的な蓄積を実施してきた。

1.2 暗号モジュールの試験及び認証に関する国際標準化動向

安心できる実用的な情報セキュリティシステムの構築において、安全で実装性能の高い暗号アルゴリズムの選択は不可欠の条件である。しかし、それだけでは不十分であり、暗号アルゴリズムを適切な方法で実装することが不可欠である。暗号アルゴリズムをソフトウェア及びハードウェアとして実装したものである、暗号モジュールに対して、動作の信頼性や安全性を評価する基準をセキュリティ要件と呼び、国際的な影響力を持つものには次の２つがある。

(1)FIPS[1] PUB 140-2/140-3（米国 NIST[2]、カナダ CSE[3]）

(2)ISO[4]/IEC[5] 19790

1.2.1 FIPS PUB 140-2/140-3

FIPS PUB 140-2 は、米国/カナダが共同運用している CMVP[6]制度で利用されているセキュリティ要件に関する規格であり、米国 NIST によって発行されている。この規格の関連文書に試験要件(DTR[7])と運用ガイダンス(IG[8])の 2 種類があり、NIST は必要に応じて適宜改訂

1 Federal Information Processing Standard
2 National Institute of Standards & Technology
3 Communications Security Establishment
4 International Organization for Standardization
5 International Electrotechnical Commission
6 Cryptographic Module Validation Program
7 Derived Test Requirements

している。DTR は暗号モジュールがセキュリティ要件を実際に満たすか確かめるための試験項目を定めたものである。また、IG には試験を実施する際の運用法を定めたもので、質問とそれに対する回答という形式で記述されている。

NIST/CSE[9]は 5 年ごとの定期見直しに従い、セキュリティ要件を次期バージョン FIPS PUB 140-3 に改訂する作業を開始している。2007 年 7 月には、FIPS PUB 140-3 の草案が公開された。

FIPS PUB 140-3 では、セキュリティレベルが 5 段階に増えると共に、サイドチャネル攻撃へのセキュリティ要件が盛り込まれていることが特徴である。

2007 年 7 月に公開された草案に対するコメントは、2007 年 10 月 11 日に締め切られ、現在 NIST で、各国から寄せられたコメントを検討の上、修正が施されている。この修正案は、早ければ、2008 年 5 月には公開される見込みである。その後、再度コメント募集が行われた後、早ければ 2008 年末には、米商務省に提出され、正式な FIPS PUB 140-3 として発行されると考えられる。

1.2.2 ISO/IEC 19790

ISO/IEC 19790 は、FIPS PUB 140-2 を基に作られた国際規格である。ISO/IEC JTC 1[10] SC 27/WG 3 のプロジェクトとして審議され、2005 年 12 月締め切りで行われた FDIS[11]投票で可決され、国際事務局の修正後 2006 年 3 月 1 日に発行された。

また、実際の運用に必要であるということで、ISO/IEC 19790 に対する試験要件の標準化が新規プロジェクトとして承認され、規格番号 24759 が割り当てられている。2005 年 11 月の Kuala Lumpur でプロジェクトの承認が報告され、エディタとして Randy Easter(米国 NIST)、コエディタとして Jean-Pierre Quemard(仏)と Hans von Sommerfeld が任命された。ISO/IEC 19790 に対する試験要件である 24759 は、ISO/IEC 19790 同様に、FIPS PUB 140-2 に対する試験要件を基に開発され、現在、Final CD[12]の投票中で、2008 年 4 月の会合で規格化される見込みである。

さらに、米国 NIST は FIPS PUB 140-2 の後継として準備中の FIPS PUB 140-3 の国際規格化を SC 27 に提案する意向であり、2007 年 10 月のスイス会合に新規検討事項(NP[13])として早期改訂に着手することが承認された。2008 年 4 月の京都会合に、改訂中の FIPS PUB 140-3 の草案が、ISO/IEC 19790 の改定案として提出される見込みである。

1.2.3 ISO/IEC 24759

ISO/IEC 19790 に対する試験要件の標準化が、FIPS PUB 140-2 同様に実際の運用に必要

---

8 Implementation Guidance
9 Communication Security Establishment
10 Joint Technical Committee 1
11 Final Draft International Standard
12 Committee Draft
13 New Work Item Proposal

であるということで、2005 年 11 月の Kuala Lumpur においてプロジェクトの承認が報告され、エディタとして Randy Easter(米国 NIST)、コエディタとして Jean-Pierre Quemard(仏)と Hans von Sommerfeld が任命された。2007 年 3 月に 1st CD[14]の投票が行われ、2007 年 5 月のロシア会合で 1st CD 案のコメント処理を経て FCD 投票に進んだ。2008 年には規格化される見込みである。

1.3 暗号モジュール委員会の活動状況

1.3.1 過去の経緯

暗号を組み込んだ製品の安全性を実現するには、安全性が確認された暗号の利用が不可欠であり、2003 年 2 月に発表された電子政府推奨暗号リストに記載された暗号から選択することによりこの条件は満たされる。しかし、暗号を組み込んだ製品の安全性を保つにはこれだけでは不十分であり、暗号アルゴリズムが適切に実装されていることを確認する必要がある。

この目的のためには、実装が適切に行われていることを確認する仕組みが必要であり、米国・カナダでは CMVP として試験及び認証の制度が実施されている。CRYPTREC では、このような制度の基となる暗号モジュールに対するセキュリティ要件等の素案作成、及びその素案作成に必要となる実装攻撃に関する知見を得るための活動が必要と判断し、2003 年度から、次の 2 つを活動の柱として、暗号技術検討会の下に暗号モジュール委員会を設置した。

(1)暗号モジュール評価基準[15]及び試験基準[16]の策定

(2)暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究

(1)では、将来的に政府調達基準として利用されることを前提に暗号モジュール評価基準及び試験基準の策定作業を行う。(2)では、暗号モジュールの実装方法の安全性評価を行うための基礎となるデータを収集する。

2003 年度の活動概要

(1) 暗号モジュール評価基準及び試験基準の策定

国内基準策定を目指し、ISO/IEC 国際規格の動向を注視しつつ、北米の評価基準及び試験基準を翻訳し、暗号モジュール評価基準及び試験基準の第0版として発行した。

(2) 暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究

暗号モジュールの実装方法に対する安全性評価法の一環として、非破壊攻撃の１つ

14 Committee Draft

15 2005 年度の活動で、「評価基準」は「セキュリティ要件」に変更された。

16 2005 年度の活動で、「試験基準」は「試験要件」に変更された。

である電力解析をテーマに選び、調査・研究の共通基盤を整えるため、FPGA[17]による評価用標準プラットフォームの要求仕様を策定した。

2004 年度の活動概要

(1) 暗号モジュール評価基準及び試験基準の策定

審議中の国際規格(ISO/IEC 19790)で、FIPS PUB 140-2 の内容を変更する方針が出された。変更点を反映すべく、前年度の基準第 0 版に対し、次の a)～e)の作業を行った。

a)暗号モジュール評価基準の差分表の作成

FIPS PUB 140-2 と国際規格(1st CD 19790)との差分表を作成し、翻訳する。

b)差分表に対応した暗号モジュール試験基準の検討表の作成

上記 a)で作成した暗号モジュール評価基準の差分表に対応した暗号モジュール試験基準の検討表の作成を行う。

c)ISO/IEC JTC 1/SC 27/WG 3 への技術コメント作成協力

国際標準(ISO/IEC 19790)案に対する日本コメント案作成の協力を行う。

d)運用ガイダンス第 0 版の作成

NIST 発行の“Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program(Last Update: April 28, 2004)”及び 4 月 28 日以降に改版に対し、逐次翻訳作業を実施する。

e)暗号モジュール評価基準及び試験基準第 0.1 版の作成

2003 年度作成した第 0 版に対して、NIST 発行の FIPS PUB 140-2, DTR の CHANGE NOTICE を反映した修正を行い、第 0.1 版とする。

(2) 暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究

2003 年度に策定した評価用標準プラットフォームの仕様に従った評価用ボードを調達し、希望する委員に配布するとともに、よりスペックの高い評価用標準プラットフォームの仕様を策定した。また、非破壊攻撃及び破壊攻撃に関する学会活動の調査を行った。具体的には、次の a)～c)の作業を行った。

a)評価用標準プラットフォーム仕様の評価用ボードの調達(8 ビット CPU)

INSTAC[18]の耐タンパー性に関する標準化調査研究委員会が策定した「電力解析のための汎用 8 ビット CPU を用いた評価用標準プラットフォーム仕様」に従った評価用標準プラットフォームを実装し、希望する委員に無償配布した。無償配布の条件として、得られた成果の学会等での発表を義務付けた。

b)評価用標準プラットフォーム仕様の策定(32 ビット CPU)

INSTAC の耐タンパー性に関する標準化調査研究委員会と協調して、「評価用標準

17 Field Programmable Gate Array

18 Information Technology Research and Standardization Center, JSA／(財)日本規格協会情報技術標準化研究センター

プラットフォーム仕様」を策定した。具体的には、INSTAC が策定した「電力解析のための汎用 32 ビット CPU を用いた評価用標準プラットフォーム仕様」と、2003 年度の暗号モジュール委員会で策定した「FPGA を用いた評価用標準プラットフォーム仕様」を融合して、「評価用標準プラットフォーム仕様」を策定した。

c)非破壊攻撃及び破壊攻撃に関する学会活動調査

次の学会に参加し、非破壊攻撃及び破壊攻撃に関する発表を聴講した。ISEC 研究会(7 月、徳島)、CHES 2004(8 月米国・ボストン)、ICD 研究会(9 月、東京)、CSS 2004(10 月、札幌市)、ASIACRYPT 2004(12 月、韓国・済州島)。また、IACR e-Print Archives を初めとする Web 上の発表論文も調査した。

2005 年度の活動概要

(1) 暗号モジュールセキュリティ要件及び暗号モジュール試験要件の策定

前年度に引き続き、FIPS PUB 140-2 と ISO/IEC 19790 に関する動向調査を行いつつ、基準類の策定作業を進めた。基準類のバージョン番号は、2006 年度に発行される正式版を第 1 版とし、それ以前は日付でバージョンを区別する方針になった。

また、前年度では、「暗号モジュール評価基準」「暗号モジュール試験基準」というタイトルで、基準類の策定を行った。しかし、FIPS PUB 140-2 では、「evaluation」と「testing(又は test)」を明確に区別して使用しており、「evaluation」は、Common Criteria 関連の部分でしか使用されていない。 Common Criteria 関連では「評価」、FIPS PUB 140-2 関連では「試験」ということで、用語の使用方法の統一を図った。これにより、基準類のタイトルを、次のように変更した。

FIPS PUB 140-2 Security requirements for cryptographic modules

→「暗号モジュールセキュリティ要件」

Derived Test Requirements [DTR] for FIPS PUB 140-2

→「暗号モジュール試験要件」

a)ISO/IEC JTC 1/SC 27/WG 3 への技術コメント作成協力

国際標準(FCD 19790, FDIS 19790)案に対する日本コメント案作成協力を行った。

b)運用ガイダンスの改訂

NIST 発行の “Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program”の改版に対し、逐次翻訳作業を実施した。

c)暗号モジュールセキュリティ要件及び暗号モジュール試験要件の策定

2004 年度作成した暗号モジュール評価基準第 0.1 版及び試験基準第 0.1 版を基に、FDIS 19790 に対応するための検討を行い、暗号モジュールセキュリティ要件及び暗号モジュール試験要件を策定した。

(2) 暗号モジュールへの非破壊攻撃及び破壊攻撃に対する調査・研究

2004 年度に仕様策定を行った評価用標準プラットフォーム(32 ビット CPU)を実装

した評価用ボードの開発を発注し、希望する委員に配布した。昨年度と同様、無償配布の条件として、得られた成果の学会等での発表を義務付けた。

2006 年度の活動概要

(1) 暗号モジュール試験要件の国際規格作成への貢献

ISO/IEC JTC 1 SC 27 において、ISO/IEC 19790 に対応する試験要件 ISO/IEC 24759 が作成中である。暗号モジュール委員会では、24759 のドラフト WD 及び 1st CD に対するコメント案を作成し、SC 27 国内委員会経由で国際事務局に提案した。

(2) 電力解析実験ワーキンググループの立ち上げ

米国では FIPS PUB 140-2 が FIPS PUB 140-3 に改訂される作業が進められており、その中でサイドチャネル攻撃に関する要件が追加される予定である。暗号モジュール委員会では、サイドチャネル攻撃の一種である電力解析に関する要件の策定に貢献するため、INSTAC-8/-32 仕様に準拠した標準プラットフォームを希望する委員に配布し、実験データの収集を進めてきた。2006 年度は、今まで独立していた実験活動を組織化し、実験効率を高めるため、電力解析実験ワーキンググループを立ち上げた。

(3) 暗号モジュールセキュリティ要件・試験要件の JIS 化

当委員会で作成した「暗号モジュールセキュリティ要件」と「暗号モジュール試験要件 2006-03-31 版」が各々、次の JIS 規格の素案として利用された。

「JIS X 19790 セキュリティ技術-暗号モジュールのセキュリティ要求事項」

「JIS X 5091 セキュリティ技術-暗号モジュールのセキュリティ試験要件」

1.3.2 2007 年度の活動概要

2007 年度暗号モジュール委員会の成果

今年度の暗号モジュール委員会の主要成果としては、次の 4 つが挙げられる。

(1) 暗号モジュール試験要件の国際規格作成への貢献

FIPS PUB 140-2 を基にセキュリティ要件の国際規格 ISO/IEC 19790 が作成され、2006 年に発行されたが、現在、ISO/IEC JTC 1/SC 27 では、19790 に対応した試験要件 ISO/IEC 24759 作成のプロジェクトを進めている。暗号モジュール委員会では、7 月 25 日の第２回暗号モジュール委員会で 24759 の最終ドラフト案を審議し、SC 27 の国内委員会に対し、コメント案の作成に協力した。

(2) FIPS 140-3 へのコメント提出

NIST は、FIPS PUB 140-2 を 140-3 に改訂する準備を進めている。7 月 13 日にドラフトが発行され､暗号モジュール委員会と INSTAC 耐タンパー性標準化調査委員会 WG1 では 9 月 28 日に合同で委員会を開催し、日本としてのコメントをまとめ、10 月 11

日に NIST へ提出した。

(3) 電力解析実験ワーキンググループの活動

米国では FIPS PUB 140-2 を FIPS PUB 140-3 に改訂する作業が進められており、その中でサイドチャネル攻撃に関する要件が追加される。暗号モジュール委員会では、サイドチャネル攻撃に関する要件の策定に貢献するため、INSTAC-8/-32 仕様に準拠した標準プラットフォームを委員に配布し、実験データの収集を進めてきた。9 月には更に産業技術総合研究所と東北大学による新たなサイドチャネル攻撃実験用標準評価ボード（SASEBO：Side-Channel Attack Standard Evaluation Board）とそれに用いる、暗号アルゴリズム（AES,Camellia,DES,Misty1）のソースコードが開発され、電力解析実験ワーキンググループの委員に配布し、暗号モジュールの安全性と標準化の検討ための実験活動とそのまとめを行った。

(4) FIPS PUB 140-2 と 暗号モジュール試験及び認証制度のための運用ガイダンスの日本語の改訂版の作成

NIST 発行の“Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program”は逐次改訂版の発行が行われている。それに対応し暗号モジュール委員会では、日本語の翻訳版の作成作業を行っており、3 月の時点では 2008 年 1 月 24 日版を「FIPS PUB 140-2 と 暗号モジュール試験及び認証制度のための運用ガイダンス」として作成している。

第 2 章　2007 年度の活動内容と成果概要

2.1　暗号モジュールセキュリティ要件等の調査

2.1.1　北米における暗号モジュールセキュリティ要件関連の調査

(1) FIPS PUB 140-2 (SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES)

FIPS PUB 140 は、コンピュータシステム及び電気通信システム内の暗号モジュールに対するセキュリティ要件を規定した、NIST が発行する米国連邦標準規格である。

FIPS PUB 140 は、政府及び産業界で構成されたワーキンググループによって開発された。1994 年 1 月に FIPS PUB 140-1 が制定され、2001 年 5 月には FIPS PUB 140-2 として改訂された。FIPS PUB 140-2 は、ベンダ、試験機関、及びユーザ団体から寄せられたコメントに基づいた変更だけでなく、FIPS PUB 140-1 が開発された以降に利用可能となった標準規格及び技術の変更も取り入れている。FIPS PUB 140-2 は適宜改訂されており、2002 年 12 月の改訂版が 2008 年 3 月時点での最新版となっているが、Annex A は MOD の部分が 2007 年 12 月 18 日に GCM と GCD が追加され、Annex B は 2007 年 7 月 14 に変更され、単一レベル OS に対する PP が追加となり、Annex C は 2007 年 10 月 18 日に SP800-90 の RNG の部分が追加となり、Annex D は IG（運用ガイダンス）の更新により 2008 年 1 月 16 日に更新されている。

FIPS PUB 140-2 は、暗号モジュールのセキュアな設計及び実装のために、暗号モジュールが満たすべき 11 分野(暗号モジュールの仕様、暗号モジュールのポート及びインタフェース、役割・サービス・認証、有限状態モデル、物理的セキュリティ、動作環境、暗号鍵管理、電磁妨害/電磁両立性、自己テスト、設計保証、その他の攻撃への対処)のセキュリティ要求事項を規定しており、さらに、保護すべきデータの重要性と使用環境に応じて暗号モジュールを提供できるように、分野ごとに 4 段階のセキュリティレベル(セキュリティレベル 1～4)を規定している。

(2) DTR (Derived Test Requirements for FIPS PUB 140-2)

DTR は、暗号モジュールが FIPS PUB 140-2 で規定されたセキュリティ要求事項を満たしているかどうかを試験する際に、試験者が実施しなければならない試験手順及びベンダが提供しなければならない情報を規定したものである。

DTR は FIPS PUB 140-2 と同様に適宜改訂されており、2004 年 3 月 24 日の改訂版が 2008 年 3 月での最新版となっている。

DTR は、全 11 章から構成されており、各章は FIPS PUB 140-2 で規定された 11 分野に対応している。各章では、FIPS PUB 140-2 に対応するセキュリティ要求事項をア

サーション[19]として記述している。全てのアサーションはFIPS PUB 140-2から直接引用している。

各アサーションの次には、順に、ベンダが提供しなければならない情報[20]、試験者が実施しなければならない試験手順[21]を記述している。

(3) IG (Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program)

IG は、CMVP、特にDTRに関する、ベンダや試験機関等からの問合せに対して、NIST及びCSEが回答したコメントをCMVPに関するガイダンスとしてまとめたものである。

IG もFIPS PUB 140-2及びDTRと同様に適宜改訂されており、2008年2月7日の改訂版[22]が2008年3月時点での最新版となっている。

IG は、全17節(OVERVIEW, GENERAL ISSUES, SECTION 1からSECTION 14, EXPIRED IMPLEMENTAITON GUIDANCE)から構成される。

“SECTION 1 からSECTION 14”は、次の表2.1のようにFIPS PUB 140-2 の各節とそれぞれ対応しており、セキュリティ要件の分野ごとに整理され、記述されている。また、複数の分野に当てはまる内容については、最適な分野のSECTIONに記述されている。

表2.1　IGとFIPS 140-2の節の対応

Implementation Guidance	FIPS PUB 140-2
SECTION 1 ～ SECTION 11	4.1 ～ 4.11
SECTION 12	APPENDIX A
SECTION 13	APPENDIX B
SECTION 14	APPENDIX C

“OVERVIEW”には“Implementation Guidance”の概要が記述されており、“GENERAL ISSUES”には、SECTION 1 から SECTION 14 の分野に特定されない全般的な問題が整理され、記述されている。また、取消された運用ガイダンスを記述するために、“EXPIRED IMPLEMENTAITON GUIDANCE”の節が用意されているが、現在、何も記述されていない。

(4) FIPS PUB 140-2のFIPS PUB 140-3への改訂

近年の暗号モジュールの実装や攻撃法に関する進歩は目覚しく、2001 年に発効し

---

19 Assertion (AS と略す)。暗号モジュールが、設定された分野のセキュリティ要件を、設定されたセキュリティレベルで満足するために適用しなければならない宣言。

20 Vender Evidence (VE と略す)

21 Tester Evidence (TE と略す)

22 日本語版は2008年1月24日の改訂版が2008年3月時点での最新版となっている。

たFIPS PUB 140-2は現状に合わなくなってきている。そこで、NISTは5年見直しとして、2006年を目処とした後継のFIPS PUB 140-3への移行準備を進めてきた。その一環として、2004年9月にメリーランド州でCMVP 2004シンポジウム[23]、2005年9月に物理セキュリティ試験のワークショップ[24]が開かれ、FIPS PUB 140-3に関する議論が行われるとともに、移行計画が発表されてきた。

2006年12月17日～22日には、米国ワシントンDC近郊のメリーランド州 ゲイザースバーグでNISTの情報セキュリティ関連部門CSD[25]とIPAセキュリティセンターの定期会議が開催され、５つの主要議題のテーマの一つとして暗号モジュール試験及び認証制度が取り上げられた。

・2006年のNIST-IPA定期会議でのFIPS PUB 140-3のアナウンスの概要

2006年の定期会議において、FIPS PUB 140-2の後継規格であるFIPS PUB 140-3についての次のようなアナウンスがあった。

・セキュリレベルは5レベルとなる（FIPS PUB 140-2は4レベルであり、2004年9月のCMVP 2004では6レベルとすることが示唆されていた)。

・11章からなる。EMI[26]に関する章は無くなった。FSM[27]はデザインアシュアランス（設計保証）の章に入れた。

・新しい章（分野）は2つ増えた。ひとつは、ソフトウエアセキュリティ、あとのひとつはnon-invasive attack [28]（非破壊攻撃)。

・ソフトウエアセキュリティの中にはハードウェア、ソフトウェア、ハイブリッドの3タイプのモジュールがある。ハイブリッドモジュールはImplementation Guidance 1.9に定義されている。

・非破壊攻撃は、FIPS PUB 140-2では、4章11節のMitigation of Other Attacksで記述していた。FIPS PUB 140-3では、独立させるとともに、セキュリレベル3から5までのレベルで要求する。但し、要求内容はFIPS PUB 140-2レベルであり、DTRで更に詳細に記述する予定である。

・2007年7月13日にFIPS 140-3の1st Draftが開示された。

・FIPS PUB 140-3への改訂スケジュールについて

FIPS PUB 140-3への改訂スケジュールは次のように公開された。

・2007年 3月31日　DraftをCMVP内部(NIST＋CSE)でレビューが完了。

・2007年 7月13日　1st Draftを開示。90日間のコメント募集期間を設

---

23 CMVP 2004 Symposium: http://csrc.nist.gov/cryptval/cmvp2004/

24 Physical Security Testing Workshop: http://csrc.nist.gov/cryptval/physec/physecdoc.html

25 Computer Security Division

26 EMI: Electro Magnetic Interference 電磁妨害

27 FSM: 有限状態モデル（Finite State Model)。暗号モジュールの動作を、有限状態モデルとして記述する。

28 非破壊攻撃：暗号モジュールに対して、物理的な侵入（カバーへ穴を開ける等の物理的手段を伴う侵入）を伴わない解析技術。代表的なものとしては、電力解析攻撃、故障誘導攻撃などがある。

ける。

・2007 年 10 月 12 日　1st Draft に対するコメント募集の〆切。

・2008 年 3 月 18 日　FIPS PUB 140-3 Software Security Workshop を開催。

・2008 年 第 2 四半期　2nd Draft のためのパブリックコメントの募集を開始（変更の可能性有り）。

・2008 年 第 4 四半期　米国商務省による承認（変更の可能性有り）。

・2008 年 その後 6 ヶ月　DTR が発行される。FIPS PUB 140-3 の試験の受け入れ開始。140-2 も試験の受け入れは継続される。

・2008 年 その後 6 ヶ月　FIPS PIUB 140-2 の試験の受け入れを終了。

・2007 年 11 月の NIST-IPA 定期会議において NIST CMVP より下記についての協力が提案された。但し実行については今後マネージメントの承認を得る必要がある。

・FIPS PUB 140-3 ドラフトのレビュー

・FIPS PUB 140-3 DTR の作成およびレビュー

・FIPS PUB 140-3 非破壊攻撃試験基準の確立

・FIPS PUB 140-3 非破壊攻撃試験手法の開発、試験機関の教育

・試験機関認定用模擬モジュールの共同開発

・暗号アルゴリズム試験ツールの共同デバッグ

2.1.2　ISO/IEC における暗号モジュールセキュリティ要件関連の調査

(1) ISO/IEC JTC 1/SC 27/WG 3

ISO/IEC JTC 1 は、ISO と IEC が共同で運営する IT 技術標準化のための技術委員会で、その下の SC 27 委員会が情報セキュリティを担当している。その下の WG 3 で情報セキュリティに関する評価基準などが扱われている。

(2) ISO/IEC 19790 (Security requirements for cryptographic modules)

ISO/IEC JTC 1/SC 27/WG 3 は、米国とカナダの提案に従い、2002 年 10 月から暗号モジュールセキュリティ要件の国際規格化を審議し、規格予定番号 19790 が割り当てられた。2005 年 10 月のマレーシア会合において FCD 案に対する編集作業が行われ、国際事務局による編集作業の後、2005 年 12 月には FDIS 投票が実施され、賛成多数で 2006 年 3 月 1 月に ISO/IEC 19790 として正式に発行された。

ISO/IEC 19790 は、FIPS PUB 140-2 をベースとした基準であり、当初 CC(Common Criteria)との関係を意識して記述様式を変更することが検討された。しかし、審議の進行に伴ってCCに対する配慮は薄れ､その点に関する影響はほとんどなくなった。なお、暗号技術に関し、FIPS PUB 140-2 では秘密鍵も公開鍵も CSP として区別しなかったのを秘密鍵は CSP、公開鍵は PSP と２種類に分解するなど、技術的な記述の精緻化が図られた。

(3) ISO/IEC 24759 (Test requirements for cryptographic modules)

2005 年 4 月のウィーン会合において、暗号モジュールセキュリティ要件の国際規格 ISO/IEC 19790 に付随して実際の試験に必要となる、暗号モジュール試験要件の規格化のプロジェクトが承認され、予定規格番号 24759 が割り当てられた。2006 年 5 月のスペイン会合で WD、2006 年 11 月の南アフリカ会合で 1st CD に関する審議が行われ、2007 年 5 月のロシア会合において FCD に進み、その後 FCD 投票が行われ、2008 年 3 月現在では FDIS が公開されている。

ISO/IEC 24759 の章立てや 4 つのセキュリティレベルは FIPS PUB 140-2 の DTR と基本的に同じである。ただし、FIPS PUB 140-2 から ISO/IEC 19790 が作成された際の修正の整合性を保ちつつ反映させる必要がある。

2.2 セキュリティ要件／試験要件標準化等に対する提案活動

今年度、暗号モジュール委員会では、暗号モジュールセキュリティ要件に関する海外動向に対応すべく、次の作業を行った。

2.2.1 ISO/IEC 24759 へのコメント提案

ISO/IEC JTC 1/SC 27 において、セキュリティ要件の国際規格 ISO/IEC 19790 に対応した試験要件の規格 ISO/IEC 24795 が作成中であり、第 2 回暗号モジュール委員会にて FDIS のドキュメントに対するコメントを作成し、8 月 27 日開催の SC 27 の国内委員会に委員経由で提出した。

コメントの内容としては、FDIS のドキュメントということでエディトリアルな記述のミスや参照先の誤った記述に関する修正を指摘する部分が多かったが、6.8.1 章の AS07.08 の Random bit generators において RBG (Random bit generators) とその動作モードについて、AS07.10、VB07.08.01、TE07.08.01、TE07.08.02 で「ISO/IEC 18031 準拠」するということになっており、正しく記述がされていないため、この部分は「承認されたものを使用する」に変更を依頼した。また、FDIS が 12 月に開示されたため、2 月の第 4 回暗号モジュール委員会では、3 月の ISO 国内委員会での FDIS 投票の検討のためのコメントが有る場合 3 月 3 日迄に事務局に連絡するように委員に依頼したが、特にコメントは無かった。

2.2.2 FIPS PUB 140-3 の 1st Draft に対するコメント作成

当初、FIPS PUB 140-3 の 1st Draft は 2006 年 11 月末にコメント募集のために公開される予定であったが、2007 年 7 月に公開となったため、暗号モジュール委員会と INSTAC 耐タンパー性標準化調査委員会 WG1 では 9 月 28 日に第 3 回暗号モジュール委員会を合同で開催し、1st Draft についての討議を行い、コメント案を作成し、10 月 11 日に NIST に提出した。(付録 1 FIPS PUB 140-3 の 1stDraft に対するコメント参照)

コメントの要点は各セキュリティレベルにおける要求事項として 4.6 章および 4.7 章で

示されている要件の記述が、そのままでセキュリティ上問題ないかどうかについてであり、検討結果として、セキュリティレベルによる要件の変更を提案した。

・レベル 3 では DPA[29]と SMEA[30]を追加

・レベル 4 では DPA と SMEA、DMEA[31]更に FI[32]を追加

・レベル 5 では FI を追加。

またレベル 3 と 4 では主要な攻撃に耐性を持つこととし、レベル 5 では一通りの攻撃に対して更なる耐性を持つ必要があることとするよう依頼した。

2.2.3 FIPS PUB 140-2 と 暗号モジュール試験及び認証制度のための運用ガイダンスの日本語の改訂版の作成

NIST 発行の“Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program”(IG) は逐次改訂版の発行が行われている。それに対応し暗号モジュール委員会では、日本語の翻訳版の作成作業を行っており、7 月 3 日版に今年度最初の翻訳版を作成し、更に 2008 年 1 月 24 日版を「FIPS PUB 140-2 と 暗号モジュール試験及び認証制度のための運用ガイダンス」として、最新の翻訳版を作成した。3 月現在 NIST からは 2008 年 2 月 8 日版が最新版として発行されている。

2.3 2007 年度電力解析実験ワーキンググループの活動

2.3.1 活動計画

電力解析実験ワーキンググループ(WG)の主要な活動目的は、電力解析攻撃等のサイドチャネル攻撃に対して暗号モジュールを防御する技術を確立すること、また暗号モジュール製品試験の為のセキュリティ要件・試験技術の開発にある。そこで、電力解析を中心とするサイドチャネル攻撃の攻撃方法及び対策方法に関する調査・検討を行い、セキュリティ要件・試験要件を開発するとともに、その国際標準化活動に対して貢献して行くものとする。具体的には INSTAC-8/-32 仕様準拠ボードを利用した実験の計画の策定・実行を行う。2006 年度開催の WG では、実験の実行のために解決すべき課題として次のものが指摘された。

1．実験結果の比較のため、共通化された実験環境や実験方法が必要である。

2．INSTAC-32 仕様準拠ボード間に消費電力等、ハードウェアのばらつきがある。

3．実験データは実験環境やノイズの影響が大きい。

4．企業からは実験に関するノウハウや生データの公開が容易でない。

5．実験結果からセキュリティ要件・試験要件を導き出す方法論がまだ明らかでない。

---

[29] DPA：(Differential Power Analysis)　差分電力解析。

[30] SEMA：(Simple Electro Magnetic Analysis)　単純電磁波解析。

[31] DEMA：(Differential Electro Magnetic Analysis)　差分電磁波解析。

[32] FIA：(Fault Induction Analysis)　故障利用解析。

課題１～３に対応するために実験の環境や方法の共通化は不可欠であるが、課題４のように企業からの情報提供には制約がある。そこで、公的研究機関や大学等、詳細な情報提供に支障の少ない組織が主体となって、実験の共通化に必要な情報を公開してゆく方針になった。また、課題５の方法論は今後、この WG で検討してゆく必要がある。このような状況を踏まえ、次のように 2007 年度の計画を設定し、年４回開催することとした。

・2007 年度上期

実験環境・実験方法の共通化についての検討

１．実験方法の共通化

２．電源のノイズに対する対策

３．実験で得られたデータの解析方法の共通化

・2007 年度下期

上期に共通化した実験方法等の有効性を確認する。

・2007 年度通年

INSTAC-32 仕様準拠ボードの個体差の比較測定も並行して実施する。

2.3.2　委員構成

電力解析実験ワーキンググループ　(2008 年 3 月現在)

委員長	松本　勉	国立大学法人横浜国立大学 大学院　教授
委員	太田　和夫	国立大学法人電気通信大学　教授
委員	栃窪　孝也	日本大学　専任講師
委員	山村　明弘	独立行政法人情報通信研究機構　グループリーダ
委員	黒川　恭一	防衛大学校　教授
委員	後藤　敏	早稲田大学　大学院　教授
委員	古屋　聡一	株式会社日立製作所　研究員
委員	井上　弘士	国立大学法人九州大学　大学院　准教授
委員	角尾　幸保	日本電気株式会社　主席研究員
委員	高橋　芳夫	株式会社 NTT データ　シニアエキスパート
委員	佐藤　証	独立行政法人産業技術総合研究所　主任研究員
委員	佐藤　恒夫	三菱電機株式会社　チームリーダー
委員	森岡　澄夫	日本電気株式会社　主任研究員
委員	山越　公洋	日本電信電話株式会社　研究主任
委員	深澤　宏	NEC マイクロシステム株式会社　主任
委員	鳥居　直哉	株式会社富士通研究所　部長
委員	藤崎　浩一	株式会社東芝　研究主務
委員	本間　尚文	国立大学法人東北大学　大学院　助教
委員	今福　健太郎	独立行政法人産業技術総合研究所　研究チーム長

2.3.3 横浜国立大学によるサイドチャネル攻撃実験用標準評価ボードの検査

産業総合技術研究所 情報セキュリティ研究センター（RCIS）と東北大学大学院 情報科学研究科による、暗号モジュールへのサイドチャネル攻撃実験を目的として新たに開発したサイドチャネル攻撃実験用標準評価ボード（SASEBO : Side-Channel Attack Standard Evaluation Board）をワーキンググループ委員等に配布することを前提として、東北大学大学院 情報科学研究科にて作成された暗号アルゴリズムを搭載し作成したボード80セット全数について、横浜国立大学にて動作特性の差異に関する実験調査を行い、その結果の報告が行われた。

実験用標準評価ボードに個体差が有り、ある実験結果が他のボードでは再現されないという状況が起きるのではないかという疑問が有った。そのため横浜国立大学において、今回作成された産業技術総合研究所開発のボードのうち、第1次配布予定の30枚について調査を行った結果､測定した電力波形には差異があり､大きく4グループに分類されるが、FPGAの特性による差異はほとんど存在せず、FPGAのVcc及びGNDに直列に挿入されているシャント用抵抗の交流特性の影響の方が大きい様であった。

ボードに搭載されているシャント用抵抗は交流特性によりAとBの2グループに分類でき、電力測定の結果にピークで数ミリボルトの差がある。また、Vcc側の抵抗とGND側の抵抗の組み合わせによるAA，AB，BA，BBの4パターンは、ボードの電力波形の4グループと対応する。各ボードに同一のシャント抵抗を載せて測定すると、ほぼ同一の電力波形が得られる。抵抗の交流特性の差異は抵抗のロットの違いによって発生したものと思われる。

ワーキンググループでは、ボードの個体差についてFPGAの影響は無く、シャント用抵抗のロットの個体差が影響していると結論付けた。

サセボ個体差調査・搭載シャント抵抗のリスト（横国大）　2007.9.20

各ボードに搭載されているシャント抵抗のグループ分け

を表 2.2 に示す

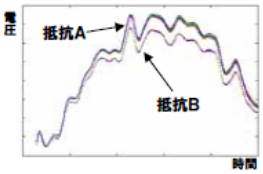

図 2.1　特性

表 2.2　シャント抵抗のグループ分け

	VCC	GND		VCC	GND		VCC	GND
G06	B	A	G16	B	A	G31	A	A
G07	B	A	G17	A	B	G32	A	B
G08	B	B	G18	A	A	G33	A	B
G09	A	B	G19	B	A	G34	A	B
G10	A	A	G20	B	A	G35	A	A
G11	A	A	G21	B	B	G36	A	B
G12	A	A	G22	B	B	G37	B	A
G13	A	A	G23	B	B	G38	A	A
G14	B	A	G24	A	A	G39	B	B
G15	A	B	G25	A	A	G40	A	A

2.3.4　サイドチャネル攻撃実験用標準評価ボードの配布

平成 19 年 9 月にサイドチャネル攻撃実験用標準評価ボード（SASEBO：Side-Channel Attack Standard Evaluation Board）とそれに用いる、暗号アルゴリズム（AES,Camellia,DES,Misty1）のソースコードを電力解析実験ワーキンググループの委員に配布した。

SASEBO は経済産業省の委託事業「暗号モジュールの実装攻撃の評価に関する調査研究」の中で産業技術総合研究所 情報セキュリティ研究センターと東北大学 大学院情報科学研究科が開発した。

また、SASEBO で用いる暗号アルゴリズムのソースコードは東北大学 大学院情報科学研究科と産業技術総合研究所 情報セキュリティ研究センターにより共同開発されたものである。

このボードは、FPGA を搭載し、各種暗号アルゴリズム及びサイドチャネル攻撃へのカウンターメジャー機能を有する暗号アルゴリズムの搭載を可能とし、暗号ハードウェアの消費電力や放射電磁波の高精度な測定を可能とするものである。

SASEBO プロジェクトの URL：　http://www.rcis.aist.go.jp/special/SASEBO/

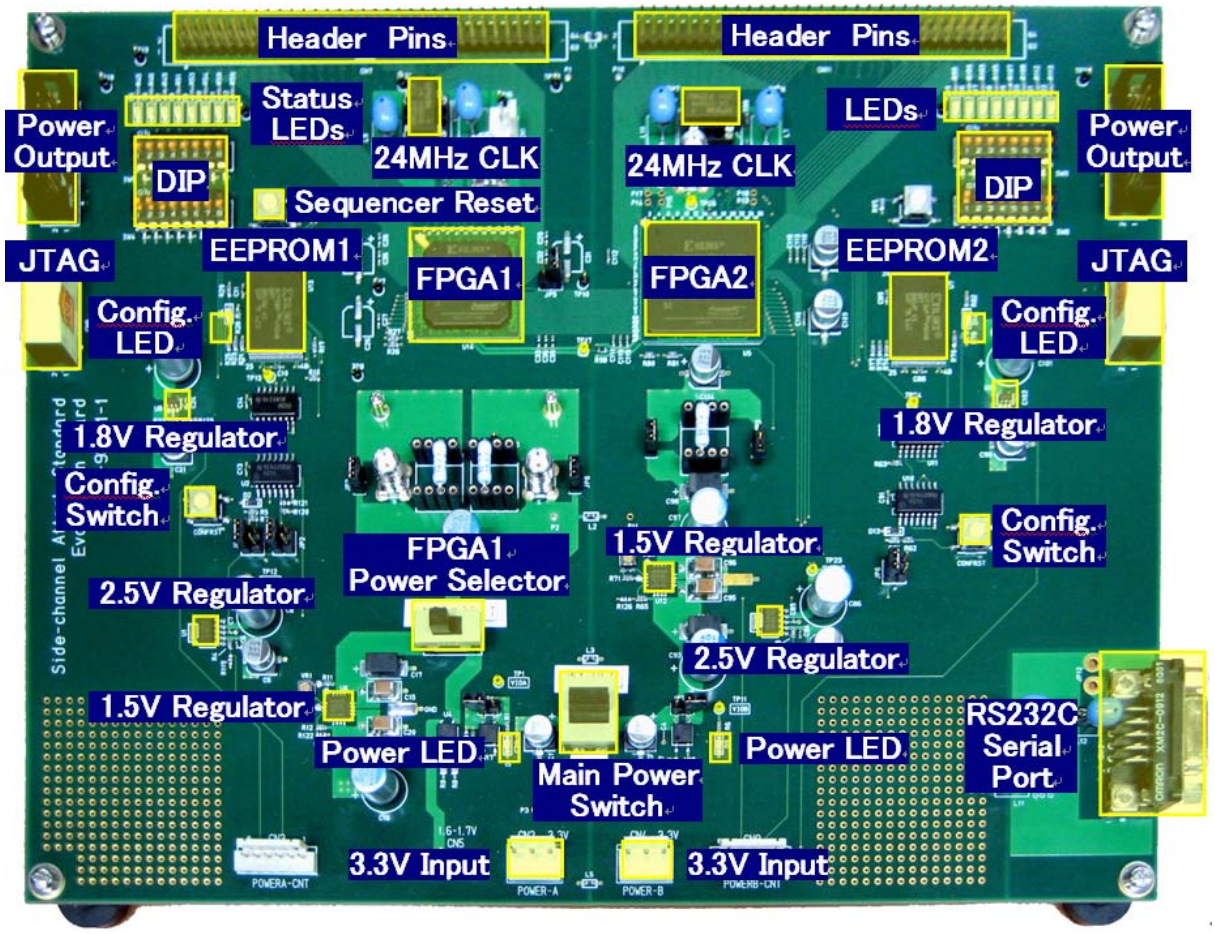

図 2.2　Side-channel Attack Standard Evaluation Board(SASEBO)の概要

2.3.5　電力解析攻撃研究会の開催

開催日時　2008 年 1 月 18 日（金）　10:00～12:00
開催場所　独立行政法人　情報処理推進機構　15 階委員会室１，２
講演者　Cryptography Research Inc. Paul Kocher 氏
講演題目　Part Ⅰ：Countermeasure Design & Validation Strategies for Power Analysis & related Attacks
Part Ⅱ：Complexity, Security, and the Future

暗号を安全に使用するために、サイドチャネル攻撃を考慮せざるを得なくなってきている。また、米国標準技術研究所（NIST）で改訂作業中の暗号モジュールに対するセキュリティ要件第三版（FIPS 140-3）でも、サイドチャネル攻撃に対する要件を盛り込む方向で検討が進んでいる。サイドチャネル攻撃の中でも電力解析攻撃は、痕跡を残さずに暗号モジュール内の鍵情報を入手できる可能性が高いため、十分な対策を施す必要がある。そこで、CRYPTREC 暗号モジュール委員会と電力解析実験ワーキンググループでは、電力

解析攻撃、タイミング攻撃を提案した米 Cryptography Research Inc.の Paul Kocher 氏を招いて、電力解析攻撃研究会を開催し、電力解析攻撃の現状を紹介するとともに、意見交換を実施した。

研究会の１部では、最初に Cryptography Research 社の沿革が紹介され、業務範囲について説明が行われた。

続いて、タンパーへの耐性について、電力解析攻撃が重要であることについて示された。更にその対策として安全な製品へのセキュリティのアプローチを説明し、DPA の評価方法としてブラックボックス試験、ホワイトボックス試験を示した。そして漏洩耐性のプロトコル例と共通鍵と公開鍵の種類について紹介し、漏洩率を分析し査定した。結論として DPA に対する試験が重要であり、ある製品については大変良い結果が出ているが、他のものは容易に攻撃されてしまうものも存在すると述べられた。また、スマートカードの暗号モジュールは最も高いレベルの安全性を有していると述べられた。

２部では複雑さと安全性について、有料 TV への攻撃、アカデミー賞委員の映画投票、電子商取引のクレジットカード、HD-DVD、ブルーレイ BD+の媒体形式 OS/アプリのセキュリティを例に挙げて示し、重要なトピックスについてレヴューを行った。DPA への耐タンパー性は漏洩への対策が重要でハードウェアとソフトウェアの暗号プロトコルについて対策を行う必要が有るとまとめた。

2.3.6　試験機関のための試験手順及び試験用機材の検討

暗号モジュールの試験機関において、各セキュリティレベルで要求されると思われる攻撃試験のための試験方法及び試験用機材について、米国 NIST による基準 FIPS 140-3(案)のセキュリティレベル１～５から、暗号モジュール委員会による案を基にして、検討を行った。

表 2.3　FIPS 140-3 のセキュリティレベルとそれに要求される攻撃試験

	タイミング解析攻撃	単純電力解析攻撃	差分電力解析攻撃
セキュリティレベル１，２			
セキュリティレベル３	セキュリティレベル３のタイミング解析攻撃に要求される試験機材と試験方法	セキュリティレベル３の単純電力解析攻撃に要求される試験機材と試験方法	
セキュリティレベル４（主要な攻撃への対策）	セキュリティレベル４のタイミング解析攻撃に要求される試験機材と試験方法	セキュリティレベル４の単純電力解析攻撃に要求される試験機材と試験方法	セキュリティレベル４の差分電力解析攻撃に要求される試験機材と試験方法

セキュリティレベル５（全ての攻撃への対策）	セキュリティレベル５のタイミング解析攻撃に要求される試験機材と試験方法	セキュリティレベル５の単純電力解析攻撃に要求される試験機材と試験方法	セキュリティレベル５の差分電力解析攻撃に要求される試験機材と試験方法

タイミング解析攻撃に関しては、セキュリティレベル１，２では要求されない。
単純電力解析攻撃に関しては、セキュリティレベル１，２では要求されない。
差分電力解析攻撃に関しては、セキュリティレベル１，２，３では要求されない。

セキュリティレベル１：

最低限のセキュリティレベルであり、製造グレードでの装備を超えた物理的なセキュリティ手段は必要とされない。

セキュリティレベル２：

レベル１の暗号モジュールの物理的セキュリティに加え、タンパリングの痕跡が残るコーティングやシール、こじあけ防止ロックなどが必要。

セキュリティレベル３：

暗号モジュール内の秘密情報への不正アクセスを防ぐため、カバーやドアなどの物理的セキュリティが必要。権限なくカバーやドアが開けられようとした場合、秘密情報をゼロ化する。

セキュリティレベル４：

暗号モジュールの周囲全体に保護用の遮蔽(envelope)が必要。レベル 3 はカバーやドアからの侵入を防ぐのに対し、レベル 4 はあらゆる方向からの侵入を検知し、秘密情報が盗まれる前にゼロ化する。また電圧や温度などの適正作動範囲からの変動を検知し、秘密情報をゼロ化する機構も要求される。

セキュリティレベル５：

下位のレベルの全ての要求事項に加え、更に以下のものが要求される。

ソフトウェアを含むモジュールはモジュールが使用中でないときには保有するすべての Sensitive Security Parameters （SSPs）と完全性のテスト・コードは暗号化と認証が要求される。 これは、モジュールが動作中でないときに、Critical Security Parameters（CSPs）と同様に Public Security Parameters(PSPs)の露呈と改竄を検出して、防御のために強い暗号による保護が要求される。

モジュールには、温度と電圧における変動からモジュールを保護する環境逸脱保護メカニズムが要求される。

モジュールは非視覚の放射試験を不明瞭にし、そしてタンパー検出とゼロ化回路は無力化に対する保護として要求される。ゼロ化が必要であるときに、CSPs と同様に PSPs はゼロ化が要求される。

CSPs は電磁放射攻撃からの保護が要求される。

モジュールの設計には、形式モデルと、形式モデルと機能的な仕様の間での一致の非公式な証拠での確認が要求される。

検討事項

米国 NIST FIPS 140-3（案） の１から５までの各セキュリティレベルを考慮して要求されるレベルにおける試験手順を検討する。

最終的には試験手順案をまとめるものとする。この中では電磁波解析（SEMA,DEMA）攻撃への対応も考慮する。

サイドチャネル攻撃への安全性試験環境の開発を行う予定である。

１．開発内容

網羅性を重視して TA,SPA,DPA,(EMC),(FI)とする。

解析方法を指定する。

標準試験環境の提示及び TA,SPA,DPA,(EMC),(FI)を指定する（安全性の試験として最低限実施すべき項目をまとめる)。

発注の内容としては、測定試験（検査）手順の改善方法も提案に含める。

２．開発のステップ

第一段階

プラットフォーム（環境を提示する）の基準をまとめる

- 機器　SASEBO-R(LSI版), SASEBO-B(ALTERA版), SASEBO-G(Counter Measure版)
- 解析対象　RSA, AES
- 解析手段、測定方法・測定点について要点を提案する。

第二段階

判定基準案をまとめる

第一段階、第二段階をまとめて米国 NIST に提示する。

2.3.7 電力解析攻撃実験のための評価ボードを利用した研究成果

電力解析実験ワーキンググループの委員による、INSTAC における耐タンパー性標準化調査研究委員会の活動成果であるサイドチャネル攻撃耐性評価用標準プラットフォーム仕様 INSTAC-8/-32 準拠プラットフォーム（INSTAC-8[33], INSTAC-32[34]）、産業技術総合研究所 情報セキュリティ研究センター（RCIS）と東北大学大学院 情報科学研究科による、暗号モジュールへのサイドチャネル攻撃実験を目的として新たに開発したサイドチャネル攻撃実験用標準評価ボード(SASEBO[35])等を使用した 2007 年度の発表についてまとめた。

表 2.4 評価ボードを使用した発表論文リスト

	タイトル	学会名・会議名	発表年月日	著者	使用ボード種類
1	DPA Using Phase-Based Waveform Matching against Random-Delay Countermeasure	ISCAS 2007[36]	2007/5/29	S. Nagashima, N. Homma, Y. Imai, T. Aoki, and A. Satoh	INSTAC-8
2	SPA Against an FPGA-Based RSA Implementation with a High-Radix Montgomery Multiplier	ISCAS 2007	2007/5/29	A. Miyamoto, N. Homma, T. Aoki, and A. Satoh	INSTAC-8
3	波形フィルタリングによる暗号モジュールへの高精度電力解析	DICOMO2007[37]	2007/7/6	長嶋 聖、本間尚文、菅原 健、青木孝文(東北大学 大学院情報科学研究科)、佐藤 証（産業技術総合研究所）	INSTAC-8
4	特定入力パターンを用いたRSA暗号ハードウェアの単純電力解析	DICOMO2007	2007/7/6	宮本篤志、本間尚文、青木孝文(東北大学 大学院情報科学研究科)、佐藤 証（産業技術総合研究所）	INSTAC-8
5	サイドチャネル攻撃標準評価 FPGA ボードを用いた暗号ハードウェアに対する電力解析実験	DICOMO2007	2007/7/6	菅原 健、本間尚文、青木孝文(東北大学 大学院情報科学研究科)、佐藤証（産業技術総合研究所）	INSTAC-32 SASEBO
6	ハードウェア実装されたXOR演算部に対するDPA手法	FIT2007[38]	2007/9/7	辻 洋平、岩井啓輔、黒川恭一（防衛大学校）	INSTAC-32
7	電力解析攻撃実験用ボードの個体差評価について	CSS2007[39]	2007/10/31	高橋芳夫(横浜国立大学、(株)NTTデータ)、 鳥越 慎、石和田大気、渡部良太、松本 勉(横浜国立大学)	SASEBO
8.	RSA暗号に対する平文選択型SPAの実験的評価	CSS2007	2007/11/2	宮本篤志、本間尚文、青木孝文（東北大学 大学院情報科学研究科)、佐藤 証（産業技術総合研究所）	SASEBO
9	AES のテーブルネットワーク型 FPGA 実装における耐電力解析テーブル設計法	ISEC[40]	2007/12/19	鳥越 慎、高橋芳夫、松本 勉（横浜国立大学）	SCAPE[41]ドータボードA
10	ハードウェア実装された AES 暗号の	ISEC	2007/12/19	辻 洋平、岩井啓輔、黒川恭一（防	SASEBO

[33] INSTAC-8：サイドチャネル攻撃耐性評価用標準プラットフォーム仕様INSTAC-8/32 準拠プラットフォーム（8bit版）

[34] INSTAC-32：サイドチャネル攻撃耐性評価用標準プラットフォーム仕様 INSTAC-8/32 準拠プラットフォーム（32bit版）

[35] SASEBO: サイドチャネル攻撃実験用標準評価ボード

[36] ISCAS: International Symposium on Circuits and Systems（The Institute of Electrical and Electronics Engineers, Inc.）

[37] DICOMO：マルチメディア，分散，協調とモバイルシンポジウム（情報処理学会）

[38] FIT：情報科学技術フォーラム（情報処理学会，電子情報通信学会）

[39] CSS：コンピュータセキュリティシンポジウム（情報処理学会）

[40] ISEC：情報セキュリティ研究会（電子情報通信学会）

[41] SCAPE：三菱電機が開発したサイドチャネルアタック評価用プラットフォーム(SCAPE: Side Channel Attack Platform for Evaluation)

	XOR 演算部に対する DPA 検証			衛大学校)	
11	RSA 暗号に対する平文選択型電力解析攻撃の検討	SCIS2008[42]	2008/1/22	本間尚文、宮本篤志, 青木孝文 (東北大学 大学院情報科学研究科)、佐藤 証 (産業技術総合研究所)	SASEBO
12	INSTAC-32 準拠ボードにおける CPU に対する電力解析／電磁波解析比較	SCIS2008	2008/1/22	庄司陽彦、野澤 晃、木村隆幸 (株式会社 ワイ・デー・ケー)、久門 亨、山下哲孝、角尾幸保 (日本電気株式会社)	INSTAC-32
13	サイドチャネル攻撃標準評価ボードを用いた電力および電磁波解析実験	SCIS2008	2008/1/22	福永利徳、高橋順子 (NTT 情報流通プラットフォーム研究所)、山越公洋 (NTT マイクロシステムインテグレーション研究所)、瀬賀研二 (長岡技術科学大学)	SASEBO
14	高分解能プローブの試作による電磁界解析実験	SCIS2008	2008/1/22	三宅秀享、藤崎浩一、清水秀夫、新保 淳 (株式会社東芝 研究開発センター)	SASEBO
15	FPGA に対する電磁界解析実験	SCIS2008	2008/1/22	藤崎浩一、三宅秀享、清水秀夫 (東芝 研究開発センター)	SASEBO INSTAC-32 S3E[43]
16	テーブルネットワーク型 AES 実装の新手法の提案	SCIS2008	2008/1/23	山口晃由 (三菱電機株式会社 情報技術総合研究所)、品川宗介 (三菱電機エンジニアリング株式会社 鎌倉事業所)、佐藤恒夫 (三菱電機株式会社 情報技術総合研究所)	INSTAC-8
17	RSL 技術を用いた耐 DPA 暗号 LSI の設計手法−スタンダードセルによる RSL の実現と AES 回路への適用−	SCIS2008	2008/1/23	鈴木大輔、佐伯 稔 (三菱電機株式会社 情報技術総合研究所)、佐藤 証 (産業技術総合研究所)	SASEBO
18	RSL 技術を用いた耐 DPA 暗号 LSI の設計手法 −設計段階における事前 DPA 評価−	SCIS2008	2008/1/23	佐伯 稔、鈴木大輔 (三菱電機株式会社 情報技術総合研究所)、佐藤 証 (産業技術総合研究所)	SASEBO
19	バンドパスフィルタを用いた高精度な差分サイドチャネル解析	ISEC	2008/2/29	久門 亨、山下哲孝、洲崎智保、角尾幸保 (日本電気株式会社)、庄司陽彦、野澤 晃、木村隆幸 (株式会社 ワイ・デー・ケー)	INSTAC-32
20	暗号モジュールへの信号ラインからのサイドチャネル攻撃 ～ FPGA 実装 AES における実験例 ～	ISEC	2008/2/29	渡部良太、鳥越 慎、高橋芳夫、松本 勉 (横浜国立大学)	SASEBO
21	サイドチャネル攻撃標準評価ボード (SASEBO)を使った AES 暗号の実装評価実験	情報処理学会第 70 回全国大会	2008/3/15	南崎大作,岩井啓輔,黒川恭一 (防衛大学校)	SASEBO

ISCAS 2007 (2007 年 5 月 29 日)

1272 DPA Using Phase-Based Waveform Matching against Random-Delay Countermeasure

S. Nagashima, N. Homma, Y. Imai, T. Aoki, and A. Satoh

著者は位相を基にした波形一致技術による差分電力解析(DPA)を提案した。通常、トリガー信号とシステムクロックは波形の捕捉に用いられるが、信号は常にジッタに関連した逸脱を含んでおり、そして、これは統計分析の精度を低下させる。この方法はこのタイミングの逸脱に、測定波形の上の後処理まで標本抽出率より高い解像度で適応することができた。したがって、測定設備を変更する必要は全くなかった。また、それらの方法はランダム遅延また

[42] SCIS : 暗号と情報セキュリティシンポジウム (電子情報通信学会)

[43] S3E : Spartan 3E starter kit

はダミーサイクルによる歪の波形を作成する DPA 対策を破れる可能性がある。彼らは、Z80 マイクロプロセッサの上に､その対策の有無のデータ暗号化規格(DES)ソフトウェアを搭載し、従来の攻撃と比較し、著者の方法の利点を示した。

ISCAS 2007　(2007 年 5 月 29 日)

1825　SPA Against an FPGA-Based RSA Implementation with a High-Radix Montgomery Multiplier

A. Miyamoto, N. Homma, T. Aoki, and A. Satoh

単純電力解析(SPA)は FPGA プラットホームの高基数モンゴメリ乗数を用いた RSA プロセッサに適用され、そして、2 つのタイプの乗算器(内蔵の、そして、カスタムの)によって発生した電力波形の異なった特性が詳細に調査された。著者は、また、モジュラ乗算を制御するために入力データが特定のパターンに設定された能動攻撃を適用した。乗法のための電力消費は、秘密鍵の全ビットの復元の成功の結果について、モジュラ平方と比較して、大いに減少した。

DICOMO2007　(2007 年 7 月 6 日)

7D-3　波形フィルタリングによる暗号モジュールへの高精度電力解析

長嶋 聖、本間尚文、菅原 健、青木孝文(東北大学 大学院情報科学研究科)、佐藤 証（産業技術総合研究所）

ここでは、波形フィルタリングによる電力解析攻撃の高精度化について述べ、その有効性を検証した。一般に暗号モジュールの消費電力は、暗号化以外の演算や電源ノイズの影響を受け、それらは統計処理による解析において精度低下の大きな要因の一つとなる。提案手法は、電力波形の周波数帯域から秘密情報の解析に有効な部分を動的に選択し、処理の精度を向上させようというものである．INSTAC-8 準拠プラットフォームの Z80 プロセッサ上に実装した DES のソフトウェアを用いた実験において本手法を適用した結果、取得波形が少ない場合でも高い精度での統計解析が可能であることが示された。

DICOMO2007　(2007 年 7 月 6 日)

7D-4　特定入力パターンを用いた RSA 暗号ハードウェアの単純電力解析

宮本篤志、本間尚文、青木孝文(東北大学 大学院情報科学研究科)、佐藤 証（産業技術総合研究所）

ここでは、RSA 暗号ハードウェアに、特定のデータパターンを入力することで単純電力解析（SPA：Simple Power Analysis）の性能を向上させる手法を提案した。RSA 暗号の SPA は、秘密鍵のビットパターンに応じて 繰り返される乗剰余算と自乗剰余算の違いを消費電力波形から見分けるものである。しかし、乗剰余算と自乗剰余算を同一の演算器・演算手順 で処理するハードウェア実装では､ランダムな入力からその消費電力差 を見分けることは極めて困難である。それに対して本手法は、乗剰余算の 2 変数の一方が入力データに直接関係して

いることを利用し、特定のデータパターンを与えることで乗剰余算と自乗剰余算の消費電力の違いを強調するものである。ここでは、2 種類の乗算器と 2 種類の演算シーケンスを組み合わせ、計 4 種類の RSA 暗号ハードウェアを FPGA 上に実装し、それらを用いた SPA 実験により、提案の有効性を検証した。

DICOMO2007　（2007 年 7 月 6 日）

7D-5　サイドチャネル攻撃標準評価 FPGA ボードを用いた暗号ハードウェアに対する電力解析実験

菅原 健、本間尚文、青木孝文(東北大学 大学院情報科学研究科)、佐藤 証（産業技術総合研究所）

ここでは、暗号モジュールへのサイドチャネル攻撃実験を目的として開発したサイドチャネル攻撃標準評価 FPGA ボード（SASEBO： Side-Channel Attack Standard Evaluation Board）を紹介した。このボードは、暗号ハードウェアの消費電力や放射電磁波の高精度な測定を可能とする。SASEBO の仕様およびアーキテクチャを説明するとともに、共通鍵暗号 AES（Advanced Encryption Standard）への電力解析攻撃実験により、INSTAC-32 との比較を行った。

FIT2007　（2007 年 9 月 7 日）

ハードウェア実装された XOR 演算部に対する DPA 手法

辻 洋平、岩井啓輔、黒川恭一（防衛大学校）

暗号デバイスに対する攻撃手法として、暗号処理時間や消費電力等の情報を利用して秘密鍵を推定するサイドチャンネル攻撃が注目されている。電力差分解析はこのサイドチャネル攻撃の 1 つであり、消費電力情報を統計処理することで秘密鍵を推定する強力な攻撃方法である。ストリーム暗号の keysetup 時等の暗号デバイスに多く用いられている XOR 演算についても、DPA 手法が幾つか提案されている。しかしこれらの手法は、CPU 処理を前提としたターゲットに実装された XOR 演算に対する DPA 手法である。著者らは、ハードウェア実装された XOR 演算に適応することは難しいことを確認した。一方、ハードウェア実装された暗号デバイスに対しての現在までに提案されている DPA 手法は、信号遷移時における遷移確率に偏りを利用したものである。XOR 演算は線形演算であり遷移確率に偏りがないため、これまでの手法は適応できない。ここでは、CMOS 素子構造におけるスイッチング特性に着目した XOR 演算に対する DPA 手法を提案した。

CSS2007　（2007 年 10 月 31 日）

2D-3　電力解析攻撃実験用ボードの個体差評価について

高橋芳夫(横浜国立大学、株式会社 NTT データ)、

鳥越 慎、石和田大気、渡部良太、松本 勉(横浜国立大学)

サイドチャネル攻撃、特に電力解析攻撃の研究促進のために開発された電力解析攻撃の実

験用ボードについて、個体差調査のために, 延べ472, 452個の電力波形を測定した。その結果、ボード自体には実験結果に大きく影響しそうな個体差は見当たらず、どのボードでも同様な実験が可能と考えられた。ただし、電力波形測定に用いるシャント用抵抗については、抵抗値が許容誤差範囲内であっても周波数特性に偏りがある抵抗もあり、周波数特性の違いは電力波形に影響を与えるため、実験内容によっては抵抗器の選択に注意が必要であることが分った。ここではこれらの個体差調査結果を紹介し、測定データを使った実験例としていくつかの攻撃結果を示した。

CSS2007　（2007年11月2日）
9B-2　RSA暗号に対する平文選択型SPAの実験的評価
宮本篤志、本間尚文、青木孝文（東北大学 大学院情報科学研究科）、佐藤 証（産業技術総合研究所）

これまで平文選択によりRSA 暗号のSPA を強化する手法がいくつか提案されている。特に、2005 年にYen らによって提案された平文選択型のSPA は、多様なアーキテクチャやアルゴリズムに適用可能であり、かつSPA 対策として挿入されるダミー乗算を無効化できるため、非常に強力な攻撃法となり得る。しかしながら、この手法に対する実験ベースの実証例はまだ報告されていない。ここでは、FPGA 上に実装したRSA 暗号へのSPA 実験により、Yen らの手法の有効性を検証した。

ISEC　（2007 年 12 月 19 日）
AES のテーブルネットワーク型 FPGA 実装における耐電力解析テーブル設計法
鳥越 慎、高橋芳夫、松本 勉（横浜国立大学）

暗号実装時に対処が必要な脅威である電力差分解析は、暗号処理時のデバイスの消費電力を測定し、統計処理を行うことで鍵を特定する攻撃法である。この論文では、鍵の導出を困難にするソフトウェア実装方式であるテーブルネットワーク型暗号実装を、電力差分解析への対策としてハードウェア実装に適用する際のテーブル設計指針について検討し、FPGA ボード実装 AES を用いて行った実験結果から、その電力差分解析耐性を示した。

ISEC　（2007 年 12 月 19 日）
ハードウェア実装された AES 暗号の XOR 演算部に対する DPA 検証
辻 洋平、岩井啓輔、黒川恭一（防衛大学校）

これまでのハードウェア実装された暗号回路に対する DPA 手法は、信号の遷移確率を利用したものであった。著者らは、 CMOS デバイスにおける上方遷移と下方遷移において、消費電力差があることを利用した DPA 手法を提案した。この論文では、 AES を FPGA 上に実装し、 その Add RoundKey の XOR 演算部に対する DPA 検証を行った結果、 128bit 型 AES 暗号の秘密鍵の一部を特定できたことを示した。

SCIS2008　（2008 年 1 月 22 日）

1A1-5　RSA 暗号に対する平文選択型電力解析攻撃の検討

本間尚文、宮本篤志、青木孝文（東北大学 大学院情報科学研究科）、佐藤 証（産業技術総合研究所）

べき乗剰余演算に対する平文選択型の電力解析攻撃を提案した。本手法は、べき乗剰余演中に異なるタイミングで発生する自乗算サイクルの波形パターンを用いて鍵情報を推定する。入力する平文ペアを適切に組み合わせることで、バイナリ法に加えて、従来の手法では不可能だった m-ary 法や Sliding Window 法を用いた実装にも適用可能となった。この論文では、RSA 暗号モジュールのハードウェアおよびソフトウェア実装を用いた実験により、提案手法が実装するプラットホームに依らず有効であることを示した。

SCIS2008　（2008 年 1 月 22 日）

1A2-1　INSTAC-32 準拠ボードにおける CPU に対する電力解析／電磁波解析比較

庄司陽彦、野澤 晃、木村隆幸（株式会社 ワイ・デー・ケー）、久門 亨、山下哲孝、角尾幸保（日本電気株式会社）

この論文では、サイドチャネル攻撃である「電力解析」と「電磁波解析」について、INSTAC-32 準拠ボード上の CPU で動作する暗号処理に対して実施した結果を報告した。

これまで、電磁波解析が電力解析より効率よく解析できるという研究結果がいくつか報告されている。著者らは既製のプローブと自作のプローブを使用して実験を行い、解析の成否に関するサイドチャネル情報の特性の違いについて考察した。

SCIS2008　（2008 年 1 月 22 日）

1A2-3　サイドチャネル攻撃標準評価ボードを用いた電力および電磁波解析実験

福永利徳、高橋順子（NTT 情報流通プラットフォーム研究所）、山越公洋（NTT マイクロシステムインテグレーション研究所）、瀬賀研二（長岡技術科学大学）

サイドチャネル攻撃標準評価ボード SASEBO に搭載した 128 ビットブロック暗号 AES に対して差分電力解析 DPA および差分電磁波解析 DEMA を行った。その結果、DPA および DEMA とも鍵の推定に成功し、SASEBO で電磁波解析の評価をすることが可能であることが実験的にわかった。鍵を推定するために必要な波形数は、DEMA の方が DPA より多く、動作周波数が高い方が低い方より多かった。

SCIS2008　（2008 年 1 月 22 日）

1A2-4　高分解能プローブの試作による電磁界解析実験

三宅秀享、藤崎浩一、清水秀夫、新保 淳（株式会社東芝 研究開発センター）

近年、サイドチャネル攻撃と呼ばれる正規の入出力以外に漏洩する情報を解析して秘密情報を導出する攻撃が現実的な脅威となっており、多くの解析手法と対策手法が提案されている。一般に、消費電力解析では解析対象全体からの漏洩情報しか入手できないのに対し、電

磁界解析では解析対象の一部からの漏洩情報が入手できるため、消費電力解析よりも強力な攻撃と成り得ると言われている。この論文では、自作した高空間分解能プローブと FPGA ボード(SASEBO) を使った電磁界解析結果を示し、空間分解能の低い市販プローブと比較してその有効性を検討した。

SCIS2008　(2008 年 1 月 22 日)
1A2-5　FPGA に対する電磁界解析実験
藤崎浩一、三宅 秀享、清水秀夫（株式会社東芝 研究開発センター）

非破壊型の実装攻撃の評価を目的として、サイドチャネル攻撃耐性評価用標準プラットフォーム仕様 INSTAC-32 や SASEBO が開発された。これらのプラットフォームを用いることで、実装攻撃手法を客観的に評価できる環境が整いつつある。SASEBO は、消費電力を高い精度で測定できるようにノイズ対策も考慮して設計されている。そこで、この SASEBO と INSTAC-32 準拠プラットフォームの FPGA ボードおよび市販されている FPGA ボードの放射電磁波を測定し、各ボード間の測定データを比較するとともに、差分電磁界解析(DEMA：Differential Power Analysis)を行った。この論文は、これらの実験結果について報告した。

SCIS2008　(2008 年 1 月 23 日)
2A1-1　テーブルネットワーク型 AES 実装の新手法の提案
山口晃由（三菱電機株式会社 情報技術総合研究所)、品川宗介（三菱電機エンジニアリング株式会社 鎌倉事業所)、佐藤恒夫（三菱電機株式会社 情報技術総合研究所)

差分電力解析が提案されて以来、その対策が急がれている。これに対し、ソフトウェアベースでの対策として、テーブルネットワークを用いる手法が提案されている。これは、設計者のみが知り得る全単射変換処理を組み込んだテーブルを用いて暗号処理を行うことで、暗号本来の中間変数と、実際に演算される中間変数との相関をなくし、差分電力解析を不可能にするものである。しかし、従来のテーブルネットワーク実装の場合、各拡大鍵に対応してテーブルを再構築する必要がある。そのため、大量のメモリを消費する。また、鍵を変更する度にテーブルを再構築しなければならず、そのための演算コストが必要となる。この論文では、各拡大鍵に応じたテーブルを必要としない手法を提案し、実験によりその有効性を検証した。

SCIS2008　(2008 年 1 月 23 日)
2A1-3　RSL 技術を用いた耐 DPA 暗号 LSI の設計手法
−スタンダードセルによる RSL の実現と AES 回路への適用−
鈴木大輔、佐伯 稔（三菱電機株式会社 情報技術総合研究所)、佐藤 証（産業技術総合研究所)

ここでは、CMOS スタンダードセルライブラリを用いたRSL の実装方式を提案し、その安全

性条件について議論した。提案方式はDPA によるリーク量を数ゲート分の回路から発生するリークに抑えることが可能であり、WDDL と比較して対策の適用による性能劣化は少なく、効率の良い対策方式である。著者らは現在、本稿で示すRSL を用いた暗号回路の設計フローに基き、スタンダードセルによるRSL を適用したプロトタイプLSI を開発している。ここでは、このLSI に搭載したAES 回路の構成と諸性能についても報告した。

SCIS2008　（2008 年 1 月 23 日）
2A1-4　RSL 技術を用いた耐 DPA 暗号 LSI の設計手法
−設計段階における事前 DPA 評価−
佐伯 稔、鈴木大輔（三菱電機株式会社 情報技術総合研究所)、佐藤 証（産業技術総合研究所）

著者らはトランジスタレベルにおける DPA 対策手法の 1 つである Random SwitchingLogic(RSL) を標準的な CMOS スタンダードセルで模擬し、AES 回路に適用した実験用 LSI を開発中である。この AES 回路は、LSI の設計情報に基づいた事前 DPA 評価により、高い DPA 耐性を有することを確認したものである。この論文では、LSI の設計段階における効率的な事前 DPA 評価手法について述べ、FPGA を用いた実験により、その手法の有効性を示した。さらに、上記 AES 回路の事前 DPA 評価結果について報告した。

ISEC　（2008 年 2 月 29 日）
バンドパスフィルタを用いた高精度な差分サイドチャネル解析
久門 亨、山下哲孝、洲崎智保、角尾幸保（日本電気株式会社)、庄司陽彦、野澤 晃、木村隆幸（株式会社 ワイ・デー・ケー）

ここでは、暗号モジュールに対する差分サイドチャネル解析において、測定波形に含まれるノイズをバンドパスフィルタにより除去することで、解析精度の改善が可能であることを示した。バンドパスフィルタの適用においては、通過帯域の設定がノイズ除去に大きな影響を与える。そこで，通過帯域の設定手法として、測定波形のパワースペクトルを利用した 2 種類の手法を提案した。また、電力と電磁波の 2 種類のサイドチャネル情報に対する評価実験により、提案手法の有効性を評価した。

ISEC　（2008 年 2 月 29 日）
暗号モジュールへの信号ラインからのサイドチャネル攻撃
～ FPGA 実装 AES における実験例 ～
渡部良太、鳥越 慎、高橋芳夫、松本 勉（横浜国立大学）

サイドチャネル攻撃の一つに、暗号処理中のハードウェアの消費電力を分析することにより暗号鍵などの秘密情報を暴露しようとする電力解析攻撃がある。消費電力の測定は通常、電源ラインで行うものであるが、電源ラインと電気的に接続されたラインならば、電源ラインでなくても消費電力と同様な情報を測定できる可能性がある。そのような消費電力の測定

ポイントとして信号ラインに注目し、FPGA に実装した AES を攻撃対象として、電源ラインによる電力解析攻撃と信号ラインを測定ポイントとした電力解析攻撃と同様な攻撃を試み、有効性を確認した。

情報処理学会第 70 回全国大会　（2008 年 3 月 15 日）
5ZB3　サイドチャネル攻撃標準評価ボード(SASEBO)を使った AES 暗号の実装攻撃実験
南崎大作、岩井啓輔、黒川恭一（防衛大学校）

情報関連産業や関連技術が顕著な成長を見せ、インターネットや携帯電話の普及に伴い、通信の安全な利用に対する要求が高まり、通信セキュリティに対する研究はその重要性を増している。

サイドチャネル攻撃に関する研究が盛んに行われている昨今、実験に関する統一評価手法の確立を目的として、標準評価プラットフォーム仕様 INSTAC-8 及び INSTAC-32 が策定され、それらの準拠ボードが開発された。

ここでは、それらの準拠ボードを用いた暗号モジュールへの攻撃実験から得られた知見を生かし、産業技術総合研究所及び東北大学が新たに開発したサイドチャネル攻撃標準評価ボード(SASEBO：Side-Channel Attack Standard Evaluation Board)に対して共通鍵ブロック暗号を実装し、サイドチャネル攻撃に関する検証を行った結果を示した。

第 3 章　開催状況

3.1　暗号モジュール委員会の開催状況

2007 年度の暗号モジュール委員会は、計 4 回開催された。各回会合の概要は表 3.1 のとおりである。

表 3.1　2007 年度暗号モジュール委員会の開催状況

回	開催日時	主な議題
第 1 回	平成 19 年 6 月 6 日 10:00～12:00	暗号モジュール委員会規程について 委員長互選 ISO/IEC SC27/WG3 のロシア会合報告 平成 19 年度暗号モジュール委員会活動計画（案）について ISO/IEC FDC 24759 の審議について CMVP 運用ガイダンス改定版の事務局による翻訳について
第 2 回	平成 19 年 7 月 25 日 14:00～16:00	ISO/IEC FDC 24759 の審議 NIST FIPS 140-3 のドラフトに関する審議 CMVP 運用ガイダンス改定版の審議について 第 1 回電力解析実験ワーキンググループの開催報告
第 3 回	平成 19 年 9 月 28 日 10:00～18:00	NIST FIPS 140-3 ドラフトのコメント審議 （INSTAC:耐タンパー委員会と合同で開催）
第 4 回	平成 20 年 2 月 15 日 10:00～12:00	ISO/IEC 24759 FDIS の報告 CMVP 運用ガイダンス改定版の事務局による翻訳版の報告 2007 年度電力解析実験ワーキンググループの活動報告 CRYPTREC Report 2007(案)について 2008 年度の活動(案)について

3.2　電力解析実験ワーキンググループの開催状況

2007 年度の電力解析実験ワーキンググループは、計 4 回開催された。各回会合の概要は表 3.2 のとおりである。

表 3.2　2007 年度電力解析実験ワーキンググループの開催状況

回	開催日時	主な議題
第 1 回	平成 19 年 6 月 27 日 14:00～16:00	電力解析実験ワーキンググループ活動計画(案) について 実験の目的と実験手順について 新たな標準評価ボードについて
第 2 回	平成 19 年 10 月 5 日 14:00～16:00	SASEBO ボードの配布と実験状況について 横浜国立大学による SASEBO ボードの個体差の確認実験結果の報告
第 3 回	平成 19 年 12 月 21 日 12:00～14:00	試験機関のための試験手順および試験機材の検討 SASEBO ボード等に関する実験の報告等
第 4 回	平成 20 年 2 月 6 日 14:00～16:00	2007 年度電力解析実験ワーキンググループの活動のまとめと報告書の作成について 電力解析攻撃実験のための評価ボードを用いたサイドチャネル攻撃の研究発表論文のまとめ 2008 年度の活動(案)について

付録

付録1　FIPS PUB 140-3 の 1st Draft に対するコメント

Comment List for Draft FIPS 140-3 "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES" by CRYPTREC and INSTAC

Date: 2007-10-11	Document: **Draft FIPS 140-3**

1	2	3	4	5
Clause No./ Subclause No./ Annex (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by CRYPTREC/INSTAC**	**Proposed change by CRYPTREC/INSTAC**
4.1.1 Types of Cryptographic Modules	2nd item in p.16	te	As an instance of a cryptographic module, there provides the software module constituted only by software in 4.1.1; however, the 4.1.2 describes that such processor implementing the software should also be included in that cryptographic boundary – this shows somewhat inconsistency.	Since software module is constituted by hardware, OSs and software, it leads misunderstanding unless describing cryptographic boundary is set within physical boundary by configuring the physical boundary. Add "define a physical boundary and define a code boundary in it." on the 4.1.2.
4.1.3 Multilevel Approved Modes of Operations	5th item in p.17	te	In the 5th paragraph, "If re-configuration from one Approved mode of operation to another alters the physical security level of the module without changing the overall security level of the cryptographic module, then the cryptographic module **shall** perform a zeroization of all CSPs within the module.": About 1) "the physical security level"; Does this mean the security level relevant to the requirements of Physical Security described in the 4.6 or the security level is also included/described in 4.7 or does this mean other than that. It needs to be clarified. (It refers the description of FIPS140-2IG.) About 2) The parameters needs to be zeroization, is the timing adequate to define when "the physical security level" is changed (It won't be a problem if "the overall security level" would not be changed?).	1) The definition of physical security level" should be added. Then the scope that the physical security level being indicated should be provided in that definition whether the security level is for 4.6 or the security level is both for 4.6 and 4.7. 2) Question is raised about the necessity of 5th "・" in the 4.1.3.
4.3.1 Roles	p.19	te	The description of Maintenance role which clearly stated in 140-2 is deleted.	It seems that the description is included in the Other roles column; however in the 4.6.1, there clearly described about Maintenance role to be used for maintenance service/access: it should not be deleted.
4.3.2 Operator Authentication	4th in the 3rd paragraph in p.20	te	In relation to the "password selection to prevent the use of weak passwords that are more susceptible to attacks":	It should specifically present the requirements to be fulfilled by the passwords.

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

Comment List for Draft FIPS 140-3 "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES" by CRYPTREC and INSTAC

Date: 2007-10-11	Document: **Draft FIPS 140-3**

1	2	3	4	5
Clause No./ Subclause No./ Annex (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by CRYPTREC/INSTAC**	**Proposed change by CRYPTREC/INSTAC**
4.3.3 Services	The 1st paragraph in p.20	te	In relation to the description of "The logic performing the external software loading shall be logically disconnected from all data output.", it is hard to comprehend its major points.	The scope of "loading logic" to be indicated should be clearly defined.
4.5 Operational Environment	p.24~27	te	As the trusted channel of Security Level 3, there required preventive measures against alteration, replacements, exposures and playbacks. Does the all parameters of "The Trusted Channel…parameter." have to be satisfied? The authentication function of "The Trusted Channel" can be altered by the function of "Operator Authentication Function" in the 4.3.2?	
4.6 Physical Security	The Chart 3 in p.28	te	What does the Radiation Fault Induction of Security Level 5 mean?	Since the 3rd "・" description of Security Level 5 in the 4.6.1 is somewhat blurry and is necessary to specifically be described. (The same review process is necessary in the description of the 4.7 as well.)
4.6.1 General Physical Security Requirement	The 3rd "・" in P29	te	About the Maintenance Role:	It is necessary to maintain consistency.
4.6.2 Single-Chip Cryptographic Modules	p.31	te	It seems that the Security Level 4 and 5 should be collectively presented.	As with the FIPS140-2: In case there is such level which does not have additional requirements, it should be described "There are no additional requirements (for xxx) at Security Level X." only when Low Level which consecutively follows from LV1 unless otherwise the concerned level should be described together with the additional requirements of the sub-levels.

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

Comment List for Draft FIPS 140-3 "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES" by CRYPTREC and INSTAC

Date: 2007-10-11	Document: **Draft FIPS 140-3**

1	2	3	4	5
Clause No./ Subclause No./ Annex (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by CRYPTREC/INSTAC**	**Proposed change by CRYPTREC/INSTAC**
4.6.5 Environmental Failure Protection/Testing	p.34	te	"EFP/EFT" in section 4.6.5 takes into account of temperature and voltage only. It is, however, well known that for a cryptographic module with external clock supply, there are attacks to manipulate clock signal from the normal operating range, e.g. to provide much faster clock signal for a short period of time, to cause faulty operation resulting in derivation of some secret parameters. Smart card is a typical cryptographic module with external clock supply.	It should be required that cryptographic module shall detect or respond appropriately if a clock signal falls out of the normal range of operation. (It seems that the relevant description is 4.6.5; it should be added that "there is no description about the malfunction in conjunction with the instantaneous environmental anomaly" either in the current description of 4.6.5 or in the Other Attacks column of 4.11.)

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

Comment List for Draft FIPS 140-3 "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES" by CRYPTREC and INSTAC

Date: 2007-10-11	Document: **Draft FIPS 140-3**

1	2	3	4	5
Clause No./ Subclause No./ Annex (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by CRYPTREC/INSTAC**	**Proposed change by CRYPTREC/INSTAC**
4.7 Physical Security-Non-Invasive Attacks	P35	Te	Description of side channel security requirement in section 4.7 is based on attack method, i.e. the requirement refers to the names of attack methods to be considered. Description method for side channel security requirement is classified into three types as (1) attack-based, (2) countermeasure-based, and (3) metric-based. Since we think the metric-based description is an ideal approach, it is preferable that forthcoming documents such as DTR should describe the requirements in the metric-based manner when well-established metrics are ready.	

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

Comment List for Draft FIPS 140-3 "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES" by CRYPTREC and INSTAC

Date: 2007-10-11	Document: **Draft FIPS 140-3**

1	2	3	4	5
Clause No./ Subclause No./ Annex (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by CRYPTREC/INSTAC**	**Proposed change by CRYPTREC/INSTAC**
4.7 Physical Security-Non-Invasive Attacks	P35	Te	**Levels and attacks.** The followings are the mapping of side channel attacks to each of five Security Levels in the draft FIPS140-3: Level 1 and 2: no requirement Level 3: Timing Analysis Level 4: SPA and DPA Level 5: EME. On the other hand, Level 1 is to achieve the lowest security and Level 5 is the highest. Therefore, the mapping above seems to assume the strength of side channel attacks increases in the following order: Timing Analysis, SPA/DPA, and then EME. Technically, however, it is not necessarily true that EME attack is stronger than Timing Analysis. Thus, the present mapping might potentially cause a conflict between security Levels and the security strength achieved, or at least mislead users to think that EME is the strongest side channel attack. **About fault based attack:** Fault-based attack is important. It is worthwhile to check whether requirements in the draft FIPS140-3 will cover fault-based attack adequately. **Setting of Cryptographic boundary:** It can be considered that side channel attack can be much more easily conducted depending on how cryptographic boundary is set.	Level 1 and 2: anything is not required. Level 3: is required to the measures against Timing Attack, SPA and SEMA. Level 4: is required to the measures against Timing Attack, SPA, DPA and EME (SEMA, DEMA). Level 5: is required to the measures against Timing Attack, SPA, DPA and EME(SEMA, DEMA). **Please refer to the attached Document 1.** We propose to add the notice that a side channel attack may become relatively easy to apply, depending on how Cryptographic boundary is defined.

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

Comment List for Draft FIPS 140-3 "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES" by CRYPTREC and INSTAC

Date: 2007-10-11	Document: **Draft FIPS 140-3**

1	2	3	4	5
Clause No./ Subclause No./ Annex (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by CRYPTREC/INSTAC**	**Proposed change by CRYPTREC/INSTAC**
4.8 Sensitive Security Parameters Management	P36	te	The sentence as follows. SSP management includes **random bit generators**, SSP generation, SSP establishment, SSP entry/output, SSP storage, and SSP zeroization. What the one included in the SSP control is not the "random bit generators", but to "conduct random bit generation (action)".	Replace "random bit generators" with "random bit generation".
4.8.4 SSP Entry and Output	P38	te	The meaning of "Non-electronically transport (definition)" is not clarified. Though it seems it is used as the antonym of "electronically transport" and is used as the synonym word of "manually transport": it still is not clearly understandable.	Definition should be added if the meaning is differed. In addition, reviewing of the expressions in the paragraph 4.8.4.8 should also be required. The meaning of "Non-electronically transport (definition)" should be clarified. In case it is the same meaning with "manually transport", it is necessary to unify the word either one of these. In such case, "Non-electronically transport" used in the 4. SECURITY REQUIREMENTS- Table 1- SSP Management "Non-electronically transport" should also be unified.
4.8.4 SSP Entry and Output	P38	te	The sentences as follows. Non-electronically transported PSPs may be entered into or output from a module in plaintext form and need not be cryptographically authenticated **regardless of whether they are entered manually or electronically**. It is inconsistent if the "Non-electronically transport" means "manually transport".	The meaning of this paragraph should be clarified.

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

Comment List for Draft FIPS 140-3 "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES" by CRYPTREC and INSTAC

Date: 2007-10-11	Document: **Draft FIPS 140-3**

1	2	3	4	5
Clause No./ Subclause No./ Annex (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by CRYPTREC/INSTAC**	**Proposed change by CRYPTREC/INSTAC**
4.8.6 SSP Zeroization	P39	te	The sentences as follows. SECURITY LEVEL 3 The cryptographic module shall control the zeroization of the CSPs. SECURITY LEVEL 4 There are no additional requirements for Security Level 4. Lv3 and 4 should be unified when presented. As with the FIPS140-2: In case there is such level which does not have additional requirements, it should be described "There are no additional requirements (for xxx) at Security Level X." only when Low Level which consecutively follows from LV1 unless otherwise the concerned level should be described together with the additional requirements of the sub-levels.	Rewrite as follows: (Use same expressions used in the Security Level 1 and2.) SECURITY **LEVELS 3 AND 4**. The cryptographic module shall control the zeroization of the CSPs.
4.11 Mitigation of Other Attacks	P48	te	TEMPEST is being missed.	It is necessary to check whether the TEMPEST should be included or not.
APPENDIX C	P56	te	About the description of APPENDIX C.	It is necessary to be rewritten.

3 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 3, 4 are compulsory.

Responses to the comments for 4.6, 4.7

The parameters to be considered upon reviewing demanded Security levels:

- **Cost for attack (time)**
- **Cost for design (time)**
- **Skills necessary for attack**
- **Cost for devices**

Respective standpoints upon reviewing:

- **as a user**
- **as a tester**
- **as a vendor**

Leakage of electromagnetic

	TA	SPA	DPA	EME		Fault Induction
				SEMA [44]	DEMA [45]	
Level 1, 2						
Level 3	**Y**	**Y**		**Y**		
Level 4 Countermeasures against significant attack	**Y**	**Y**	**Y**	**Y**		**Y**
Level 5 All countermeasures (needs to discuss)	**X**	**X**	**X**	**X**		**X**

Blue Line is proposed by the Draft FIPS 140-3.

Leakage of electromagnetic emission is the part of EME (i

Colored parts are the suggested parts for alteration.

The reasons for alteration

Reviewed from the standpoints of cryptographic module users

- **SPA and SEMA are comparable threats.**
  + Cost of attack may be differed, but the cost of design is almost the same
- **Fault induction attack is necessary for over Level 4**
  + Needs to add the definition of Fault induction attack or Fault based attack.
- **About the difference of level 4 and level 5, it is desirable to describe a difference with a qualitative expression.**

  + For example,

  - **Security Level 4: The cryptographic module resists the principal attack methods.**
  - **Security Level 5: The cryptographic module resists the attack by more powerful attacker.**

  + In DTR/IG, you should describe the difference in the security level specifically (see X).
- **We think that CPA (Correlative Power Analysis) is included in DPA.**
  *** Is CPA contained in DPA in Draft FIPS 140-3?**

[44] SEMA Simple ElectroMagnetic Analysis

[45] DEMA Differential ElectroMagnetic Analysis

+ We have classified the Side channel Attacks as follows from required capability for processing of the obtained side information.

*** SPA, SEMA..... possible with simple process**

*** DPA (CPA), DEMA, Cache attack..... needs statistic process**

発行日　2008 年 5 月 30 日第 1 版
発行者
・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
独立行政法人 情報処理推進機構
（セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY JAPAN
2-28-8 HONKOMAGOME, BUNKYO-KU
TOKYO, 113-6591 JAPAN

・〒184-8795
東京都小金井市貫井北四丁目 2 番 1 号
独立行政法人 情報通信研究機構
（情報通信セキュリティ研究センター セキュリティ基盤グループ）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI, KOGANEI
TOKYO, 184-8795 JAPAN