CRYPTREC Report 2004

平成 17 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 2004 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[1])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を評価するための基準の策定等を行っている。

海外では既に米国とカナダが共同で、FIPS 140-2 という政府調達基準に基づいて暗号モジュールに関する評価・認証制度を運用している。また、ISO/IEC JTC1/SC27/WG3 においては、暗号モジュール評価基準の国際標準化に向けた審議が開始されている。これらの動向を考慮し、昨年度は、わが国における基準策定作業を開始し、北米で運用されている基準の翻訳版として、暗号モジュールの評価基準及び試験基準の第 0 版を作成した。

本年度の暗号モジュール委員会の活動としては、昨年度作成した暗号モジュールの評価基準と試験基準の第 0 版をベースに、ISO/IEC JTC1/SC27/WG3 での国際標準化動向を調査し、国際標準との整合性を保ちつつ、わが国に適した基準策定の検討を行うとともに、暗号モジュールに対する攻撃法や対策の調査研究を実施した。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、関係者の皆様に謝意を表する次第である。

暗号モジュール委員会　委員長　松本　勉

[1] Cryptography Research and Evaluation Committees

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、暗号モジュールの評価基準及び試験基準、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。また、本報告書の別冊として、暗号モジュール評価基準の差分表、差分表に対応した暗号モジュール試験基準の検討表、運用ガイダンス第 0 版、暗号モジュール評価基準第 0.1 版、及び暗号モジュール試験基準第 0.1 版をまとめた。

これらについては、下記 URL の「CRYPTREC Report 2004 の公開」で参照できる。ただし、暗号モジュール評価基準の差分表及び差分表に対応した暗号モジュール試験基準の検討表については、対象である暗号モジュール評価基準が ISO/IEC JTC1/SC27/WG3 で現在審議中のため、非公開としている。

http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://www2.nict.go.jp/ns/s801/102/index.html

別冊(非公開)の暗号モジュール評価基準の差分表は、米国 NIST が発行している下記(1)の FIPS PUB 140-2 と ISO/IEC JTC1/SC27/WG3 で作成した下記(2)の ISO/IEC 1st CD 19790 との差分を表にまとめたものである。

別冊(非公開)の差分表に対応した暗号モジュール試験基準の検討表は、暗号モジュール評価基準の差分表において、基準内容に追加等が発生していた場合、それらの対応部分について、試験基準への追加等について検討し、表にまとめたものである。

別冊の運用ガイダンス第 0 版は、米国 NIST が発行する下記(5)の Implementation Guidance を翻訳したものである。

別冊の暗号モジュール評価基準第 0.1 版は、運用ガイダンス第 0 版の訳語との統一を図るために、昨年度作成した暗号モジュール評価基準第 0 版(下記(1)を翻訳したもの)の訳語の見直しを行ったものである。

別冊の暗号モジュール試験基準第0.1版は、昨年度作成した暗号モジュール試験基準第0版(下記(3)を翻訳したもの)に対し、下記(4)の Derived Test Requirements の Change Notice を反映させ、かつ運用ガイダンス第0版の訳語との統一を図るために、訳語の見直しを行ったものである。

(1)FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, CHANGE NOTICE (12-03-2002)

(2)ISO/IEC 1st CD 19790 Information Technology Security Techniques - Security requirements for cryptographic modules (2004-10-06)

(3) Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules (February 12, 2003 Draft)

(4) Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules (March 24, 2004 Draft)

(5)Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program (Initial Release: March 28, 2003; Last Update: September 22, 2004)

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】　cryptrec@ipa.go.jp 又は cryptrec@ml.nict.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。

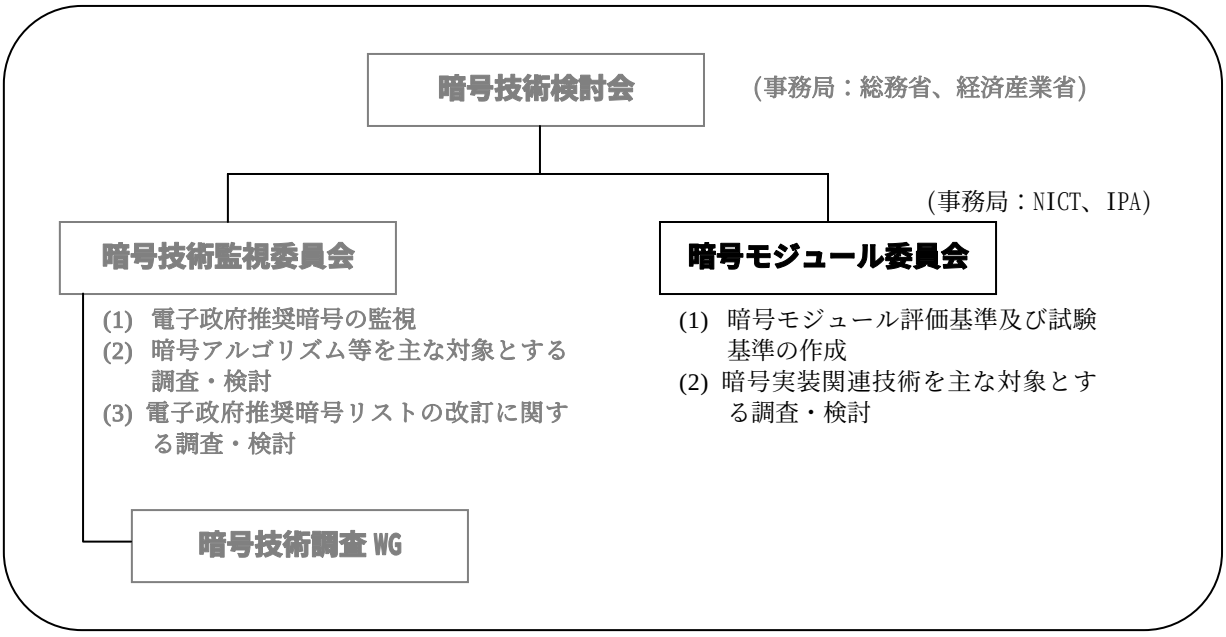

図１　2004 年度の CRYPTREC の体制

委員名簿

暗号モジュール委員会

委員長	松本　勉	横浜国立大学 大学院　教授
委員	石田　修一	株式会社日立製作所　研究員
委員	上野　天徳	財団法人日本品質保証機構　主任
委員	植村　泰佳	電子商取引安全技術研究組合　常務理事
委員	大須賀　勝美	NTT エレクトロニクス株式会社　技術主査
委員	太田　和夫	電気通信大学　教授
委員	大塚　浩昭	日本電信電話株式会社
委員	佐伯　正夫	三菱電機インフォメーションシステムズ株式会社 副センター長(2005 年 1 月まで)
委員	佐伯　稔	三菱電機株式会社　主席研究員
委員	佐藤　証	日本アイ・ビー・エム株式会社　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	東芝ソリューション株式会社　SI 技術担当
委員	鳥居　直哉	株式会社富士通研究所　部長
委員	細川　正広	日本電気株式会社　マネージャー(2004 年 11 月まで)
委員	森岡　澄夫	ソニー株式会社　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　参与
委員	米倉　昭利	財団法人日本情報処理開発協会　センター長

オブザーバ

山田　浩一	警察庁　情報通信局
中山　毅彦	警察庁　情報通信局
知識　親美	警察大学校　警察情報通信研究センター
富田　哲	防衛庁　長官官房(2004 年 4 月まで)
山城　瑞樹	防衛庁　長官官房
一條　靖彦	防衛庁　陸上幕僚監部(2004 年 7 月まで)
加納　信生	防衛庁　陸上幕僚監部
石川　正興	防衛庁　技術研究本部

小森　旭　　防衛庁　技術研究本部
山本　寛繁　　総務省　行政管理局
野崎　雅稔　　総務省　情報通信政策局
榎本　淳一　　総務省　情報通信政策局
黒田　崇　　総務省　情報通信政策局
石川　雅一　　外務省　大臣官房
勝亦　眞人　　経済産業省　産業技術環境局
小谷　光弘　　経済産業省　産業技術環境局
北浦　康弘　　経済産業省　商務情報政策局 (2004 年 7 月まで)
南　　英生　　経済産業省　商務情報政策局 (2004 年 7 月まで)
柳原　聡子　　経済産業省　商務情報政策局
松井　洋二　　経済産業省　商務情報政策局
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
早貸淳子、西原正人、網島和博、大熊建司、大塚玲、小柳津育郎、杉田誠、
山岸篤弘

独立行政法人 情報通信研究機構
大久保明、鳥居秀行(2004 年 7 月まで)、曽根裕、天野滋、太田将史、高橋靖典、
田中秀磨、半澤則之(2004 年 10 月まで)、山村明弘

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で相手と直接対面することなしに受発注や決済等の重要な情報をやり取りする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行政手続きの電子化を実現する電子政府システムの構築が精力的に進められている。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。そのため、暗号技術を電子政府等で利用するためには、暗号技術を客観的に評価することが極めて重要となる。

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。この委員会は、産学の最高水準の暗号専門家により構成され、わが国における本格的な暗号技術評価プロジェクトがスタートすることになった。2001 年度から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)が参加することとなった。

また、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して政策的な観点から検討が開始された。暗号技術評価委員会と暗号技術検討会には、関係する省庁もオブザーバとして参加する等、政府横断的な活動となっており、これらを総称して、CRYPTREC(Cryptography Research and Evaluation Committees)と呼ぶことになった。

2000 年度から 2002 年度までの 3 年間に及ぶ CRYPTREC 活動によって、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に客観的な評価が実施された結果、合計 29 方式の暗号技術が安全性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 年度には、電子政府推奨暗号の監視活動を含め、電子政府の安全性及び信頼性を

引き続き確保していく必要があるため、暗号技術検討会を存続させ、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、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 に再編された。

1.2 暗号モジュール評価の標準化に関する国際動向

暗号モジュール評価の国際的な標準化活動としては、(1)米国/カナダが共同運用しているCMVP[2]、(2)ISO/IEC JTC1/SC27/WG3 で審議中の暗号モジュール評価基準の国際標準化、の 2 つが重要である。

CMVPは米国のNIST[3]とカナダのCSE[4]が共同運用している暗号モジュールの評価プログラムである。米国連邦政府が調達する、機微であるが機密でない情報の秘匿･完全性･認証を実現する暗号モジュールの評価・認証は、評価基準FIPS[5] 140-2 に基づいて行われる。

CMVPでは、現行の評価基準FIPS 140-2 を改訂し、新基準FIPS 140-3 に移行する方針であり、その説明のためにCMVPシンポジウム 2004[6]を 2004 年 9 月にワシントンDC郊外のRockvilleで開催した。会合でのトピックスは、(1)FIPS 140-3 の発行に向けた、FIPS 140-2 の改訂作業の開始、(2)DESの廃止、(3)暗号モジュール評価に関する国際相互承認への言及、の 3 点である。FIPS 140-3 の発行に向けたFIPS 140-2 の改訂作業は 2005 年 1 月に開始し、2006 年 11 月の完了を目指している。FIPS 140-3 の発効に伴い、FIPS 140-2 は 2007 年 5 月に失効する予定である。

FIPS 140-2 の主な改訂の予定箇所は、ソフトウエア暗号モジュールの取り扱い、動作モード、物理的セキュリティ、鍵管理など 8 項目である。日本で関心の高い電力解析関係は言及されなかったものの、EMI/EMC[7]関連基準の見直しと、スマートカードを評価対象に含める方針は示された。

ISO/IEC JTC1[8]は、ISO[9]とIEC[10]が共同で運営するIT技術標準化のための組織で、SC27 委員会で情報セキュリティを、その下のWG3 で情報セキュリティの評価基準を担当している。

---

[2] Cryptographic Module Validation Program
[3] National Institute of Standards and Technology
[4] Communications Security Establishment
[5] Federal Information Processing Standards
[6] Cryptographic Module Validation Program Symposium 2004, http://csrc.nist.gov/cryptval/cmvp2004/
[7] Electromagnetic Interference / Electromagnetic Compatibility
[8] Joint Technical Committee 1
[9] International Organization for Standardization
[10] International Electrotechnical Commission

ISO/IEC JTC1/SC27/WG3 は、2002 年 10 月から暗号モジュール評価基準の国際標準化[11](規格予定番号 19790)を審議している。2004 年の国際会合は、4 月(シンガポール)と 10 月(ブラジル)の 2 回開催された。この間に暗号モジュール評価基準の国際標準化フェーズは、2nd WD[12]からFCD[13]へと進捗し、2006 年 4 月にはIS[14]化される見込みである。

図 2 に FIPS 140 と IS 19790 の関係を示す。IS 19790 は、FIPS 140-2 をベースとした基準であるが、CC(Common Criteria)への連接性を意識しているため、詳細な評価項目は異なる部分が存在する。また、FIPS 140-3 については、成立見込み時期が IS 19790 よりも遅いことから、IS 19790 の内容を反映する可能性がある。

さらに、暗号モジュール評価基準の国際標準化に付随して、実際の評価・運用に必要となる、運用ガイダンスと暗号モジュール試験基準の標準化も study period として検討されることとなった。

ここで紹介した標準化動向に関するより詳細な内容については、本報告書の 3.1.2.1 節を参照されたい。

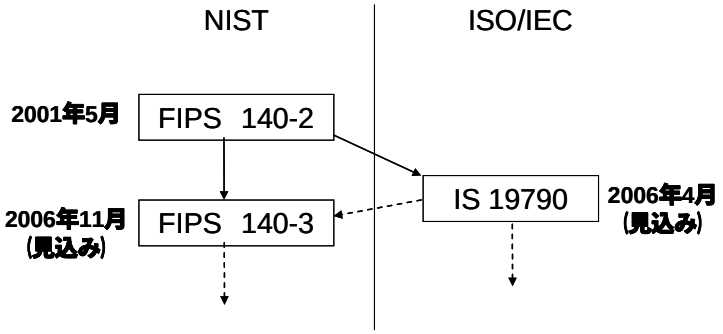

図 2 FIPS 140とIS 19790の関係

1.3 暗号モジュールに対する攻撃に関する研究動向

暗号モジュールの安全性評価には、使用される暗号方式の数学的安全性に加え、実装に伴った情報漏洩の可能性も考慮する必要がある。このような実装の特性に着目した攻撃法は近年盛んに研究されている。表 1 に今年度中に学会発表されたもの（予定を含む）を示す。

[11] Security Requirements for Cryptographic Modules
[12] Working Draft
[13] Final Committee Draft
[14] International Standard

表１　暗号モジュールに対する攻撃に関する学会別発表件数

学会名	発表件数
ASIACRYPT 2004	1
CHES[15] 2004	6
EUROCRYPT 2004	1
PKC[16] 2005	1
情報セキュリティ研究会(ISEC 研究会)	10
SCIS[17] 2005	21
CSS[18] 2004	3
集積回路研究専門委員会（ICD[19]）	3
その他（e-Print 等）	1

実装の特性に着目した攻撃は、破壊攻撃と非破壊攻撃の 2 種類に大別できる。破壊攻撃は、暗号モジュールのパッケージを剥がして配線を読み取るといった、不可逆的な改変を伴うものである。一方、非破壊攻撃は、動作時の実行時間や消費電力量等の観測だけで、暗号モジュール自体の改変を伴わないものである。現状では、非破壊攻撃の研究がより盛んである。

非破壊攻撃はサイドチャネル攻撃とも呼ばれ、今年度の重要な発表としては、(1)スマートカードに実装された DSA 署名の署名鍵を実際に求めてみせた Naccache らの研究(PKC 2005)、(2)DES の実装に対する従来の電力解析への防御策のほとんどを無効にする Kunz-Jacques らの研究(ASIACRYPT 2004)、(3)電力解析用評価環境の開発とそれを利用した評価実験（ISEC 7 月)、などがある。

破壊攻撃に関しては、電子情報通信学会の時限研究会・LSI 動作解析研究会において、LSI 研究者と暗号研究者が現状の LSI 解析技術で実際の LSI チップがどの程度解析可能かを検討した。研究成果は、集積回路研究会(ICD)の平成 16 年度 9 月研究会で発表された。

ここで紹介した研究発表に関するより詳細な内容については、本報告書の 3.2.3 節及び参考文献を参照されたい。

[15] Workshop on Cryptographic Hardware and Embedded Systems
[16] International Workshop on Practice and Theory in Public-Key Cryptography
[17] Symposium on Cryptography and Information Security
[18] Computer Security Symposium
[19] Integrated Circuits and Devices

1.4 暗号モジュール委員会の活動目的

以上のような状況を踏まえ、昨年度、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得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作業を開始し、北米の評価基準及び試験基準の翻訳版として、暗号モジュール評価基準及び試験基準の第0版を発行した。また、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・研究として、その具体的テーマに、非破壊攻撃の1つである電力解析に関する調査・研究を選定し、電力解析のためのFPGA[20]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。

今年度の活動として、暗号モジュール委員会では、昨年度に引き続き、次の2つを主な活動項目とした。

(1)暗号モジュール評価基準及び試験基準の策定

(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

各活動項目の詳細は以下のとおりである。

(1)暗号モジュール評価基準及び試験基準の策定

現在審議中の国際標準(ISO/IEC 19790)は、当初、FIPS 140-2ベースでIS化されるものと予想していたが、審議状況から、内容的にFIPS 140-2と大きな差が発生する可能性が出てきた。そのため、今年度予定していた評価基準及び試験基準第1版の策定作業を休止し、国際標準にも対応可能なように、準備として以下のa)～e)の作業を行うこととする。

a)暗号モジュール評価基準の差分表の作成

FIPS 140-2と国際標準（1st CD 19790）との差分表を作成し、作成した差分表の翻訳を行うことで、暗号モジュール評価基準第0版と国際標準との差分表の作成を行う。

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

暗号モジュール評価基準第0版の内容に追加等が発生した場合、対応部分について暗号モジュール試験基準第0版の内容についても追加等が必要である。上記a)にて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。

[20] Field Programmable Gate Array

c)ISO/IEC JTC1/SC27/WG3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)”の翻訳版の作成を行う。4月28日以降に改版が発行された場合には、逐次、翻訳対応することとする。

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

昨年度作成した暗号モジュール評価基準及び試験基準第 0 版に対して、NIST発行のFIPS 140-2, DTR[21]のCHANGE NOTICEへの対応等を行った修正版の作成を行う。

(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

今年度は、評価用標準プラットフォームを用いた評価データの蓄積期間と位置付け、原則、委員会内での検討作業は行わないこととする。なお、昨年度、暗号モジュール委員会にて仕様策定を行った評価用標準プラットフォームの入手及び委員への評価用標準プラットフォームの配布は次のように実施することとする。

a)評価用標準プラットフォームの入手

暗号モジュール委員会では、INSTAC[22]の耐タンパー性に関する標準化調査研究委員会（委員長：横浜国立大学 松本教授）と協調して、暗号モジュールへの非破壊攻撃及び破壊攻撃に対する評価基準の検討を行っている。

今年度、耐タンパー性に関する標準化調査研究委員会では、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に、暗号モジュール委員会にて昨年度策定した FPGA を用いた評価用標準プラットフォーム仕様を加えた評価用標準プラットフォーム仕様の策定を行う。

INSTACの委託先が、今年度、本仕様にもとづく評価ボード（INSTAC-32準拠評価用標準プラットフォーム）を作成し、実証実験を行うため、その委託先からプラットフォームの入手を行う。

---

[21] Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules

[22] 日本規格協会　情報技術標準化研究センター

b)委員への評価用標準プラットフォームの配布

得られた成果について、学会等で発表いただく条件にて、希望する委員に対して無償配布を行う。

第 2 章　委員会の開催状況

2004 年度の暗号モジュール委員会は、計 5 回開催された。各回会合の概要は表 2 のとおりである。

表 2　2004 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 16 年 6 月 23 日 10：00～12：00	ISO/IEC JTC1/SC27/WG3 シンガポール会合報告 平成 16 年度暗号モジュール委員会活動計画（案）について
第 2 回	平成 16 年 9 月 10 日 10：00～13：40	差分表の検討について 運用ガイダンス第 0 版の検討について
第 3 回	平成 16 年 11 月 12 日 14：00～18：00	CMVP シンポジウム 2004 及び NIST 定期会議報告について ISO/IEC JTC1/SC27/WG3 ブラジル会合報告について 評価基準の差分に対応した試験基準の検討について シングルチップモジュールの validation 後のアプリケーション追加について
第 4 回	平成 16 年 12 月 10 日 14：00～18：00	評価基準の差分に対応した試験基準の検討について 運用ガイダンス第 0 版の検討について 暗号モジュール委員会活動報告書の作成について シングルチップモジュールの validation 後のアプリケーション追加について
第 5 回	平成 17 年 2 月 18 日 10：00～12：00	FIPS 140-2 及び Final CD に対するコメント作成について 暗号モジュール委員会活動報告書の作成について 来年度以降のスケジュールについて

第 3 章　活動内容と成果概要

3.1　暗号モジュール評価基準及び試験基準の策定

3.1.1　基準類の概要

(1)FIPS 140-2

FIPS 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求事項を規定した、NIST が発行する米国政府標準である。

FIPS 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 140-1 が制定され、2001 年 5 月には FIPS 140-2 として改訂された。FIPS 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 140-1 が開発された以降に利用可能となった標準及び技術の変更も取り入れている。FIPS 140-2 は適宜改訂されており、2002 年 12 月の改訂版が 2005 年 3 月時点での最新版となっている。

FIPS 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

DTR は、暗号モジュールが FIPS 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 も FIP 140-2 と同様に適宜改訂されており、2004 年 3 月の改訂ドラフト版が 2005 年 3 月時点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 140-2 で規定された 11 分野に対応している。各章では、FIPS 140-2 に対応するセキュリティ要求事項をアサーション(すなわち、設定されたセキュリティレベルで、設定された分野のセキュリティ要求事項を暗号モジュールが満足するために適用しなければならない宣言)として記述している。全てのアサーションは FIPS 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、試験者が実施しなければならない試験手順を記述している。

(3) Implementation Guidance

Implementation Guidance 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。

Implementation Guidance も FIPS 140-2 及び DTR と同様に適宜改訂されており、2005 年 1 月の改訂版が 2005 年 3 月時点での最新版となっている。

Implementation Guidance は、全 17 節(OVERVIEW, GENERAL ISSUES, SECTION 1 から SECTION 14, EXPIRED IMPLEMENTAITON GUIDANCE)から構成されている。

“SECTION 1 から SECTION 14”は、FIPS 140-2 の 4.1 節から 4.11 節(SECTION 1 から SECTION 11 に対応)、APPENDIX A(SECTION 12 に対応)、 APPENDIX B(SECTION 13 に対応)、APPENDIX C(SECTION 14 に対応)にそれぞれ対応しており、FIPS 140-2 で規定されるセキュリティ要求事項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。

“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。

3.1.2 国際標準への対応検討

3.1.2.1 国際標準の動向

暗号モジュール評価に関する国際的な動向としては、(1)米国/カナダが共同運用している CMVP、(2)ISO/IEC JTC1/SC27/WG3 で審議中の暗号モジュール評価基準の国際標準化、の 2 つが重要である。

(1)CMVP 動向

2004 年 9 月 14 日、15 日の 2 日間にわたり、CMVPシンポジウム 2004[23]がワシントン DC郊外のRockvilleで開催された。CMVPシンポジウム 2004 は米国NISTとカナダCSEが主催し、米国連邦政府が調達する機微であるが機密でない情報の秘匿・完全性・認証を実現する暗号モジュールに対する要求基準とその評価に関する会合である。

会合は、以下のセッションとパネルディスカッションがあり、米国・カナダ以外に日本、フランス、韓国、ブラジルなど 8 カ国 120 名の参加があった。

[23] Cryptographic Module Validation Program Symposium 2004, http://csrc.nist.gov/cryptval/cmvp2004/

a) Keynote Address (Miles E. Smid)
b) CMVP Perspective and Standards Update(Ed Roback)
c) CMVP Status and FIPS 140-2 (Randall Easter, Ken Lu)
d) Hot Topics in Testing
- New Implementation Guidance (Randall Easter)
- FIPS 140-2 Expectation Management(Jean Campbell)
e) New CAVS Tool Development(Sharon Keller)
f) NVLAP - What Does It Mean to be an Accredited Laboratory?(Jeffrey Horlick)
g) International Topics - ISO/IEC Update(Randall Easter)
h) Other Hot Topics(Ghislain Lagace)
i) Vendor Panel Discussion - Impact of FIPS 140-2
j) Future Directions(Jean Campbell, Ray Snouffer,)
- FIPS 140-3 - Looking over the Horizon
- Cost Recovery
k) FISMA Implementation(Ron Ross)

今回の会合でのトピックスとしては、FIPS 140-3 の発行に向けた、FIPS 140-2 の改訂作業が開始[24]されること、DESの廃止[25]、及び暗号モジュール評価に関する国際相互承認に言及されたことの３点である。

・FIPS 140-2 の改訂作業は、2005 年 1 月から開始され、2006 年 11 月の完成を目指している。FIPS 140-3 の発効に伴い、FIPS 140-2 は 2007 年 5 月に失効するとアナウンスされた。主な改訂の予定箇所は、ソフトウエア暗号モジュールの取り扱い、動作モード、物理的セキュリティ、鍵管理など８項目が挙げられていたが、日本で学問的な関心も高い電力解析関係の言及はなかった。ただし、EMI/EMC 関連基準の見直し、スマートカードを評価対象に含めたいとの発言もあった。FIPS 140-2 の改訂スケジュールを表 3 に示す。

・DES 暗号に関しては、Triple-DES の部品としての位置づけとなり、Approved という位置づけを失う（ただし、当面下位互換性を維持するための使用は容認されている）。

・ 暗号モジュール評価の国際相互承認に関しては、従来よりも柔軟な姿勢が示された。

なお、CMVP シンポジウム 2004 での講演内容の詳細については、下記 URL を参照されたい。

[24] http://csrc.nist.gov/cryptval/Jan12-2005-FR-FIPS1403-Notice.pdf
[25] http://csrc.nist.gov/Federal-register/July26-2004-FR-DES-Notice.pdf

http://csrc.nist.gov/cryptval/cmvp2004/agenda.html

表 3　FIPS 140-2 の改訂スケジュール

Milestones	期間/期日
現行の FIPS 140-2 に対する意見招請	2005 年 1 月 5 日～2005 年 2 月 28 日
Draft #1 FIPS 140-3 の作成 ・ユーザからの意見の反映 ・新しい要求項目の盛り込み	2005 年 4 月 5 日～2005 年 8 月 4 日
Draft #1 FIPS 140-3 への意見招請	2005 年 10 月 5 日～2006 年 1 月 4 日
FIPS PUB 140-3 の作成 ・ユーザからの意見の反映	2006 年 1 月 6 日～2006 年 2 月 5 日
FIPS 140-3 承認 process	2006 年 2 月 6 日～2006 年 5 月 5 日
FIPS 140-3 承認	2006 年 5 月 6 日
FIPS 140-3 試行期間	2006 年 5 月 6 日～2006 年 11 月 6 日
FIPS 140-2 の廃止(FIPS 140-3 の正式発効) ・validations still effective	2006 年 11 月 7 日

(2)ISO/IEC JTC1/SC27/WG3 動向

ISO/IEC JTC1/SC27/WG3 では、2002 年 10 月から暗号モジュール評価基準の国際標準化に関する審議を行っている。2004 年度は、2004 年 4 月 19 日～4 月 23 日(シンガポール)と 2004 年 10 月 18 日～10 月 22 日(ブラジル)の 2 回の会合があり、2nd WDからFCDへと標準化フェーズが進捗した、2006 年 4 月にはIS化される見込みとなった。両会合には、暗号モジュール委員会での修正コメントをベースにISO/IEC JTC1/SC27/WG3国内委員会でのコメント審議を行い、日本NB[26]としての修正コメントを提出した。日本NBとしては、44 件のコメントを提出し、内 42 件が受理され、2 件がRejectされた。Rejectされた 2 件のうち、1 件は英文表記(米式綴りと英式綴りの混在を指摘した)であり、ISO/IEC JTC1/SC27 事務局として「ISOの正式文書では英語を採用する」という方針の再確認につながった。

さらに、暗号モジュール評価基準の国際標準化に追従して、試験基準と運用ガイダンスの標準化も study period として検討されることとなった。

また、暗号モジュール評価基準の国際標準案（ISO/IEC 19790）は、FIPS 140-2 をベースとした標準であるが、CC（Common Criteria）への連接性を意識しているため、詳細な評価項目は異なる部分が存在する。国際標準案（1st CD 19790）と FIPS 140-2 との差分及び差分に対応する試験基準については、後述の通り、暗号モジュール委員

[26] National Body

会で検討を実施している。

3.1.2.2 国際標準への対応

今年度、暗号モジュール委員会では、3.1.2.1 で述べたような暗号モジュール評価の標準化に関する国際動向に対応すべく、その準備として、以下の(1),(2)の作業を行い、表に整理してまとめた。なお、本表については、ISO/IEC JTC1/SC27/WG3 での審議内容を多く含んでいるため、2005 年 3 月時点での公開を予定していない。

(1)暗号モジュール評価基準の差分表の作成

FIPS 140-2 と国際標準案（1st CD 19790）との差分表を作成し、暗号モジュール委員会内での検討を完了した。検討結果については、表に整理してまとめた。また、国際標準案が 1st CD から FCD へ進む際に修正部分が多数発生しており、今後も継続的な検討が必要である。

なお、差分表の翻訳については、国際標準案（ISO/IEC 19790）がほぼ確定した時点で改めて実施することとなった。

(2)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(1)の差分表に対応した暗号モジュール試験基準案を作成し、暗号モジュール委員会内での検討を完了した。検討結果については、表に整理してまとめた。また、国際標準案が 1st CD から FCD へ進む際に上記(1)の差分表の修正部分が多数発生していることや試験基準の国際標準化の動きがある（study period）ことから、今後も継続的な検討が必要である。

3.1.3 運用ガイダンス第 0 版の検討

(1) 第 0 版の作成

まず、事務局にて“Implementation Guidance”の 2004 年 4 月改訂版の翻訳案を作成し、翻訳案に対して委員会内での審議を行い、英文解釈の統一化を図った。

次に、“Implementation Guidance”が 2004 年 9 月に改訂されたため、その差分について、事務局にて翻訳案を作成し、同様に委員会内での審議を行い、英文解釈の統一化を図った。

そして、委員会内での英文解釈を統一化した“Implementation Guidance”の 2004 年 9 月改訂版の翻訳を運用ガイダンス第 0 版としてまとめた。また、2005 年 1 月にはさらに改訂されたため、その差分について翻訳検討中である。

今後、“Implementation Guidance”のさらなる改訂版にも追従していくとともに、国際動向も考慮しながら、わが国の運用ガイダンス第 1 版を作成していく予定であ

る。

(2) 第0版の構成

運用ガイダンス第0版は、“Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, Initial Release: March 28, 2003; Last Update: September 22, 2004”を翻訳したものであり、構成は、3.1.1節(3)で述べた“Implementation Guidance”と同様である。

本文は全17節から構成されており、「概要」、「全般的な問題」、「第1章　暗号モジュールの仕様」、「第2章　暗号モジュールのポート及びインタフェース」、「第3章　役割、サービス、及び認証」、「第4章　有限状態モデル」、「第5章　物理的セキュリティ」、「第6章　動作環境」、「第7章　暗号鍵管理」、「第8章　電磁妨害/電磁両立性(EMI/EMC)」、「第9章　自己テスト」、「第10章　設計保証」、「第11章　その他の攻撃への対処」、「第12章　Appendix A: 文書要求事項のまとめ」、「第13章　Appendix B: 推奨ソフトウエア開発手順」、「第14章　Appendix C: 暗号モジュールのセキュリティポリシ」、「取消された運用ガイダンス」が記述されている。

各節の冒頭には、NIST及びCSEからの解答内容に関し、適用されるセキュリティレベル、有効期間、最終改訂日、DTRの関連するアサーションの番号(AS番号)、DTRの関連する試験者に課せられる要求事項の番号(TE番号)、DTRの関連するベンダに課せられる要求事項の番号(VE 番号)が記述されている。その後に、背景(節によっては記述されない)、NIST及びCSEへの質問内容、NIST及びCSEからの解答、NIST及びCSEからの追加コメントが順に記述されている。

運用ガイダンス第0版については、下記URLの「CRYPTREC Report 2004 の公開」から参照できる。

http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://www2.nict.go.jp/ns/s801/102/index.html

3.1.4 評価基準/試験基準第0.1版の作成

3.1.4.1 評価基準第0.1版の作成

昨年度の暗号モジュール委員会では、“FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, CHANGE NOTICE(12-03-2002)”を翻訳したものを暗号モジュール評価基準第0版として発行した。

今年度の暗号モジュール委員会では、運用ガイダンス第0版の訳語との統一を図るために、暗号モジュール評価基準第0版の訳語の見直しを行い、暗号モジュール評価基準第0.1版として発行した。

暗号モジュール評価基準第 0.1 版については、下記 URL の「CRYPTREC Report 2004 の公開」から参照できる。

http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://www2.nict.go.jp/ns/s801/102/index.html

なお、昨年度、問題点整理表としてまとめた、基準内容に関する不明点及び問題点に関し、その回答を表 4 に記載した。表中の「---」と記載されている内容については、引き続き、検討が必要な項目である。

3.1.4.2 試験基準第 0.1 版の作成

昨年度の暗号モジュール委員会では、“Derived Test Requirements for FIPS PUB 140-2, Security Requirement for Cryptographic Modules (February 12, 2003 Draft)”を翻訳したものを暗号モジュール試験基準第 0 版として発行した。

上記 DTR は 2004 年 3 月 24 日に改訂ドラフト版が発行されたため、今年度の暗号モジュール委員会では、暗号モジュール試験基準第 0 版に対して、主に DTR の改訂部分を反映させるとともに、運用ガイダンス第 0 版の訳語との統一を図るために、暗号モジュール試験基準第 0 版の訳語の見直しを行い、暗号モジュール試験基準第 0.1 版として発行した。

暗号モジュール試験基準第 0.1 版については、下記 URL の「CRYPTREC Report 2004 の公開」から参照できる。

http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://www2.nict.go.jp/ns/s801/102/index.html

なお、昨年度、問題点整理表としてまとめた、基準内容に関する不明点及び問題点に関し、その回答を表 4 に記載した。表中の「---」と記載されている内容については、引き続き、検討が必要である。

表4　暗号モジュールの評価基準及び試験基準における問題点整理表(1/4)

No.	対象	指摘箇所	問題点(上段)/回答(下段)
1	評価基準	1.2節　第4段落	電子政府向け暗号モジュールの要求事項において、CC(Common Criteria)への適合を含めてよいのかの検討が必要である。

2	試験基準	TE01.08.05	試験者は、何をもって十分詳細と判断するのかをNISTに確認する必要がある。 TE01.08.02やTE01.08.03にて挙げられている箇条書き項目が含まれていれば十分詳細とするのか、それとも、その箇条書き項目の内容が十分詳細であるかどうかを判断する必要があるのか？
			試験者自身が納得できるまで、ベンダに対し、さらなる情報提供を要求したり、ベンダとの会議を何回も実施したりする。
3	評価基準 試験基準	4.1節 第11段落 AS01.14	「高級言語(High-level specification languages)を用いて設計されていなければならない」とあるが、「高級仕様言語を用いた設計」がどのようなことを指すのかをNISTに確認する必要がある。
			試験者が設計内容を理解しやすいように、高級言語を指定しているだけである。
4	試験基準	TE02.01.04	実際どのように検証すればよいのかをNISTに確認する必要がある。
			試験者自身が納得できるまで、ベンダに対し、さらなる情報提供を要求したり、ベンダとの会議を何回も実施したりする。
5	試験基準	VE02.11.01	主要カテゴリが何を指しているかをNISTに確認する必要がある。
			認証データや鍵など、ごく一般的なカテゴリのことである。
6	試験基準	VE03.20.01	"authentication"は、"authorization"の誤りではないかをNISTに確認する必要がある。ただし、TE03.20.02の内容から、誤りでない可能性もある。
			誤りである。
7	試験基準	VE03.22.01	"authentication data to the module"は、直前のAS03.22の"authentication data within the cryptographic module"と同じ意味かどうかをNISTに確認する必要がある。
			同じ意味である。 DTR全体において、用語の表現に関しては、アサーションで記述されている用語の表現の方が正しい表現と考えてよい。

表 4　暗号モジュールの評価基準及び試験基準における問題点整理表(2/4)

No.	対象	指摘箇所	問題点(上段)/回答(下段)
8	試験基準	TE04.05.02	"the finite state diagrams"は"the state transition diagrams"と同じ意味かどうかを NIST に確認する必要がある。
			同じ意味である。
9	評価基準 試験基準	4.5 節 第 1 段落 AS05.01	(1)"When installed"は、" to deter unauthorized use or modification of the module (including substitution of the entire module)"にかかるのか、又は、文章全体にかかるのかを NIST に確認する必要がある。 (2)"When installed"は、「インストールの作業中」か、又は、「インストールされている状態」の意味のどちらであるかを NIST に確認する必要がある。
			(1)文章全体にかかる。 (2)「暗号モジュールが物理的に設置されている状態」を指している。通常、暗号モジュールの物理的な設置は、ユーザに渡ったときではなく、ユーザに渡す前に行われる。
10	試験基準	TE05.09.02	"operational keys"の定義を NIST に確認する必要がある。
			あらかじめ暗号モジュールの中に入れてある鍵を指し、セッションキー等ではない。
11	評価基準 試験基準	4.5.3 節 第 4 段落 AS05.34	"production-grade"の定義を NIST に確認する必要がある。
			"industry standard"(工業標準)であること。
12	試験基準	VE05.37.03	機械的錠が掛けられている場合において、錠についての文書の必要性を NIST に確認する必要がある。
			(2 時間の)ピッキング耐性があることを示す文書が必要である。 また、試験を行うために、ベンダに対し、特殊なピッキングツールの提供も要求する。
13	評価基準 試験基準	4.5.3 節 第 22 段落 AS05.41	"strong enclosure"の定義を NIST に確認する必要がある。
			次のいずれか。("strong"と"hard"は意味が異なる) ・"Maintenance Interface or Removable Covers/Doors ”をもち、"Tamper Response and Zeroization Circuitry"を含む enclosure ・"Non-Removable Enclosure(verify cannot be removed)"であって、"High Probability of Incurring Serious Damage"である enclosure

表 4　暗号モジュールの評価基準及び試験基準における問題点整理表(3/4)

No.	対象	指摘箇所	問題点(上段)/回答(下段)
14	試験基準	TE05.47.01	"The vendor literature"は、"documentation"の間違いかどうか確認する必要がある。間違いでなければ、"The vendor literature"の定義を NIST に確認する必要がある。
			間違いである。
15	試験基準	TE05.53.04	本試験は、「囲いが除去可能なカバー若しくはドアを有する場合」に必要な試験かどうかを NIST に確認する必要がある。
			必要である。レベル 3 では、タンパー時にゼロ化が要求される。 「7.6 鍵のゼロ化」はドキュメントチェックのみである。実際にゼロ化の動作確認を行うテストとして TE05.53.04 が必要である。
16	試験基準	TE06.08.02	(1)「改ざん」の定義を NIST に確認する必要がある。(意味を持たない変更も改ざんと扱うのかどうか？) (2)「完全性が維持される場合には」とは、「事実として完全性が維持されている」のか、又は「事実として完全性は崩れているが維持されているように見える」のか、どちらの意味なのかを NIST に確認する必要がある。
			(1)同じデータを上書きするなど意味を持たない変更は「改ざん」と扱わない。 (2)後者である。すなわち、「改ざんしたにもかかわらず、改ざんを検出できない場合には」の意味である。
17	試験基準	TE07.01.02	本試験内容は、1 項、2 項の条件の両方があって初めて成立する内容であり、かつ、1 項の"access"には、"modify"も含まれるが、"modify"に関しては、2 項で述べているので、1 項では暗号化された鍵にアクセスできてもよいという解釈でよいかを NIST に確認する必要がある。
			1 項は、「暗号化された鍵にアクセスできてもよい」との解釈でよい。
18	評価基準 試験基準	4.8 節全体 8 章全体	本節/本章に記載されている FCC(強制法規)に相当する規格は日本にはないため、電子政府向け暗号モジュールの要求事項として、本節/本章をどのように扱うかについて検討が必要である。

表 4　暗号モジュールの評価基準及び試験基準における問題点整理表(4/4)

No.	対象	指摘箇所	問題点(上段)/回答(下段)
19	試験基準	VE09.31.01, VE09.33.01	DTR における AS と VE の TE において、AS の段階で明示的に文書化の要求と実装上の要求をしている場合と、AS では機能面の要求だけで、VE や TE で文書化と実装面に分離している場合と１つの VE や TE の中で文書化と実装の一致を要求している場合があり、首尾一貫していないため、第１版作成に向け、記載されている内容が何を要求しているのか(例えば、文書化のみを要求/実装の一致を要求/文書化 + 実装の一致の要求等をコメント欄に記載する)を明確化するかどうかを含め、再度整理が必要である。

20	評価基準 試験基準	4.9.2 節 第 14 段落 AS09.43	本試験は、次のｎbit を生成して比較するのか、又はシフト詰めして比較するのか、又はどちらでもよいのかを NIST に確認する必要がある。 例：1 bit 単位で乱数生成する場合、 ・初期化後：2n bit 生成して、n bit で分けて、比較する。 ・その後： <A> 1 bit 生成して、2n bit を 1 bit シフト詰めして比較する？ <B> n bit 生成して、2n bit を n bit シフト詰めして比較する？
			Fig.1※の例(RNGの出力が 12bitずつでn=18 の場合)では、Way3 がベターであるが、Way1 でも可である。Way2 はだめである。試験時には、ソースコードもチェックしている。
21	試験基準	TE10.15.01	注に記載されている"NCSC-TG-10"に相当する規格は日本にはないため、電子政府向け暗号モジュールの要求事項として、本注をどのように扱うかについて検討が必要である。

22	評価基準 試験基準	APPENDIX A 第１段落 AS12.01	"the validation facility"は「試験機関」の誤りではないかを NIST に確認する必要がある。
			誤りである。CMT Lab のことである。

※表 4(4/4)の No.20 の回答欄で参照されている Fig.1

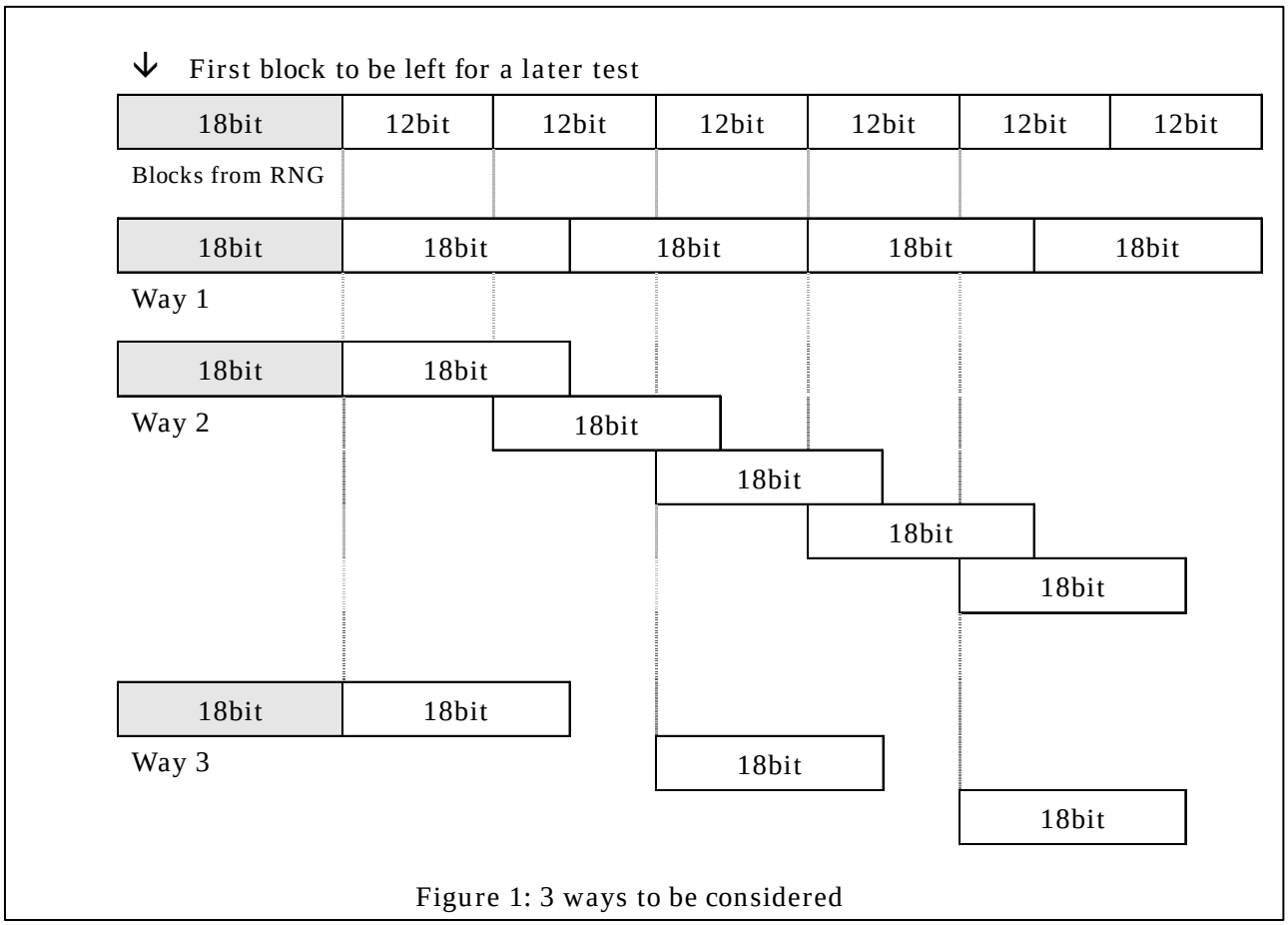

Figure 1: 3 ways to be considered

3.2 非破壊攻撃及び破壊攻撃に対する調査・研究

3.2.1 評価用標準プラットフォームの検討方針

昨年度、暗号モジュール委員会では、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・研究において、その具体的テーマを検討するにあたり、INSTAC の耐タンパー性に関する標準化調査研究委員会(委員長:横浜国立大学 松本教授)と共同で文献調査を行い、暗号モジュールへの電力解析に関する調査・研究を具体的テーマとして決定した。

また、その研究の位置づけは、暗号モジュールへの電力解析への対策に関する評価基準及び試験基準策定のための予備的な研究とし、理論だけでなく、攻撃及び対策の効果に対する追試実験等を行い、実データに基づいた研究を行うことを研究方針とした。本研究を進めるにあたり、基準策定のための必要なデータを多くの研究機関から効率的に収集できるよう、評価用標準プラットフォームを構築し、このプラットフォーム上での評価手法の確立を目指すこととした。

また、評価用標準プラットフォームにおいて、早期に着手可能であり、評価対象を柔軟かつ広範囲に設定できることから、FPGA による評価用標準プラットフォームを作成することとし、その要求仕様を決定した。

詳細は、昨年度公開した「CRYPTREC Report 2003 の公開」の「CRYPTREC Report 2003 暗号モジュール委員会報告書」[27]を参照されたい。

今年度は、FPGA による評価用標準プラットフォームを作成し、委員への配布を行うこととし、評価用標準プラットフォームを用いた評価データの蓄積期間と位置付け、原則、暗号モジュール委員会内での検討作業は行わないこととした。

3.2.2 評価用標準プラットフォームの作成

暗号モジュール委員会では、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、暗号モジュールへの非破壊攻撃及び破壊攻撃に対する評価基準の検討を行っている。

昨年度、耐タンパー性に関する標準化調査研究委員会では、電力解析攻撃のための汎用 8 ビットCPUを用いた評価用標準プラットフォーム仕様を策定し、INSTACの委託先が本

[27] http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
http://www2.nict.go.jp/ns/s801/102/index.html

仕様にもとづいた評価ボード(INSTAC-8 準拠評価用標準プラットフォーム)を作成し、電力解析の実証実験を行った。なお、その報告書は、INSTACのホームページ上に公開されている[28]。

INSTAC-8 準拠評価用標準プラットフォームを用いた電力解析の実証実験は１社のみの実施であったため、暗号モジュール委員会では、評価基準の検討には複数の実証実験データの収集が必要との判断から、今年度、本プラットフォームを INSTAC の委託先より入手し、委員への配布を行い、現在、実証実験データの収集をお願いしているところである。

また、今年度、耐タンパー性に関する標準化調査研究委員会では、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に､暗号モジュール委員会にて昨年度策定した FPGA を用いた評価用標準プラットフォーム仕様を加えた評価用標準プラットフォーム仕様を策定した。INSTAC の委託先が本仕様にもとづく評価ボード(INSTAC-32 準拠評価用標準プラットフォーム)を作成し、電力解析の実証実験を行っている。

暗号モジュール委員会では、この INSTAC-32 準拠評価用標準プラットフォームを今年度中に入手し、委員への配布を行うべく、INSTAC の委託先との調整を実施してきたが、今年度中の入手が困難な状況となり、現在、2005 年 6 月以降に入手できるよう、再度調整を進めているところである。

3.2.3 暗号モジュールに対する攻撃に関する研究動向

従来の暗号アルゴリズムに対する攻撃の研究は、利用できるデータを暗号処理の入出力である平文と暗号文や、公開鍵暗号の公開鍵に限定した。しかし、実際の暗号の利用形態である暗号モジュールでは、その物理的特性から、暗号処理において内部状態の情報が漏洩し、鍵などの秘密情報が推定される可能性がある。

暗号モジュール委員会では､暗号モジュールを動作させた時の実行時間や消費電力量等、外部から観測することにより得られる情報のみを用いて、秘密情報を取り出すような攻撃を非破壊攻撃、暗号モジュールを包んでいるパッケージ等をレーザや薬品などで破壊し、暗号モジュール内部の回路を露出させ、秘密情報を取り出すような攻撃を破壊攻撃として区別している。また、非破壊攻撃はサイドチャネル攻撃とも呼ばれている。

暗号モジュールへの非破壊攻撃及び破壊攻撃に関する研究が発表された今年度の学会等では、サイドチャネル攻撃、特に電力解析に注目が集まっていた。電力解析は、暗号モジ

[28] 「耐タンパー性に関する標準化調査研究開発　第一部 」､「耐タンパー性に関する標準化調査研究開発　第二部」, http://www.jsa.or.jp/domestic/instac/index.htm

ュールで消費される電力や入出力データから、鍵を推定する攻撃法であり、個々の電力消費パターンから直接、鍵を推定する SPA(単純電力解析)と電力消費パターン間の差分を利用する DPA(差分電力解析)が代表的である。IC カード（スマートカード）に対して、特に注意を払う必要のある攻撃である。

電力解析以外のサイドチャネル攻撃としては、暗号モジュールに対する意図的な誤動作を利用するフォールト・ベース攻撃や、平文(入力)と処理速度の関係を利用するタイミング攻撃などが研究されている。従来なかったものとしては、Shamirらが提案した暗号化処理の際に発生する音波を利用する音響攻撃やディスプレー、ケーブル等から発生する電磁波を介した情報漏えいに関する技術、いわゆるTEMPEST[29]等がある。

暗号モジュールへの非破壊攻撃及び破壊攻撃に関する研究が発表された今年度の学会は以下の通りである。

（１）ASIACRYPT 2004

Asiacrypt は、IACR が主催する 3 大会議の一つで、毎年、年末にかけてアジアで開催される。ASIACRYPT 2004 では、Kunz-Jacques らが DES の実装に対する Davies-Murphy Power Attack を提案した[1]。この攻撃法の元になった Davies-Murphy 攻撃は、DES の隣り合う S-box が入力 2 ビットを共有し、出力が独立でない性質を利用して鍵を推定する攻撃法であり、提案は差分解読や線形解読より古い。オリジナルの Davies-Murphy 攻撃には平文を必要としない長所があったが、今回の提案では、これに電力解析を組み合わせることで、平文に加え、暗号文も不要になった。この結果、攻撃が可能となる条件は大幅に緩和された。提案者の実験結果では、従来の電力解析に対する防御策のほとんどが無効だとしており、その有効性は大きく、注目されている。

（２）CHES 2004

CHES 2004 は暗号のハードウェアと組込みシステムに特化したワークショップで、採択 32 件中、Side Channel 攻撃に関するものが 15 件と約半数あった。この中で、電力解析に関する最も重要な発表は Waddle らによる改良型 2 次(2nd)DPA の提案で、DPA 対策を施した実装に対する攻撃を可能にしており、今年の論文賞を受賞している。電力解析ではこの他に、通常の DPA で利用しているハミング距離の代わりに消費電力とハミング距離の共分散を利用することで攻撃能力を高めた Brier らによる Correlation Power Analysis の発表が注目された。DPA 以外では、Collision Attack 及び、Fault Attack に関して重要な発表があった。Collision Attack は、暗号処理の

[29] Transient Electromagnetic Pulse Surveillance Technology

中間出力が一致するとき(Collision)、ハミング重みの差がゼロになることに注目した攻撃法である。Ledig らによる発表では、DES の第 1 ラウンド通過後の Collision を利用して雑音の影響を抑えることで Collision 発生を正確に特定できることが示された[5]。Fault Attack は、電源ラインへのグリッチ重畳やチップ表面へのレーザ光照射といった物理的刺激を暗号モジュールに加えることで誤動作を引き起こし、正常動作との出力の違いから鍵を推定する攻撃法である。 Hoch らは LFSR を利用したストリーム暗号に対する攻撃結果について発表した[6]。また、Hemme は Triple DES に対する攻撃で、通常、第 1 ラウンドの鍵だけを推定していたのを、第 2、第 3 ラウンドの鍵も正しく推定することに成功した[7]。

（3）EUROCRYPT 2004

EUROCRYPT 2004 のランプセッションでは、Tromer らが、PC 上でソフトウエア実装した RSA の動作時に発生する音の波形によって鍵の違いを区別できることを紹介した[8]。

Bernstein は私的な Web サイトで従来より現実的なキャッシュ・タイミング攻撃の提案した論文を掲載している[9]。従来のキャッシュ・タイミング攻撃では、平文の入力ごとにキャッシュのクリアを行う必要があった。Bernstein は、暗号処理以外のプロセスでキャッシュ・メモリ上のデータが書き換わるため同等の効果があり、明示的なクリアは必要でないと考え、実験によりその有効性を確認した。

（4）ISEC 研究会及び CSS 2004

7 月の ISEC 研究会では、三菱電機(株)が自ら開発した電力解析等のための FPGA を用いた評価ボード(SCAPE)とそれを利用した解析・防御技術に関する発表 [10-12]、INSTAC からの委託で（株）東芝が自ら開発した汎用 8bit-CPU を用いた評価用標準プラットフォーム（INSTAC-8 準拠評価用標準プラットフォーム）で行った実験結果に関する発表[40]等が報告された。また、7 月と 9 月の ISEC 研究会、10 月の CSS 2004 では、電力解析モデルの提案とその評価が現れた[10,16,31,42]。これらの研究動向も注視する必要がある。2005 年 3 月の ISEC 研究会でもこれらの研究に関連した 3 件の発表が予定されている[44-46]。

（5）SCIS 2005

2005 年 1 月に開催された SCIS 2005 では、サイドチャネル攻撃に関する 4 つのセッションが設けられなどサイドチャネル攻撃に関する研究が活発化したことを示している。サイドチャネル攻撃以外のセッションでの発表も含め、サイドチャネル攻撃および耐タンパー技術に関連した発表が 21 件あった。内訳は、解析・評価関連 2 件、対策法提案 7 件、解析結果報告 4 件、解析手法の提案 6 件および解析モデル 2 件となっている[19-39]。

（６）PKC 2005

故障解析の分野では、2005 年 2 月に開催された PKC 2005 において、スマートカードに実装された DSA 署名に対して、フランスの Naccache-Nguyen- Tunstall-Whelan らは電気的刺激を加えることにより、署名鍵を実際に求める(公開されているものとしては最初の)実験が報告された[47]。DSA 署名アルゴリズムで使用する乱数 k の値を電気的刺激で制御することによって、k の最上位バイトを実際に 0 に制御し、署名を計算させることによって、出力された署名に対して Howgrave-Graham Smart の Lattice を用いた攻撃法を適用して署名鍵を求めている。

（７）集積回路研究専門委員会(ICD)

平成16年9月に開催された電子情報通信学会 集積回路研究専門委員会(ICD)において、LSI 動作解析研究会の活動成果が報告された[13-15]。

LSI 動作解析研究会は、電子情報通信学会の時限研究会であり、主として、LSI の解析技術に関する調査研究を行っている。この LSI 解析技術は、IC カード等の破壊攻撃技術にも流用が可能である。

今年度の LSI 動作解析研究会は、現状の故障解析技術を用いた破壊攻撃を整理した上で、攻撃対象に応じた解読困難度のランク付けの検討等が行われた。ここで言う故障解析技術とは、暗号研究におけるフォールト・ベース攻撃とは異なり、LSI の実装における故障箇所を、配線の切断・つなぎかえ等の技術を駆使して特定する技術を意味する。

参考文献

[1] S. Kunz-Jacques, F. Muller, and F. Valette. “The Davies-Murphy Power Attack”, ASIACRYPT 2004, LNCS, No.3329, pp.451-467, 2004.
[2] J. Waddle and D. Wagner. “Towards Efficient Second-Order Power Analysis”, CHES 2004, LNCS, No.3156, pp.1-15.
[3] E.Brier, C.Clavier, and f.Olivier. “Corellation Power Analysis ”, CHES 2004, LNCS, No.3156, pp.16-29.
[4] S.B. Ors, E. Oswald, and B. Preneel. “Power-Analysis Attacks on an FPGA : First Experimental Results”, CHES 2004, LNCS, No.3156, pp.30-44.
[5] H. Ledig, F. Muller, and F. Valette. “Enhancing collision Attacks”, CHES 2004, LNCS, No.3156, pp.176-190.
[6] J.J. Hoch and A. Shamir. “Fault Analysis of Steam Ciphers”, CHES 2004, LNCS, No.3156, pp.240-253.
[7] L. Hemme. “A Differential Fault Attack against Early rounds of (Triple) DES”, CHES 2004, LNCS, No.3156, pp.254-267.
[8] E. Tromer and A. Shamir. “On Nosy People and Noisy Machines”, Eurocrypt Rump Session, http://www.zurich.ibm.com/eurocrypt2004/rump.html , http://www.wisdom.weizmann.ac.il/~tromer/acoustic/ .
[9] D.J. Bernstein. “Cache-timing attacks on AES”, D.J.Bernstein's home page, http://cr.yp.to/antiforgery.html#cachetiming .
[10] 佐伯、鈴木、市川.“論理シミュレーションによる DPA 評価とリークモデルの構築”, 電子情報通信学会技術研究報告, vol.104, no.200, ISEC2004-57, pp. 111-118, 2004 年 7 月.
[11] 市川、鈴木、佐伯.“データマスクを利用した DPA 対策に対する攻撃”, 電子情報通信学会技術研究報告, vol.104, no.200, ISEC2004-58, pp.119-126, 2004 年 7 月.
[12] 鈴木、佐伯、市川.“遷移確率を考慮した DPA 対策手法の提案”, 電子情報通信学会技術研究報告, vol.104, no.200, ISEC2004-59, pp.127-134, 2004 年 7 月.
[13] 中島蕃、柴田直、山岸篤弘、松本勉“集積回路のセキュリティ:故障解析技術を用いた攻撃に対する耐性(I) - 故障解析技術からみた LSI の耐タンパー性 -”, 電子情報通信学会技術研究報告, vol.104, no.288, ICD2004-105, pp.47-52, 2004 年 9 月.
[14] 中島蕃、柴田直、山岸篤弘、松本勉“集積回路のセキュリティ:故障解析技術を用いた攻撃に対する耐性(II) - LSI の耐タンパー性向上技術 -”, vol.104, no.288, ICD2004-106, pp.53-58, 2004 年 9 月.
[15] 中島蕃、柴田直、山岸篤弘、松本勉.“集積回路のセキュリティ:故障解析技術を用い

た攻撃に対する耐性（III） - 代表的なサイド攻撃とこれに必要なリソースおよびスキル - ”，vol.104，no.288，ICD2004-107，pp.59-63，2004 年 9 月.
[16] 渡邊高志，神永正博，遠藤隆，大河内俊夫，"論理シミュレーションによる耐タンパー性評価システムの検討"，Computer Security Simposium 2004(CSS2004)予稿集，8C-4，2004 年 10 月
[17] 森岡澄夫，秋下徹，"合成体を用いた AES S-Box 回路に対する DPA 攻撃"，Computer Security Simposium 2004(CSS2004)予稿集，9C-2，2004 年 10 月
[18]小池正修，松本勉，"剰余演算系基底のランダム選択手法に対する電力解析"，Computer Security Simposium 2004(CSS2004)予稿集，9C-4，2004 年 10 月
[19] 松永明，四方順司，松本勉，"テーブルネットワーク型暗号実装ソフトウェアの耐タンパー性評価法"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，1E2-4，2005 年 1 月
[20] 小黒博昭，飯野徹，平井康雅，箱守 聰，"White-box 攻撃に対する耐性を向上させた多倍長演算の実装"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，1E2-5，2005 年 1 月
[21] 伊藤孝一，伊豆哲也，武仲正彦，"ランダム化初期点を用いた電力解析対策法について(その３)"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，2D1-1，2005 年 1 月
[22] C. Vuillaume，K. Okeya，T.Takagi，"Security Analysis of OT Scheme"，2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，2D1-1，2005 年 1 月
[23] 高島克幸，"格子基底縮小アルゴリズムを用いた (EC)DSA へのサイドチャネル解析について"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，2D1-3，2005 年 1 月
[24] 小池正修，松本勉，"Gauss のアルゴリズムを利用する RNS モンゴメリ乗算に対する電力解析"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，2D1-4，2005 年 1 月
[25] D. G. Han，D. Yang，J. Lim，K. Sakurai，"DPA on Hybrid XTR Single Exponentiation"，2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，2D2-1，2005 年 1 月
[26] 一色寿幸，辻原悦子，峯松一彦，角尾幸保，"A5/1 に対するサイドチャネル攻撃"，2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，2D2-2，2005 年 1 月
[27] 佐々木明彦，阿部公輝，太田和夫，"暗号回路の耐タンパー性評価手法の構築"，2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，2D2-3，2005 年 1 月
[28] 内藤祐介，指田岳彦，根岸大宙，太田和夫，國廣昇，"TOYOCRYPT への故障利用攻撃"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，2D2-4，2005 年 1 月
[29] 酒井康行，櫻井幸一，"楕円曲線暗号のための剰余算に対するサイドチャネル解析"，2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，3D4-4，2005 年 1 月
[30] 三宅秀享，野崎華恵，清水秀夫，新保淳，"SBOX の特性を利用した DPA 評価手法"，

2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，4E1-1，2005 年 1 月
[31] 佐伯 稔，鈴木大輔，市川哲也,"CMOS 論理回路の電力解析モデル"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，4E1-2，2005 年 1 月
[32] 市川哲也，鈴木大輔，佐伯稔,"FPGA を用いた電力解析モデルの検証"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，4E1-3，2005 年 1 月
[33] 鈴木大輔，佐伯稔，市川哲也，"RSL の安全性評価とハイブリット DPA に対する改良"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，4E1-4，2005 年 1 月
[34] 池田尚隆，市川武宜，金子 敏信，"SEED に対するキャッシュ攻撃"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，4E1-5，2005 年 1 月
[35] Y. Sasaki, C. Fidge, "Security Information Flow Analysis for Data Diode with Embedded Software", 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，4E2-1，2005 年 1 月
[36] 山口晃由，佐藤恒夫，山田敬喜，"マスク付き入力の多項式展開によるガロア体上の逆元演算マスク法"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，4E2-2，2005 年 1 月
[37] 田中秀磨，滝澤修，山村明弘，"Tempest fonts の安全性に関する一考察"，2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，4E2-3，2005 年 1 月
[38] 秋下徹，高木剛，"剰余平方算処理の電力差分を利用した楕円曲線暗号に対する DPA 攻撃"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，4E2-4，2005 年 1 月
[39] D. G. Han, K. Okeya, T. H. Kim, Y. S. Hwang, Yong Ho Park, "Side Channel Attacks on the Countermeasures Using Randomized Binary Signed Digits"， 2005 年暗号と情報セキュリティシンポジウム(SCIS2005)予稿集，4E2-5，2005 年 1 月
[40]藤崎浩一，友枝裕樹，三宅秀享，駒野雄一，新保　淳，川村信一，"8bitCPU を対象とした電力解析用評価環境の開発と実証実験"，電子情報通信学会技術研究報告，vol.104，no.200，ISEC2004-55，pp.　95-102 ，2004 年 7 月.
[41]DongGuk Han, Jongin Lim, ,kouichi, Sakurai, "Side Channel Attacks on XTR and Efficient Countermeasures"，電子情報通信学会技術研究報告，vol.104，no.200，ISEC2004-56，pp. 103-110 ，2004 年 7 月.
[42] 清水秀夫，"マスク論理素子を使ったサイドチャネル攻撃対策"，電子情報通信学会技術研究報告，vol.104，no.315，ISEC2004-69，pp. 15-20 ，2004 年 9 月.
[43]小池正修，松本勉，"RNS 表現に基づくべき乗剰余算に対するサイドチャネル解析"，電子情報通信学会技術研究報告，vol.104，no.53，ISEC2004-7，pp. 43-50 ，2004 年 9 月.
[44]池田尚隆，市川武宜，金子敏信，"SEED に対するキャッシュ攻撃の一考察"，電子情報通信学会技術研究報告，2005 年 3 月（発表予定）.
[45]高橋芳夫，福永利徳，大塚浩昭，神田雅透，"CPU ボード上のブロック暗号に対するサイドチャネル攻撃"，電子情報通信学会技術研究報告，2005 年 3 月（発表予定）.

[46]間宮英世，宮地充子，"固定ハミングウェイト表現による SPA 対策法"，電子情報通信学会技術研究報告，2005 年 3 月（発表予定）．
[47]D. Naccache, P. Nguyen, M. Tunstall, C. Whelan, "Experimenting with Faults, Lattices and the DSA", Public Key Cryptography - PKC 2005, LNCS, No.3386 , pp.16-28, Feb, 2005.