CRYPTREC Report 2009

平成 22 年 3 月

独立行政法人情報通信研究機構
独立行政法人情報処理推進機構

「暗号実装委員会報告」

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実装委員会の 2009 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きた。

本年度は「電子政府推奨暗号リスト」の改訂に対応するため、暗号モジュール委員会は暗号実装委員会に移行し、暗号監視委員会を継承した暗号方式委員会とともに「電子政府推奨暗号リスト改訂のための暗号技術公募 (2009 年度)」を行い、計 6 件の応募を受けた。

暗号実装委員会では公募実施と並行し、応募暗号に対する実装性能評価とサイドチャネル攻撃対策の実施可能性検証の詳細について検討を行った。

暗号実装委員会の下に置かれたサイドチャネルセキュリティワーキンググループ(WG)は 2008 年度までの電力解析実験 WG の活動を引き継ぎ、米国 FIPS 140-3 をベースとしたドラフト 1st WD ISO/IEC 19790 を検討してコメント案を作成、国内 SC27/WG3 小委員会経由で国際事務局に提案するとともに、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。

本委員会の活動が、わが国における電子政府推奨暗号リストの改訂作業と暗号実装関連技術の研究の進展に寄与できれば、幸いである。

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。

2010 年 3 月

暗号実装委員会　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[1]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章には暗号実装委員会の活動の背景と目的、第2章には暗号実装委員会の活動内容と成果概要、第3章には暗号実装委員会の委員会開催状況を記述した。

2008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

[1] GPKI：Government Public Key Infrastructure（政府認証基盤）

委員会構成

暗号実装委員会は、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。

暗号実装委員会では、ISO[2]/IEC[3]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。

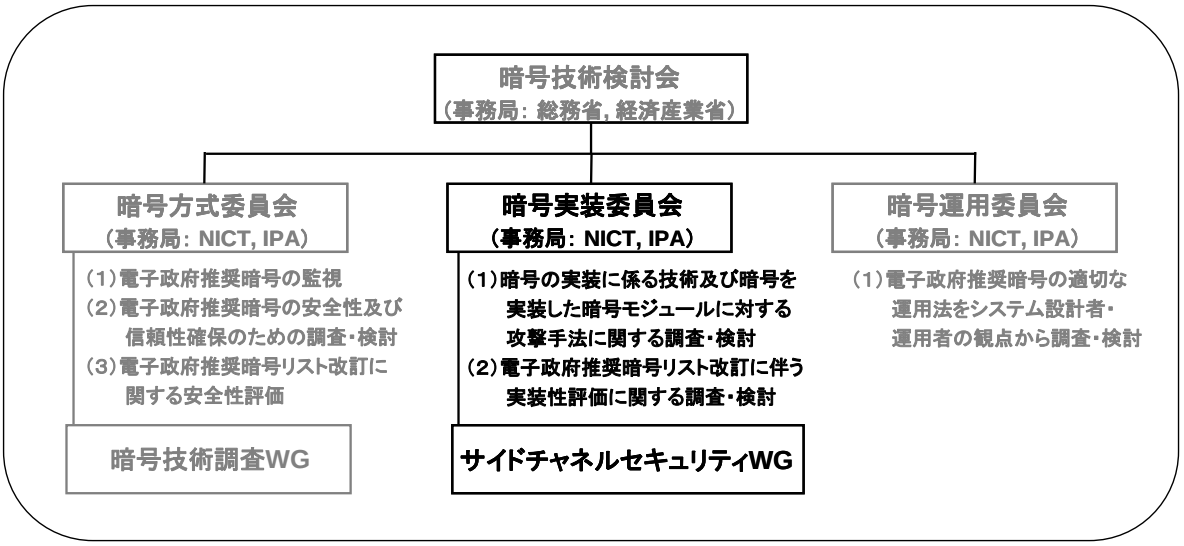


図１　2009 年度の CRYPTREC の体制

[2] ISO：International Standard Organization
[3] IEC：International Electrotechnical Commission

委員名簿

暗号実装委員会 （2010 年 3 月現在）

委員長	松本　勉	国立大学法人横浜国立大学　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	亀田　繁	財団法人日本情報処理開発協会　センター長
委員	崎山　一男	国立大学法人電気通信大学　准教授
委員	佐藤　証	独立行政法人産業技術総合研究所　研究チーム長
委員	佐藤　恒夫	三菱電機株式会社　チームリーダ
委員	清水　秀夫	株式会社東芝　研究主務
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	鳥居　直哉	株式会社富士通研究所　部長
委員	福永　利徳	日本電信電話株式会社　研究主任
委員	本間　尚文	国立大学法人東北大学　准教授
委員	松崎　なつめ	パナソニック株式会社　チームリーダ
委員	渡辺　大	株式会社日立製作所　研究員

オブザーバ

氏原　正勝	警察庁　情報通信局（2009 年 10 月まで）
赤澤　康之	警察庁　情報通信局（2009 年 10 月から）
伊東　信孝	警察大学校　警察情報通信研究センター
松本　和人	総務省　行政管理局
荻原　直彦	総務省　情報通信国際戦略局（2009 年 8 月まで）
島田　淳一	総務省　情報通信国際戦略局（2009 年 8 月から）
古賀　康之	総務省　情報通信国際戦略局（2009 年 8 月から）
梶原　亮	総務省　情報通信国際戦略局
齊藤　修啓	総務省　情報通信国際戦略局
東山　誠	外務省　大臣官房（2009 年 8 月まで）
荒木　美敬	外務省　大臣官房（2009 年 8 月から）
山元　明裕	外務省　大臣官房（2009 年 9 月まで）

森田　信輝　　経済産業省　産業技術環境局（2009 年 8 月まで）
山中　豊　　経済産業省　産業技術環境局（2009 年 8 月から）
黒田　俊久　　経済産業省　商務情報政策局
下里　圭司　　経済産業省　商務情報政策局
池西　淳　　経済産業省　商務情報政策局
千葉　修治　　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（2009 年 9 月まで）
坂下　圭一　　防衛省　運用企画局（2009 年 9 月から）
滝澤　修　　独立行政法人　情報通信研究機構
川村　信一　　独立行政法人　産業技術総合研究所
青木　林　　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
山田　安秀(2009 年 7 月まで)
矢島　秀浩(2009 年 7 月から)
山岸　篤弘
近澤　武
小暮　淳
星野　文学
神田　雅透（2009 年 8 月から）
大熊　建司
鈴木　幸子

独立行政法人　情報通信研究機構
篠田　陽一
田中　秀磨
松尾　真一郎
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

インターネットの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。中でも、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行われ、国民生活に浸透し始めている。また、高度情報通信ネットワーク社会推進戦略本部（ＩＴ戦略本部）の重点計画等で、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。特に、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してきた。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、暗号技術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している。また、暗号モジュール委員会では、暗号技術を実装した暗号モジュール製品（暗号製品）の安全性確保のために、暗号モジュール製品に対するセキュリティ要件とその試験方法の検討を行ってきた。

特に、暗号モジュール委員会では、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[4]（Federal Information Processing Standard） PUB[5] 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[6]） 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[7]準拠のプラットフォーム（INSTAC-8, INSTAC-32）や産業技術総合研究所情報セキュリティ研究センターが、経済産業省からの委託を受けて開発したサイドチャネル攻撃用標準評価ボード（SASEBO：Side-channel Attack Standard Evaluation BOard）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ている。

電子政府推奨暗号リストは 2013 年度までに改訂することが決まっており、2008 年度に暗号技術監視委員会において、改訂及び新設する暗号技術カテゴリーを決め公募要項の検討を行った。2009 年度には、暗号技術公募に備えるために CRYPTREC の体制を変更し、暗号技術監視委員会は暗号方式委員会に、暗号モジュール委員は暗号実装委員会に改称し、従来の活動内容を引き継ぐとともに、各々、応募暗号技術の安全性評価、及び、応募暗号技術の実装性能評価とサイドチャネル攻撃の対策可能性確認を活動目標に加えた。また、暗号モジュール委員会下の電力解析実験 WG はサイドチャネルセキュリティ WG に改称し、電力解析に限らず、電磁波解析やキャッシュタイミング攻撃などサイドチャネル攻撃一般に対象を広げることになった。

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[8]とカナダ CSE[9]が運用している

---

[4] FIPS：Federal Information Processing Standard
[5] FIPS PUB:Federal Information Processing Standards Publication
[6] INSTAC：情報技術標準化研究センター（Information Technology Research and Standardization Center）
[7] INSTAC-8/-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（-8 は 8bit 版，-32 は 32bit 版）
[8] NIST：National Institute of Standards & Technology（米国国立標準技術研究所）

CMVP[10]（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 を国際標準規格とする審議が ISO[11]/IEC[12] JTC[13]1 SC[14]27/WG[15]3 で開始されたため、2004 年度からは、規格文書の草案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FIPS 140-2の改訂版である FISP 140-3 に対する検討作業を行ってきた。

2006 年 12 月には、FIPS 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、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ことを目指している。

2009 年 7 月には、電子政府推奨暗号リストの改訂に向け、「暗号モジュール委員会」は「暗号実装委員会」に改称し、従来の活動を引き継ぐとともに、暗号技術の公募要項作成、及び、実装性能等の評価を活動目的に加えた。また、「電力解析実験ワーキンググループ」は「サイドチャネルセキュリティワーキンググループ」に改称し、調査対象を電力解析からサイドチャネル攻撃一般に拡張するとともに、FIPS 140-3 及びそれに対応する国際規格 ISO/IEC 19790 の改訂の草案に対するコメント作成作業を継承している。

1.1.2 暗号モジュール委員会／暗号実装委員会を取り巻く環境の変化

2003 年に暗号モジュール委員会が活動を開始した後、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[16])の情報セキュリティ研究センター(RCIS[17])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/IEC JTC1 SC27 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(ISO/IEC 19790)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。

2006 年度に FIPS 140-2 の次期バージョン FIPS 140-3 の作成検討が始まり、2007

---

[9] CSE：Communications Security Establishment
[10] CMVP：(Cryptographic Module Validation Program)
[11] ISO：International Standard Organization（国際標準化機構）
[12] IEC：International Electrotechnical Commission（国際電器標準会議）
[13] JTC：Joint Technical Committee（合同技術委員会）
[14] SC：SubCommittee（副委員会）
[15] WG：Working Group（ワーキンググループ）
[16] AIST：Advanced Industrial Sciens and Technology
[17] RCIS：Research Center for Information Security

年 7 月に第 1 次草案が公開、これに対するコメントを反映した改訂草案が 2009 年 12 月に公開された。この草案に対するコメントを反映して、FIPS 140-3 が制定される予定である。一方、ISO/IEC JTC1 SC27 では、2008 年 5 月に FIPS 140-3 をベースとして ISO/IEC 19790 を改訂することが決まり、2010 年 2 月に 1st WD が発表された。

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 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[18]）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。

2009 年度には、暗号モジュール委員会は電子政府推奨暗号リスト改訂に向け、暗号実装委員会に改称した。同時に、電力解析実験 WG は調査対象を電力解析からサイドチャネル攻撃一般に拡張し、サイドチャネルセキュリティ WG に改称し、FIPS 140-3 と ISO/IEC 19790 の改訂草案に対するコメント作成作業を引き継いだ。

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を暗号モジュールとよび、暗号モジュールに対して、動作の信頼性や安全性を規定した規格をセキュリティ要件と呼ぶ。この暗号モジュールに対するセキュリティ要件として、国際的な影響力を持つものには、米国及びカナダで運用されている CMVP[19]制度で用いられている FIPS 140-2 と FIPS 140-2 をベースとして国際規格となった ISO[20]/IEC[21] 19790 が存在する。

1.2.1 FIPS 140-2/140-3

FIPS 140-2 は、米国 NIST/カナダ CSE[22]が共同運用している CMVP 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

---

[18] SASEBO: 平成 18～20 年度経済産業省委託事業「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と東北大学が開発を行った、サイドチャネル攻撃実験用標準評価ボード(Side-channelAttack Standard Evaluation BOard)。

Xilinx 社製 FPGA を実装した初代 SASEBO とその改良版の SASEBO-G および SASEBO-GII、ALTERA 社製 FPGA を実装した SASEBO-B、そしてカスタム暗号 LSI を実装した SASEBO-R の 5 種類が、電力解析実験ワーキンググループの委員が所属する研究機関に対して提供され、これにより、アーキテクチャの異なるハードウェア上でのサイドチャネル攻撃実験が行える環境が整った。そこで、本ワーキンググループにおいても産総研の了承のもと、各委員がこれらの SASEBO ボードを活用した比較実験を行うこととした。

[19] Cryptographic Module Validation Program

[20] International Organization for Standardization

[21] International Electrotechnical Commission

[22] Communication Security Establishment

格の関連文書としては、試験要件(DTR[23])と運用ガイダンス(IG[24])の 2 種類がある。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 はこれら関連文書を必要に応じて適宜改訂することで、暗号モジュール試験及び認証制度を柔軟に運用している。

NIST/CSE 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 140-3 に改訂する作業を行っている。2007 年 7 月には、FIPS 140-3 の第 1 次草案が公開され、これに対するコメントを反映した改訂草案は予定よりも大幅に遅れたものの、2009 年 12 月に公開された。改訂草案に対するコメント受付は、2010 年 3 月 11 日に締め切られた。

FIPS 140-3 では、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。第 1 次草案ではセキュリティレベルを 5 段階に増やしていたが、改訂草案では FIPS 140-2 と同様、4 段階に戻っている。

1.2.2 ISO/IEC 19790 と ISO/IEC 24759

ISO/IEC 19790 は、FIPS 140-2 を基に作られた国際規格である。ISO/IEC JTC 1 SC 27/WG 3 のプロジェクトとして審議され、2006 年 3 月 1 日に発行された。

また、FIPS 140-2 に対応する試験要件(DTR)に対応した ISO/IEC 19790 に対する試験要件の標準化は、FIPS 140-2 に対応する試験要件(DTR)と運用ガイダンス(IG)をベースとして、2008 年 6 月に ISO/IEC 24759 として規格化された。

ISO/IEC 19790 は、2007 年 3 月に日本工業標準調査会(JISC[25])によって JIS[26]化され、JIS X 19790 として発行された。また、JIS X 19790 に対応する試験規格は、暗号モジュール委員会で検討してきた「暗号モジュール試験基準第 0.1 版」をベースとして、2007 年 3 月に、JIS X 5091 として発行された。しかし、ISO/IEC 24759(2008 年 6 月発行)をベースとした JIS X 24759 が JIS X 19790 に対する試験規格として 2009 年 10 月に発行されるに伴い、JIS X 5091 は廃止された。

2006 年 3 月に発行された ISO/IEC 19790 は、米国 NIST で進められている FIPS140-2 の改訂に対応し、FIPS 140-2 の後継標準となる FIPS 140-3 をベースに改訂するべく早期改訂を開始した。その後、FIPS 140-3 の改訂草案作成が大幅に遅れたため、FIPS 140-3 と ISO/IEC 19790 の改訂を並行して行うことが決まった。これに従い、ISO/IEC 19790 改訂版(2nd ed.)の 1st WD は FIPS 140-3 の改訂草案に若干遅れた 2010 年 2 月に発表され、同年 3 月 30 日にコメント受付が締め切られた。これらの草案は、両標準化団体の規約の違いを反映して編集上の差異は若干異なるものの、技術的内容は同じである。

---

[23] Derived Test Requirements
[24] Implementation Guidance
[25] JISC : Japanese Industrial Standards Committee（日本工業標準調査会）
[26] JIS : Japanese Industrial Standards（日本工業規格）

1.3 暗号実装委員会の活動状況

1.3.1 暗号モジュール委員会時代の活動

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[27]及び試験基準[28]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[29]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 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。

---

[27] 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。
[28] 2005 年度の活動で、「試験基準」は「試験要件」に変更された。
[29] Field Programmable Gate Array

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 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 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 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 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 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 の草案 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 140-2 が FIPS 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」

2007 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

FIPS 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 の最終草案を審議し、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 140-2 を FIPS 140-3 に改訂する準備を進めている。7 月 13 日に草案が発行され、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 140-2 を FIPS 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[30],Camellia,DES[31],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。

---

[30] AES：Advanced Encryption Standard（米国標準暗号）

[31] DES：Data Encryption Standard（旧米国標準暗号）

(4) FIPS 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」として作成した。

2008 年度の活動概要

(1) 電子政府推奨暗号リスト改訂のための公募要項における、ハードウェア実装及びソフトウェア実装の性能評価項目作成

電子政府推奨暗号リスト改訂のための「暗号技術公募要項（2009 年度）（案)」作成において暗号技術検討会の依頼を受け、応募暗号の実装性能に関する第一次評価と第二次評価の評価項目を作成した。

(2) 暗号モジュールに対するサイドチャネル攻撃の監視と分析

監視要員による国内外で開催された会議等への出席により、最新情報を収集し、監視委員会にて報告を行い、情報を共有した。

(3) 電力解析実験ワーキンググループよる実験

サイドチャネル解析用プラットフォームの仕様である INSTAC-8/-32 仕様に準拠したボードや SASEBO ボード等を用いた比較実験を依頼した結果、電力解析実験ワーキンググループから以下の項目に関する報告が提出された。

1．サイドチャネル攻撃に関する比較実験
2．採取データの形式の統一化
3．実験データの標準評価方法の検討
4．電力解析攻撃実験のための評価ボードを利用した研究の調査
5．今後の検討項目

1.3.2 2009 年度の活動概要

2009 年度暗号実装委員会の成果

今年度の暗号実装委員会の主要成果としては、次の 3 つが挙げられる。

(1) 電子政府推奨暗号リスト改訂のための公募評価における、ハードウェア実装及びソフトウェア実装の性能評価の詳細検討

応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術に対するハードウェア及びソフトウェア実装性評価の実装環境及び必要とされる実装性能の基準を決定した。具体的には次の項目の基本線を決定した。

・ソフトウェア及びハードウェア実装性能評価ツールに関する仕様
・実装性能評価のための実装用インタフェース仕様
・ソフトウェア及びハードウェア実装性能評価の評価項目、評価手法、評価結果の判断基準

(2) 電子政府推奨暗号リスト改訂のための公募評価における、サイドチャネル攻撃耐性の評価の詳細検討

応募暗号技術及び現行の電子政府推奨暗号リスト掲載暗号技術のサイドチャネル攻撃耐性に関する評価項目、評価手法の検討及びそのためのソフトウェア/ハードウェア実装要件の検討を行い、暗号方式委員会と連携して、基本方針を決定した。

(3) 暗号モジュールのセキュリティ要件 ISO/IEC 19790 等、標準化への協力

FIPS 140-3 の改訂草案が 2009 年 12 月に、これに対応する国際規格 ISO/IEC 19790 早期改訂の草案 1st WD が 2010 年 2 月に公開された。これに対応し、サイドチャネルセキュリティ WG においてこれらの文書を検討し、1st WD 19790 に対するコメントを作成し、松本委員長が ISO/IEC JTC1 SC27/WG3 国内小委員会に対して提出した。提案コメントは、SC27/WG3 小委員会に提案された他のコメントとして国際事務局に提出された。

(4) 暗号モジュールへの攻撃の監視と分析

監視要員による国内外で開催された会議等への出席により、最新情報を収集し、監視委員会にて報告を行い、情報を共有した。

第 2 章　2009 年度の活動内容と成果概要

2.1　電子政府推奨暗号リスト改訂のための公募評価における、ハードウェア実装及びソフトウェア実装評価の詳細検討

2.1.1　実装性評価の概要

電子政府推奨暗号リスト改訂のための公募評価における、実装性に関わる評価について 2008 年度の暗号モジュール委員会で検討した結果の概要を図 2.1 に示す。今年度は、「ソフトウェア処理性能評価」、「ハードウェア処理性能評価」、「サイドチャネル攻撃耐性評価」の詳細を決定すべく検討を行った。

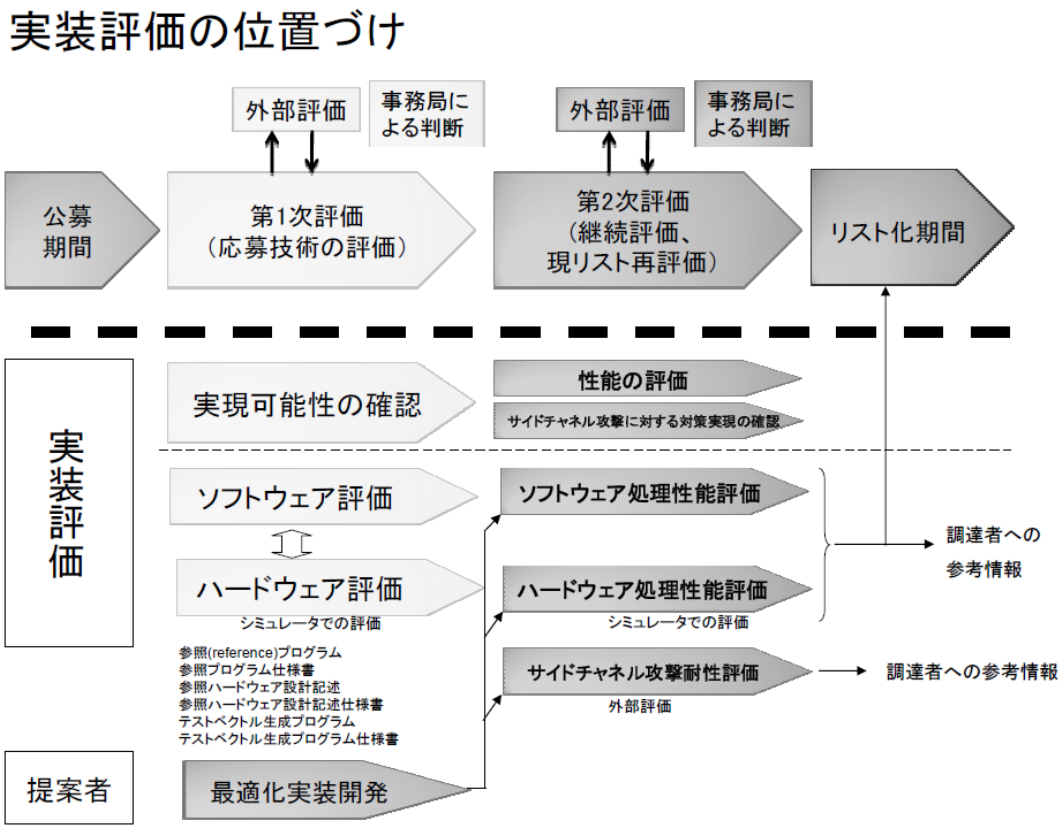


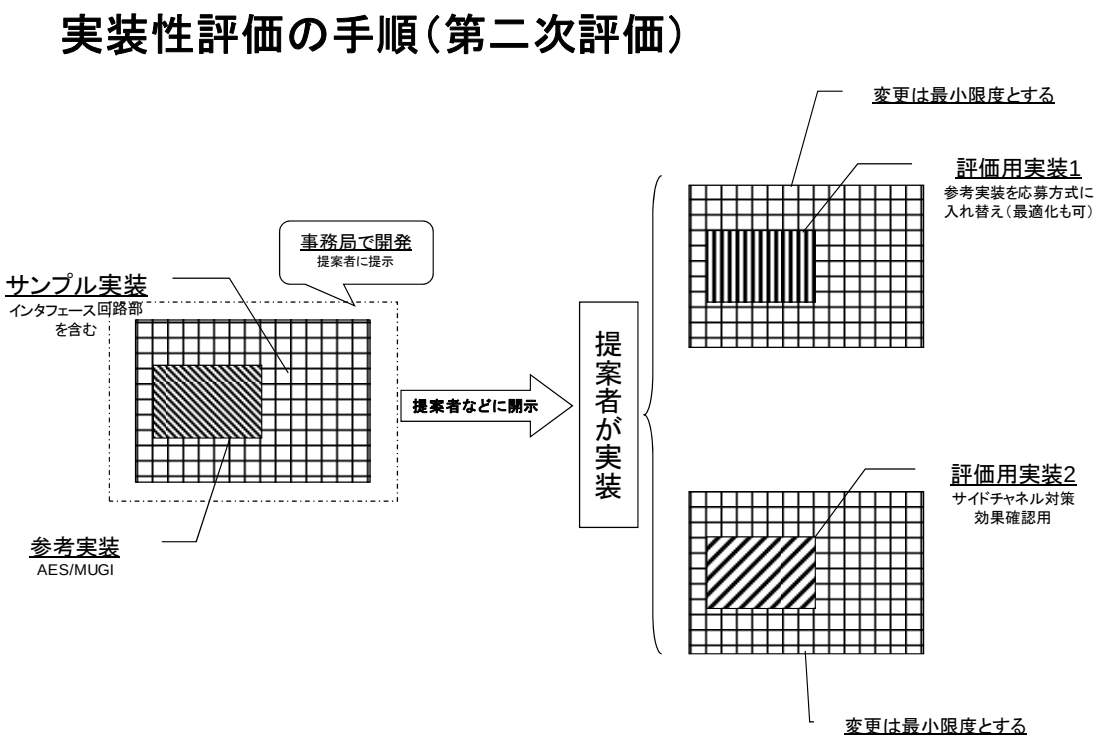
図 2.1　実装性評価の位置づけ

2.1.2　実装性評価の詳細

2009 年度は、2008 年度に引き続き、以下の事項について検討を行った。

ア　実装性評価の方法

・ 図 2.2 に第二次評価での実装性評価の実施手順に関するイメージを示す。



・ 図 2.2　実装性評価の手順

・ 事務局は図 2.2 の左に示したサンプル実装を開発し、暗号技術応募者に提示する。

・ サンプル実装は、暗号アルゴリズム・コアとしての現電子政府推奨暗号リストに記載されているブロック暗号 AES とストリーム暗号 MUGI を参考実装と、インターフェース（回路）とで構成される。

・ 応募者は参考実装の部分を応募暗号技術で書き換えた評価用実装を作成し、事務局に提出する。

・ 評価用実装には処理性能を評価するための評価用実装１（ハードウェア／ソフトウェア両方）とサイドチャネル攻撃対策を施した評価用実装２（ハードウェアのみ）の２種類があり、インターフェースの部分は必要最小限の変更を許すものとする。

・ 事務局は参考実装の開発を外部に委託する。委託先が開発するのは次の通り。

(1)参考実装（デファクト暗号を例としたソースコードとインターフェース）

(2)処理性能評価ツール

(3)実装性能評価ツール

イ　実装性評価環境

・ ソフトウェア評価

Intel x86 CPU + MS-Windows XP（バージョンは状況に応じて変更する）

・ ソフトウェア評価

Xilinx Virtex-5 LX30/LX50(SASEBO-GⅡ搭載の FPGA) + ISE WebPACK

ウ　処理性能評価基準

(i)スピード／処理性能、サイズの２つを基本とする。

(ii)ハードウェア評価

(1)処理速度(スループット)は I/F に依存するので、critical path 遅延とサイクル数に置き換える。

(2)実装での I/F の書き換えは認めるが、書き換える範囲は限定する。

(3)実装方針の説明にアーキテクチャを書かせる。

(4)記述のレベル（マクロ／ミクロ）は今後検討する。

(5)情報公開は CRYPTREC 委員会の席上で確認。

(6)

(iii) ソフトウェア評価

(1)処理速度と使用リソース利用を評価基準とする。

(2)参考用実装を公開するか否かは継続検討とする。

(iv)性能評価の比較の基準とする暗号技術

(1) 処理速度と使用リソース利用を評価基準とする。

エ　サイドチャネル攻撃に対する対策実現の確認

(i)スピード／処理性能、サイズの２つを基本とする。

(ii)評価対象のカテゴリーは、ブロック暗号およびストリーム暗号とする。

(iii) 応募者に、サイドチャネル攻撃対策を組み込んだ実装情報の提供を求める。

・

2.2　サイドチャネル攻撃のセキュリティ要件の検討

FIPS 140-3 の改訂草案が 2009 年 12 月に、これに対応する国際規格 ISO/IEC 19790 早期改訂の草案 1st WD が 2010 年 2 月に公開された。これに対応し、暗号実装委員会の下に設置したサイドチャネルセキュリティ WG においてこれらの文書を検討して 1st WD 19790 に対するコメントを作成、暗号実装委員会での承認を経て、松本委員長が ISO/IEC JTC1 SC27/WG3 国内小委員会に対して提出した。提案コメントは、SC27/WG3 小委員会に提案された他のコメントとして国際事務局に提出された。

2.3 暗号モジュールへの攻撃の監視と分析

暗号実装委員会に関連する活動として、2009 年度も CHES[32]および FDTC[33]等に参加し、情報収集を行い、国際会議等の報告として暗号方式委員会に監視状況の報告を行った。

2009 年度の監視状況は、CRYPTREC Report 2009 の、「暗号技術監視委員会報告」付録 4 学会等での主要論文発表一覧、としてまとめた。

2.4 2009 年度サイドチャネルセキュリティワーキンググループの活動

2.4.1 活動目的

暗号モジュールへのサイドチャネル攻撃は、特に IC カードのようなワンチップモジュールにとっては大きな脅威となる。サイドチャネル攻撃の中でも、暗号モジュールの消費電力を計測することで、鍵情報を推定する電力解析攻撃（DPA[34]攻撃、SPA[35]攻撃、タイミング攻撃等）は、簡便な攻撃環境・リソースで実現することが可能となるため、今後対策の実施が必須となると考えられる。

しかし、サイドチャネル攻撃に対するセキュリティ要件や試験要件は現在作成途上にある。

そこで、サイドチャネルセキュリティワーキンググループでは、実験データを収集・分析し、サイドチャネル攻撃に対するセキュリティ要件、試験要件の検討に資することを目的としている。

2.4.2 今年度の成果概要

本ワーキンググループの前身である平成 18 年度に設置された電力解析実験ワーキンググループのときから、実験用標準評価ボード等に搭載された暗号モジュールについて、電力解析攻撃に関する実験方法と、標準的な試験方法と、安全性の基準の検討を行ってきた。産業技術総合研究所と東北大学が開発した実験用評価ボード SASEBO（Xilinx 版）の利用に加え、平成 20 年度は、新たに FPGA を搭載した SASEBO-G（Xilinx 版）[36]と ASIC[37]を搭載した SASEBO-R（LSI 版）[38]等が開発された。平成 21 年度には、SASEBO-G の FPGA

---

[32] CHES：Workshop on Cryptographic Hardware and Embedded Systems（International Association for Cryptologic Research(IACR)）

[33] FDTC：WORKSHOP ON FAULT DIAGNOSIS AND TOLERANCE IN CRYPTOGRAPHY

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

[35] SPA：Simple Power Analysis（単純電力解析）

[36] SASEBO-G：SASEBO-G は SASEBO の改良版で Xilinx 社の Virtex-II Pro FPGA である xc2vp7 と xc2vp30 を搭載したサイドチャネル攻撃実験用標準評価ボード。

[37] ASIC：Application Specific Integrated Circuit

[38] SASEBO-R：TSMC 社の 130nm CMOS ライブラリによって製造された、専用暗号 LSI を搭載した ASIC 版のサイドチャネル攻撃実験用標準評価ボード。ASIC には、6 種類の AES 暗号モジュール（①合成体（暗号化

を Virtex-5 LX30/50 バージョンアップし、ロジック容量の増加などの機能追加を行った SASEBO-GII が開発・製品化された。今年度も昨年度に続き、これらの SASEBO シリーズを中心とするサイドチャネル評価用標準プラットフォームを使ったサイドチャネル攻撃及び防御法に関する実験データの収集を行った。

また、暗号実装委員会からの依頼を受け、暗号モジュールのセキュリティ要件に関する国際規格 ISO/IEC 19790 の早期改訂文書 1st WD に対する日本コメントの作成に寄与した。

(1) 暗号モジュールのセキュリティ要件等の標準化に対する貢献

FIPS 140-3 の改訂草案が 2009 年 12 月に、これに対応する国際規格 ISO/IEC 19790 早期改訂の草案 1st WD が 2010 年 2 月に公開された。これに対応し、暗号実装委員会からの依頼により、これらの文書を検討して 1st WD に対するコメントを作成、暗号実装委員会での承認を経て、松本委員長が ISO/IEC JTC1 SC27/WG3 国内小委員会に対して提出した。提案コメントは、SC27/WG3 小委員会に提案された他のコメントとして国際事務局に提出された。

(2) 電力解析攻撃実験のための評価ボードを利用した研究の調査

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 情報科学研究科が開発したサイドチャネル攻撃実験用標準評価ボード（SASEBO）等を使用した、電力解析実験ワーキンググループの委員による、2009 年度の発表についてまとめた。

/復号実装），②合成体（暗号化のみ実装），③CASE 文記述（暗号化のみ実装），④AND-XOR1 段（暗号化のみ実装），⑤AND-XOR3 段（暗号化のみ実装），⑥①の FPGA 用ネットリストを使用）と DES, MISTY-1, Camellia，SEED，CAST128，RSA(1024bit)の暗号モジュールを実装している。

2.4.3　委員構成

サイドチャネルセキュリティワーキンググループ （2010 年 3 月現在）

主査	松本　勉	国立大学法人横浜国立大学　教授
委員	黒川　恭一	防衛大学校　教授
委員	崎山　一男	国立大学法人電気通信大学　准教授
委員	佐藤　証	独立行政法人産業技術総合研究所　研究チーム長
委員	佐伯　稔	三菱電機株式会社　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	田中　秀磨	独立行政法人情報通信研究機構　主任研究員
委員	角尾　幸保	日本電気株式会社　主席研究員
委員	鳥居　直哉	株式会社富士通研究所　部長
委員	深澤　宏	NEC マイクロシステム株式会社　主任
委員	藤崎　浩一	株式会社東芝　研究主務
委員	渡辺　大	株式会社日立製作所　研究員
委員	本間　尚文	国立大学法人東北大学　准教授
委員	山越　公洋	日本電信電話株式会社　研究主任

事務局

独立行政法人　情報処理推進機構

山岸　篤弘
近澤　武
神田　雅透
大熊　建司
鈴木　幸子

独立行政法人　情報通信研究機構

松尾　真一郎
黒川　貴司
金森　祥子

2.4.4　サイドチャネル攻撃実験のための評価ボードを利用した研究の調査

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開発したサイドチャネル攻撃実験用標準評価ボード（SASEBO）等を使用した、サイドチャネルセキュリティワーキンググループの委員による、2009 年度の発表についてまとめた。（表 2.7）

表 2.7　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	SASESBO-R 上の AES 回路に対する 2 種の CPA の比較	電子情報通信学会総合大会	2009.3.20	川村 和範，岩井 啓輔，黒川 恭一(防衛大学校)	SASEBO-R
2	SCAPE ボードでの差分電力解析と差分電磁波解析の比較	電子情報通信学会総合大会	2009.3.20	菅野 哲太郎，岩井 啓輔，黒川恭一(防衛大学校)	SCAPE
3	Fault Analysis Attack against an AES Prototype Chip using RSL	CT-RSA[39] 2009	2009.4.24	崎山 一男，八木 達哉，太田 和夫(電気通信大学)	SASEBO
4	AES に対する CPA 攻撃のシミュレーション評価	ISEC[40]	2009.5.22	山越　公洋，山岸　明洋(日本電信電話株式会社))	シミュレーション(FPGA+RTL)
5	Evaluation of Simple/ Comparative Power Analysis against an RSA ASIC Implementation	ISCAS[41] 2009	2009.5.25	宮本 篤志，本間 尚文，青木 孝文(東北大学)，佐藤 証(産業技術総合研究所)	SASEBO-R
6	An Analysis of Information Leakage from a Cryptographic Hardware via Common-Mode Current	EMC[42]2009	2009.7.21	林 優一，菅原 健，，本間 尚文，水木 敬明(東北大学)，佐藤 証(産業技術総合研究所)，青木 孝文，嶺岸 茂樹，曽根 秀昭，井上 浩(東北大学)	SASEBO
7	Spectrum Analysis of Cryptographic Modules to Counteract Side-Channel Attacks	EMC2009	2009.7.21	菅原 健，林 優一，本間 尚文，水木 敬明，青木 孝文，曽根 秀昭(東北大学)，佐藤 証(産業技術総合研究所)	SASEBO
8	Differential Power Analysis of AES ASIC Implementations with Various S-box Circuits	ECCTD[43] 2009	2009.8.25	菅原 健，本間 尚文，青木 孝文(東北大学)，佐藤 証(産業技術総合研究所)	SASEBO-R
9	Complementary Logics vs Masked Logics: which Countermeasure is a better selection?	ECCTD 2009	2009.8.25	松本 勉，三村 英伸(横浜国立大学)，鈴木 大輔(横浜国立大学/三菱電機株式会社)	SASEBO
10	Development of Side-Channel Attack Standard Evaluation Environment	ECCTD 2009	2009.8.25	片下 敏宏(東北大学)，佐藤 証(産業技術総合研究所)，菅原 健，本間 尚文，青木 孝文(東北大学)	SASEBO GII
11	Mechanism behind Information Leakage in Electromagnetic Analysis of Cryptographic Modules	WISA[44] 2009	2009.8.25	菅原 健，林 優一，本間 尚文，水木 敬明，青木 孝文，曽根 秀昭(東北大学)，佐藤 証(産業技術総合研究所)	SASEBO
12	AES暗号回路へのCPA攻撃の適用範囲に関する検証	防衛大学校理工学研究報告	2009.9	南崎大作，岩井啓輔，黒川恭一(防衛大学校)	SASEBO
13	SASEBO-R を使用した電磁波解析と電力解析の比較	FIT[45] 2009	2009.9.2	菅野哲太郎、岩井啓輔、黒川恭一(防衛大学校)	SASEBO

[39] CT-RSA：Cryptographers' Track at the RSA Conference
[40] ISEC：情報セキュリティ研究会（電子情報通信学会）
[41] ISCAS：International Symposium on Circuits and Systems（IEEE）
[42] EMC：International Symposium on Electromagnetic Compatibility（電子情報通信学会）
[43] European Conference on Circuit Theory and Design（IEEE）
[44] WISA：International Workshop on Information Security Applications
[45] FIT：情報科学技術フォーラム（情報処理学会）

14	Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers	FDTC[46] 2009	2009.9.6	福永 利徳，高橋 順子(ＮＴＴ情報流通プラットフォーム研究所)	SASEBO-R
15	A Design Methodology for a DPA-Resistant Cryptographic LSI with RSL Techniques	CHES[47] 2009	2009.9.8	佐伯 稔，鈴木 大輔，清水 孝一(三菱電機株式会社), 佐藤 証(産業技術総合研究所)	SASEBO-R
16	Side Channel Attack to Magnetic Near Field of Cryptographic LSI and Its Protection by Magnetic Thin Film	MCC[48]19	2009.9.9	山口正洋，鳥塚 英樹，小林 翔一，菅原 健，本間 尚文(東北大学)，佐藤 証(産業技術総合研究所)，青木 孝文(東北大学)	SASEBO-R
17	RSA 暗号プロセッサの FPGA 実装に対する平文選択型 SPA の評価	電子情報通信学会論文誌	2009.12.1	宮本篤志，本間尚文，青木 孝文(東北大学), 佐藤 証(産業技術総合研究所)	SASEBO SASEBO-R
18	Security Evaluation of a DPA-resistant S-box Based on the Fourier Transform	ICICS[49] 2009	2009.12.15	李 陽，崎山 一男(電気通信大学)，川村 信一，駒野 雄一(株式会社東芝)，太田 和夫(電気通信大学)	SASEBO
19	暗号ハードウェアの局所情報と電磁波解析	ISEC	2009.12.16	森田秀一，高橋芳夫，松本 勉，四方順司(横浜国立大学)	SASEBO
20	On Clock-based Fault Analysis Attack for an AES Hardware Using RSL	電子情報通信学会英文論文誌	2010.1.1	崎山 一男，太田 和夫(電気通信大学)	SASEBO
21	SASEBO における電磁波解析攻撃に対する FPGA 周辺回路の影響	SCIS[50]	2010.1.19	落合 隆夫，山本 大，伊藤 孝一，武仲 正彦，鳥居 直哉，内田 大輔，永井 利明，若菜 伸一(株式会社富士通研究所)	SASEBO
22	波形積分手法に基づく高速の CPA 攻撃	SCIS	2010.1.20	Guoyu Qian，Ying Zhou，Yueying Xing，Hongying Liu(早稲田大学)，角尾 幸保(日本電気株式会社), 後藤 敏(早稲田大学)	SASEBO-R
23	CPA Attack with Switching Distance Model on AES ASIC Implementation	SCIS	2010.1.20	Hongying Liu，Guoyu Qian(早稲田大学), 角尾 幸保(日本電気株式会社)，後藤 敏(早稲田大学)	SASEBO-R
24	DPA 耐性のあるソフトウェア実装のための安全な CPU	SCIS	2010.1.20	中津 大介，李 陽，崎山 一男，太田 和夫(電気通信大学)	SASEBO-G
25	公開鍵暗号の SPA/DPA 耐性向上に向けた対策アルゴリズムの再考	SCIS	2010.1.20	泉 雅巳，崎山 一男，太田 和夫(電気通信大学), 佐藤 証(産業技術総合研究所情報セキュリティ研究センター)	SASEBO-R
26	ハイブリッド型相関電力解析	SCIS	2010.1.21	山本 大，落合 隆夫，伊藤 孝一，武仲 正彦，鳥居 直哉，内田 大輔，永井 利明，若菜 伸一(株式会社富士通研究所)	SASEBO
27	変調されたサイドチャネル信号の周波数領域での電力解析	SCIS	2010.1.21	菅原 健，本間 尚文，林 優一，水木 敬明，青木 孝文，曽根 秀昭(東北大学), 佐藤 証(産業技術総合研究所)	SASEBO
28	偏らせた波形セットを用いた電力解析攻撃の高精度化	SCIS	2010.1.21	金 用大，菅原 健，本間 尚文，青木 孝文(東北大学), 佐藤 証(産業技術総合研究所情報セキュリティ研究センター)	SecmatV3 SoC SASEBO
29	FPGA に対する漏洩電磁波の局所性を利用した電磁波解析	SCIS	2010.1.21	庄司 陽彦(株式会社ワイ・デー・ケー), 角尾 幸保(日本電気株式会社), 板倉 征男(情報セキュリティ大学院大学)	SASEBO
30	High security countermeasure method against differential power analysis attack	SCIS	2010.1.21	Ying Zhou，Guoyu Qian，Yueying Xing，Hongying Liu(早稲田大学), 角尾 幸保(日本電気株式会社), 後藤	SASEBO

[46] FDTC：Fault Diagnosys and Tolerance in Cryptography
[47] CHES：Workshop on Cryptographic Hardware and Embeded Systems（IACR）
[48] MCC：Soft Magnetic Materials Conference
[49] ICICS：International Conference on Information and Communications Security
[50] 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）

				敏(早稲田大学)	
31	暗号機器の物理形状を考慮したサイドチャネル情報の評価	SCIS	2010.1.21	林 優一，菅原 健，池松 大志，本間 尚文，水木 敬明，青木 孝文，曽根 秀昭(東北大学)	SASEBO
32	サイドチャネル標準シミュレーションモデル構築に向けた標準評価ボードの DPA 特性測定	SCIS	2010.1.22	片下 敏宏，佐藤 証(産業技術総合研究所)，永田 真，藤本 大介(神戸大学大学院)，菊地 克弥，仲川 博，青柳 昌宏(産業技術総合研究所)	SASEBO-GII
33	DPA 攻撃の成功率向上のためのノイズ検出手法	SCIS	2010.1.22	Yueying Xing，Ying Zhou，Guoyu Qian，Hongying Liu(早稲田大学)，角尾 幸保(日本電気株式会社)，後藤 敏(早稲田大学)	SASEBO-R
34	暗号モジュールの信号ラインに着目した電力解析攻撃に関する考察	SCIS	2010.1.22	渡部 良太，高橋 芳夫，松本 勉(横浜国立大学)	SASEBO-R SASEBO
35	故障利用攻撃に必要な信号出力の見積もりに関する一考察	SCIS	2010.1.22	田中 秀磨(情報通信研究機構)	SASEBO-GII
36	暗号モジュールへのサイドチャネル攻撃とその安全性評価の動向	電子情報通信学会論文誌	2010.2.1	本間 尚文，青木 孝文(東北大学)，佐藤 証(産業技術総合研究所)	SASEBO
37	Biasing power traces to improve correlation in power analysis attacks	COSADE[51] 2010	2010.2.5	金 用大，菅原 健，本間 尚文，青木 孝文(東北大学)，佐藤 証(産業技術総合研究所)	SASEBO SecmatV3 SoC
38	異なる実装方法による暗号モジュールに対する離散フーリエ変換を用いた CPA の適用	情報処理学会 全国大会	2010.3.10	櫻井 敦規，黒川 恭一，岩井 啓輔（防衛大学校）	SASEBO-G SASEBO-R
39	相関値の変化傾向に着目した篩い分けの CPA への適用	情報処理学会 全国大会	2010.3.10	若林 邦爾，黒川 恭一，岩井 啓輔（防衛大学校）	SASEBO-R
40	SASEBO-R の電源ラインへの電磁波解析	ISEC	2010.3.5	菅野 哲太郎・岩井 啓輔・黒川 恭一（防衛大学校）	SASEBO-R
41	アセンブリコードレベルの電力解析攻撃への対策	ISEC	2010.3.5	川村 和範・岩井 啓輔・黒川 恭一（防衛大学校）	SASEBO
42	Improved Countermeasure against Address-bit DPA for ECC Scalar Multiplication	DATE[52] 2010	2010.3.10	泉 雅巳，池上 淳，崎山 一男，太田 和夫(電気通信大学)	SASEBO
43	Power Variance Analysis Breaks a Masked ASIC Implementation of AES	DATE 2010,	2010.3.10	李 陽，崎山 一男，Lejla Batina，中津 大介，太田 和夫(電気通信大学)	SASEBO

(1) SASESBO-R 上の AES 回路に対する 2 種の CPA の比較

川村 和範，岩井 啓輔，黒川 恭一(防衛大学校)

電子情報通信学会 総合大会 （2009 年 3 月 20 日）

AES のソフトウェア実装に対する電力解析攻撃への対策として、中間値が生で表れないように乱数でマスクし、Sbox の入力マスクは乱数でなく固定値 0xFF とすることで、Sbox を暗号化の度に作り替えるコストを節約する方法提案している。ただし、マスクを 1 回で掛けると高次 DPA で攻撃可能となるため、さらに 8 次 DPA 対策を施す。この提案方法を SASEBO 上の MicroBlaze 及び PowerPC に実装し、CPA への耐性を評価した。10 万波形取得して CPA を実施した結果、部分鍵は全く特定されなかった。

[51] COSADE：International Workshop on Constructive Side-Channel Analysis and Secure Design

[52] DATE：Design, Automation and Test in Europe（ACM）

(2) SCAPE ボードでの差分電力解析と差分電磁波解析の比較

菅野 哲太郎，岩井 啓輔，黒川恭一(防衛大学校)

電子情報通信学会 総合大会 （2009 年 3 月 20 日）

電磁波解析は電力解析と比べ、測定場所が自由に選べる点に長所があり、暗号モジュールから伸びる電源ライン等の電線は漏洩電磁波の測定箇所として特に有効であると考える。しかし、ほぼ抵抗を無視出来る電線ラインからの電磁波を実際に測定し、相関電磁波解析(Correlation ElectroMagnetic Analysis) を行った結果、全鍵ビットの特定に必要な波形数は、電力解析の数倍になった。これは、電磁波解析の欠点である、電磁波測定におけるノイズの混入が大きな要因になっていると考えられる。そこで解析の効率を改善するため、測定した波形データにデジタルフィルタを適用し、解析に要する波形数が約 1/2 以下に低減できることを実験的に確認し、有効性を検証した。

(3) Fault Analysis Attack against an AES Prototype Chip using RSL

崎山 一男，八木 達哉，太田 和夫(電気通信大学)

CT-RSA 2009 （2009 年 4 月 24 日）

本論文ではロジック・レベルのサイドチャネル攻撃対策である Random Switching Logic (RSL)を施した AES のハードウェア実装のプロトタイプに対し、故障利用攻撃(FA)が有効であることを確認した。RSL は DPA に対する最も有効な防御対策の一つとして提案され、0.13-μm スタンダード CMOS ライブラリを使った AES の ASIC 実装のプロトタイプに適用された。RSL の主目的は DPA 耐性の強化であったが、著者らはこの対策が逆に FA に対する耐性を弱めることになり、RSL を使った回路はクロック周波数を上げることで潜在的に FA によって攻撃可能であることを示した。

(4) AES に対する CPA 攻撃のシミュレーション評価

山越 公洋，山岸 明洋(日本電信電話株式会社))

ISEC2009-3 （2009 年 5 月 22 日）

AES の CMOS 論理回路によるハードウェア実装に対し、DPA の一種である CPA(Correlation Power Analysis)攻撃がどの程度有効であるかをシミュレーションによって解析した結果を示した。このシミュレーションでは、CMOS 論理回路の消費電力に相当する論理ゲートの状態遷移回数の時間遷移を一定の時間間隔で計算し、レジスタのハミング距離との相関係数を計算した。評価の結果、状態遷移回数計測の時間間隔を小さくするのに伴い、秘密鍵の推定精度が低下する場合があることがわかった。この結果は、CPA 攻撃を行うための消費電力測定環境は必ずしもハイスペックである必要はないことを意味する。今回用いた回路設計段階でのシミュレーションによる CPA 攻撃に対する耐性評価手法は、製造後の回路修正が困難である ASIC 設計において特に有効である。

(5) Evaluation of Simple/Comparative Power Analysis against an RSA ASIC Implementation

宮本 篤志，本間 尚文，青木 孝文(東北大学)，佐藤 証(産業技術総合研究所)

ISCAS 2009 （2009 年 5 月 25 日）

SPA 攻撃の効率改善のため、メッセージを適切に選択する手法を標準 CMOS 技術による RSA 暗号の ASIC 実装に適用し有効性を確認した。また、ASI 実装と FPGS 実装における電力波形の特性の違いを詳細に観察した。さらに、剰余べき乗計算の波形パターンの違いを強める入力データをペアで与える比較電力解析手法を適用した。その結果、剰余乗算と比較すると剰余二乗算の波形の散逸が著しく小さくなることが確認でき、全秘密鍵ビットを得ることに成功した。

(6) An Analysis of Information Leakage from a Cryptographic Hardware via Common-Mode Current

林 優一, 菅原 健, 本間 尚文, 水木 敬明(東北大学), 佐藤 証(産業技術総合研究所), 青木 孝文，嶺岸 茂樹，曽根 秀昭，井上 浩(東北大学)

EMC2009 Kyoto （2009 年 7 月 21 日）

漏洩情報が暗号モジュールから同相電流を通して伝搬する様子を解析した。ここでは、漏洩の機構を一般的な方法で議論するために単純化されたボードのモデルを提案した。シミュレーションと実験によって、実際の暗号ボードにおける周波数特性が提案モデルから得られるものと良く一致することが確認できた。これらの結果を踏まえ、暗号モジュールの対策は電磁両立性とサイドチャネル攻撃の両方の視点から議論すること提案する。

(7) Spectrum Analysis of Cryptographic Modules to Counteract Side-Channel Attacks

菅原 健，林 優一，本間 尚文，水木 敬明，青木 孝文，曽根 秀昭(東北大学)，佐藤 証(産業技術総合研究所)

EMC2009 Kyoto （2009 年 7 月 21 日）

本論文では、通常の DPA では時間領域における波形の代わりに、周波数領域における分布を解析対象とし、電力解析攻撃に適した周波数帯を特定するためのスペクトル解析方法を提案する。提案方法の有効性は AES の FPGA 実装に対する実験によって検証された。また、提案方法の結果を利用して設計したノイズフィルターは電力解析に対する有効な防御になることを示す。

(8) Differential Power Analysis of AES ASIC Implementations with Various S-box Circuits

菅原 健，本間 尚文，青木 孝文(東北大学)，佐藤 証(産業技術総合研究所)

ECCTD 2009 （2009 年 8 月 25 日）

異なる S-box アーキテクチャを持つ AES の ASIC 実装に DPA を適用した。S-box のアー

キテクチャは次の 4 種類を用意した。(i)逐次拡大を使ったガロア体 GF(((22)2)2)上の逆元計算、(ii)テーブル参照、(iii)PPRM(正極 Reed-Muller 形式)、(iv)3 状態 PPRM。これらの AES 実装のための専用 ASIC を開発し、SASEBO-R の上で測定した。その結果、S-box の実装の仕方で DPA 耐性が大きく変ることが示された。これらの結果は FPGA 実装結果とも比較し、プラットフォームによる違いを観察した。

(9) Complementary Logics vs Masked Logics: which Countermeasure is a better selection?

松本 勉，三村 英伸(横浜国立大学)，鈴木 大輔(横浜国立大学/三菱電機株式会社)

ECCTD 2009 （2009 年 8 月 25 日）

本論文ではサイドチャネル攻撃対策としての相補ロジックとマスク・ロジックを比較することに目的を絞り、これらの対策を適用した AES コプロセッサを開発した。ターゲットのデバイスとプロセスの違いに依存した違いを評価するため、コプロセッサは 3 種類の実装環境 130nm-ASIC、90nm-ASIC、FPGA で開発した。これらの実装性能と安全性を評価した結果、相補ロジックとマスク・ロジックで実装性能の差はないものの、セミカスタムのデザインフローにおけるサイドチャネルセキュリティの観点によれば、マスク・ロジックが優位であることが明らかになった。

(10) Development of Side-Channel Attack Standard Evaluation Environment

片下 敏宏(東北大学)，佐藤 証(産業技術総合研究所)，菅原 健，本間 尚文，青木 孝文(東北大学)

ECCTD 2009 （2009 年 8 月 25 日）

サイドチャネル攻撃及び対策の評価用標準プラットフォームとして、FPGA ボード SASEBO-GII を開発した。SASEBO-GII では、新しい FPGA デバイス Virtex-5 LX30/50 が搭載され、大きなロジック容量とダイナミックな部分的再構成が可能である。構成データは USB 接続経由でホスト PC から FPGA に転送でき、JTAG ケーブルが必要ない。USB ポートからボードが同左するための電力が供給される。これらの機能追加にもかかわらず、SASEBO-GII のサイズは一つ前のボード SASEBO-G の 1/3 しかない。この小型化と回路デザインによって、サイドチャネル解析の妨げとなるノイズが低減した。本論文では、様々な AES 実装とそれらに対する CPA 実験を通して、SASEBO-GII の優位性をアピールした。

(11) Mechanism behind Information Leakage in Electromagnetic Analysis of Cryptographic Modules

菅原 健，林 優一，本間 尚文，水木 敬明，青木 孝文，曽根 秀昭(東北大学)，佐藤 証(産業技術総合研究所)

WISA 2009 （2009 年 8 月 25 日）

暗号チップから電磁放射が生じていて、サイドチャネル攻撃に利用できる可能性は広く知

られていたが、集中的に研究されることはなかった。本論文では、環境電磁気学(EMC)の観点から、暗号チップから発せられる電気的ゆらぎが周辺回路に伝わり、放射を引き起こすことを説明し、それがサイドチャネル攻撃に利用できることを実験的に示した。具体的には、RSA と AES を実装した FPGA を用意し、FPGA プラットフォームに接続された電源ケーブル及び通信ケーブルの放射を測定し、単純電磁解析(SEMA)と差分電磁解析(DEMA)を適用した。実験の結果、暗号モジュールに対策を施し、安全領域(security boundary)内へのアクセスを拒否するようになっていても、安全領域につながっているケーブルを通じて情報が漏えいすることが示された。提案した放射の機構を使うことにより、情報漏えいを起こす回路要素を予想することが可能になる。さらに、著者らは攻撃の改良法と攻撃対策としてのノイズ抑制技術についても議論している。

(12) AES 暗号回路への CPA 攻撃の適用範囲に関する検証

南崎 大作，岩井 啓輔，黒川 恭一(防衛大学校)

防衛大学校 理工学研究報告, 第 47 巻 1 号,pp.47-55 （2009 年 9 月 1 日）

電力解析攻撃の一種である CPA(Correlation Power Analysis)において、相関の計算に利用する時間領域の選び方によって、鍵特定に必要な波形数や計算時間がどのように影響されるかを調べるため、SASEBO 上に実装された AES を用いた実験を行った。実験の結果、電圧変動のピーク部を相関計算の対象範囲とすることで、他の対象範囲の選び方に比べ、波形数・計算時間ともに小さくなることが分かった。

(13) SASEBO-R を使用した電磁波解析と電力解析の比較

菅野 哲太郎、岩井 啓輔、黒川 恭一(防衛大学校)

FIT 2009 （2009 年 9 月 2 日）

SASEBO-R のシャント抵抗部について、電力解析と電磁波解析を適用し、特性を比較した。単純に波形を比べると、電磁波形は帯域に制限のあるときは正弦波形に近い形になるものの、帯域制限をなくすと電力波形に近い形になった。相関攻撃では、相関電力解析(CPA)に比べ相関電磁解析(CEMA)は、鍵正答率・必要波形数ともに対象時間領域の選び方の影響が大きく、適切に選んだときは CEMA が優れた結果を示した。また、最適の時間領域は、CEMA の方が短くなることが分かった。

(14) Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers

福永 利徳，高橋 順子(ＮＴＴ)

FDTC 2009 （2009 年 9 月 6 日）

ブロック暗号の国際規格 ISO/IEC 18033-3 に記載された 6 種類の暗号 AES, DES, Camellia, CAST-128, SEED, MISTY1 を、暗号専用 LSI を搭載したサイドチャネル攻撃用標準評価ボード SASEBO-R に実装し、クロック信号にグリッチを乗せることによって誤作動を希望する段で引き起こせることを確認した。AES に関しては Piret の攻撃法を適用し、

誤りを含む暗号文１個だけを用いて、鍵が復元できることを確認した。

(15) A Design Methodology for a DPA-Resistant Cryptographic LSI with RSL Techniques

佐伯 稔，鈴木 大輔，清水 孝一(三菱電機株式会社)，佐藤 証(産業技術総合研究所)

CHES 2009 （2009 年 9 月 8 日）

CMOS 標準セル上に暗号を実装した暗号モジュールの有効な DPA 対策として、RSL(Random Switching Logic)が提案されている。RSL で利用される独自の RSL-gate では、ランダムなマスクとグリッチの抑制が必要となる。本論文では標準セル・ライブラリによる一般的な論理ゲートを使って、同様の効果を実現する“pseudo RSL”を提案した。この有効性を検証するため 130-nm CMOS 標準セル・ライブラリで実装した。同じ条件で実装した既存の DPA 対策である WDDL ではゲート数が 3 倍、速度が 1/4 になったのに対し、pseudo RSL では各々、2 倍、1/2 であり、実装性で優った。また、DPA 耐性にも優れていた。ただし、論文採録後、pseudo RSL を実装したものが、1 ビット DPA で攻撃可能であることが分かり、その原因が遅延に関する条件が満足されていないことが分かった。遅延に関する条件に合わせた修正は実施中。

(16) Side Channel Attack to Magnetic Near Field of Cryptographic LSI and Its Protection by Magnetic Thin Film

山口正洋，鳥塚 英樹，小林 翔一，菅原 健，本間 尚文(東北大学)，佐藤 証(産業技術総合研究所)，青木 孝文(東北大学)

MCC19 （2009 年 9 月 9 日）

シールドされたループコイル持つオンチップの超小型磁気プローブ使って、暗号 LSI の近接磁場の測定を行った結果、高周波電流が計測できた。差分電磁解析を適用したところ、暗号 IP コアでは鍵推定が少ない観測波形で出来、暗号 IP コアから離れるに従って必要な波形数が増える傾向が見られた。

(17) RSA 暗号プロセッサの FPGA 実装に対する平文選択型 SPA の評価

宮本 篤志，本間 尚文，青木 孝文(東北大学)，佐藤 証(産業技術総合研究所)

電子情報通信学会 論文誌 Vol.J92-D No.12 （2009 年 12 月 1 日）

RSA 暗号に対する平文選択型 SPA が提案されているが、そのほとんどが理論解析であり、実機よる検証はあまり行われていない。本論文では、SASEBO の FPGA と SASEBO-R の ASIC に 4 種類の RSA 暗号プロセッサを実装し、平文選択型 SPA を適用し、実装の違いによる有効性の違いを明らかにした。

(18) Security Evaluation of a DPA-resistant S-box Based on the Fourier Transform

李 陽，崎山 一男(電気通信大学)，川村 信一，駒野 雄一(株式会社東芝)，太田 和夫(電気通信大学)

ICICS 2009 （2009 年 12 月 15 日）

離散フーリエ変換を利用した S-box 計算の DPA 対策は、最初、Prouff らが CHES 2006 で提案し、Coron らが CHES 2008 で改良版を提案し、1 次 DPA で攻撃できる欠陥を解消した。本論文では、Coron らの S-box アルゴリズムは現実的なソフトウェア実装では攻撃できることを示す。攻撃は前処理と 2 種類の後処理で構成される。前処理では、電力波形を各々がバイアスマスクを持つ 2 つのサブグループに分ける。後処理の一つでは、サブグループの一つに対して CPA を行い、他の後処理では、2 つのサブグループの平均の差とパターンマッチングを利用する。これら 2 種類の攻撃を比較した後、Coron の S-box 計算の安全性を改善するアルゴリズムレベルの対策が提案されている。

(19) 暗号ハードウェアの局所情報と電磁波解析

森田 秀一，高橋 芳夫，松本 勉，四方 順司(横浜国立大学)

ISEC2009-75 （2009 年 12 月 16 日）

電磁波を用いたサイドチャネル攻撃の利点として測定場所による選択的な情報取得可能性が指摘されている。電力/電磁波を用いた攻撃法である Differential Power/ElectroMagneticAnalysis(DPA/DEMA)は共に測定値に含まれる情報を選択できればより少ないコストで攻撃できる為、測定場所で取得情報を選択できれ ば、DEMA は DPA より強力な攻撃となる。本稿では、SASEBO の暗号実装用 FPGA に実装した 128bit ブロック暗号 AES を攻撃対象に、暗号 ハードウェアから放射される電磁波を複数ポイントで測定し、得られた情報について分析した。その結果、測定する場所によって得られる情報は異なっており、 着目するビットにより最適な測定場所は異なっていることがわかった。

(20) On Clock-based Fault Analysis Attack for an AES Hardware Using RSL

崎山 一男，太田 和夫(電気通信大学)

ICICE Trans. Vol.E93-A No.1, pp.172-179 , Jan., 2010. （2010 年 1 月 1 日）

本論文ではロジック・レベルのサイドチャネル攻撃対策である Random Switching Logic (RSL)を施した AES のハードウェア実装のプロトタイプに対し、クロックベースの故障利用攻撃(CFA)が有効であることを確認した。RSL は DPA に対する最も有効な防御対策の一つとして提案され、0.13-μm スタンダード CMOS ライブラリを使った AES の ASIC 実装のプロトタイプに適用された。RSL の主目的は DPA 耐性の強化であるが、著者らは RSL を使った回路に CFA を適用することで、鍵情報を取り出すことに成功した。著者らは CFA のメカニズムを説明した後、CFA が成功した理由を考察し、攻撃対象の実装では S-box ごとにマスクを変えていないという結論を導いた。さらに、S-box ごとのマスクをランダムに変えるなど、理想的な実装を行えば、RSL-AES は CFA に対して安全であろうという見解を述べている。

(21) SASEBO における電磁波解析攻撃に対する FPGA 周辺回路の影響

落合 隆夫，山本 大，伊藤 孝一，武仲 正彦，鳥居 直哉，内田 大輔，永井 利明，若菜 伸一(株式会社富士通研究所)

SCIS2010　1B2-4 （2010 年 1 月 19 日）

本論文は、SASEBO ボード上の FPGA に実装された AES に対して電磁波解析を行い、ボード上の電力解析用試験抵抗など、周辺回路からの漏洩電磁界がサイドチャネル解析に与える影響について議論する。さらに、FPGA の異なる位置、および試験抵抗上からの電磁界ノイズを磁界プローブで検出することにより、測定箇所によって解析成功率に差があることを示す。本研究の本来の目的は、FPGA に実装された暗号レジスタの局所情報から、暗号化鍵とレジスタ位置との対応を明らかにすることができるか検証することにあるが、今回は、その前段階の基礎的な検討として、SASEBO 上に実装された電力解析用の試料抵抗など、周辺回路がサイドチャネル解析に与える影響について調べた。また、FPGA 近傍の電磁界ノイズを磁界プローブで検出することにより、FPGA チップを直接攻撃せずとも CPA が可能であること、測定箇所により推定可能な部分暗号鍵に分布が存在することを示す。

(22) 波形積分手法に基づく高速の CPA 攻撃

Guoyu Qian，Ying Zhou，Yueying Xing，Hongying Liu(早稲田大学)，角尾 幸保(日本電気株式会社)，後藤 敏(早稲田大学)

SCIS2010　2B1-4 （2010 年 1 月 20 日）

本論文は、オリジナルの CPA が電力波形上の 1 時刻での相関しか利用せず、情報を十分活用していない点を改良するため、波形の時間積分(Wave Integral)を利用する改良型の CPA である CPA-WI を提案し、その有効性を SASEBO-R の ASIC 上に実装された AES に対する実験で確認した。CPA-WI の適用において、対象とする時間領域の選び方が適切でなければ効率が悪いが、適切に選べば、オリジナルの CPA よりも少ない波形数と少ない計算量で正しく鍵を推定できる。

(23) CPA Attack with Switching Distance Model on AES ASIC Implementation

Hongying Liu，Guoyu Qian(早稲田大学)，角尾 幸保(日本電気株式会社)，後藤 敏(早稲田大学)

SCIS2010　2B1-5 （2010 年 1 月 20 日）

本論文は、CPA において、通常使われるハミング距離を漏洩情報とするモデルの代わりに、スイッチ距離を漏洩情報とするモデル(SD モデル)に基づく解析を適用することを提案する。SASEBO-R の LSI 上に実装された AES を使った実験によって、SD モデルに戻づく CPA では、鍵の正しい推定に必要な電力波形数が、従来の CPA より 25%少ない結果が得られ、その有効性が確認された。

(24) DPA 耐性のあるソフトウェア実装のための安全な CPU

中津 大介，李 陽，崎山 一男，太田 和夫(電気通信大学)

SCIS2010　2B3-1 （2010 年 1 月 20 日）

本論文は DPA 耐性のある AES のソフトウェア実装を実現するための CPU の構築法を示し、SASEBO-G の FPGA 上に CPU を仮想的に実装することでその有効性を確認した。AES の DPA 対策はソフトウェア／ハードウェア両方の対策を施しており、ソフトウェアでの対策は、Coron による離散フーリエ変換を利用する方法をベースに Li らによるアドレスのランダム化による改良を施した方法を利用する。また、ハードウェアでの対策では、鈴木らが提案した RSL (Random Switchnig Logic)を用いる。

(25) 公開鍵暗号の SPA/DPA 耐性向上に向けた対策アルゴリズムの再考

泉 雅巳，崎山 一男，太田 和夫(電気通信大学)，佐藤 証(産業技術総合研究所)

SCIS2010　2B3-2 （2010 年 1 月 20 日）

本論文では、ECC 回路に対する 2 種類の既存の電力解析対策法の有効性を検討した。一つは著者らが提案した SPA 対策法である MPL 法(Montgomery Powering Ladder 法)であり、SASEBO-R の LSI 上に実装し、その有効性を確認した。もう一つは伊藤らが提案した ADPA(Address-bit DPA)対策法であり、アーキテクチャの構成を考える必要のないアルゴリズムレベルの変更で済み、アーキテクチャや回路構成法を考慮する必要があり、かつ、DPA 対策にならない MPL 法に対する優位性を持つ。解析の結果、ADPA 対策法はほとんどの場合、SPA/DPA 対策として有効であるが、特別な状況下では DPA に対して脆弱となる可能性があることを示唆する結果となった。

(26) ハイブリッド型相関電力解析

山本 大，落合 隆夫，伊藤 孝一，武仲 正彦，鳥居 直哉，内田 大輔，永井 利明，若菜 伸一(株式会社富士通研究所)

SCIS2010　3B1-2 （2010 年 1 月 21 日）

ハードウェアに対する従来の電力解析では、レジスタの遷移に着目したハミングディスタンス(HD)モデルを用いた CPA が有効であるが、組み合わせ回路の消費電力の割合が大きくなると、HD モデルだけでなく、ハミングウェイト(HW)モデルに基づく CPA も有効となる。本論文では、組み合わせ回路の消費電力が大きなハードウェア実装に適するよう、HD と HW の両方を考慮したハイブリッド(HB)モデルを提案し、SASEBO-R の AES 回路(PPRM1)を使用した基礎実験を通して有効性を検証した。実験の結果、正しい鍵推定に必要な波形数が、HD モデルでは 1800、HW モデルでは 1200 だったのに対し、HB モデルでは 800 となり、有効性が確認できた。

(27) 変調されたサイドチャネル信号の周波数領域での電力解析

菅原 健，本間 尚文，林 優一，水木 敬明，青木 孝文，曽根 秀昭(東北大学)，佐藤 証(産業

技術総合研究所)
SCIS2010　3B1-4　(2010 年 1 月 21 日)

本論文では、周波数領域における暗号モジュールの電力解析に基づく、漏洩情報(サイドチャネル信号)を含む帯域の検知法ついて述べる。提案手法では、周波数領域での CPA を行い、その結果を用いて帯域を効率的に検知する。今回は特に、変調されたサイドチャネル信号が電力波形に含まれる場合でも提案手法により検知可能であることを理論的に示し、FPGA 上に AES コア実装した SASEBO に対する計測で得られた波形から生成した変調波に、提案手法を適用して有効性を確認した。

(28) 偏らせた波形セットを用いた電力解析攻撃の高精度化

金 用大，菅原 健，本間 尚文，青木 孝文(東北大学)，佐藤 証(産業技術総合研究所)
SCIS2010　3B1-5　(2010 年 1 月 21 日)

本論文では、CPA の効率を改善するため、計測した大量の波形中から特定の波形セットを選択し、電力波形の確率分布を偏らせる方法を提案し、提案法を 2 種類の暗号モジュールに適用することで有効性を確認した。2 種類の暗号モジュールは、ASIC 上に DES を実装した SecmatV3 SoC(DPA Contest で使用)と FPGA 上に AES を実装した SASEBO である。一方、このように攻撃に使用する波形を選択することは、攻撃や安全性の公平な評価を妨げるので、与えられた波形セットの偏りを評価する方法も提案した。

(29) FPGA に対する漏洩電磁波の局所性を利用した電磁波解析

庄司 陽彦(株式会社ワイ・デー・ケー)，角尾 幸保(日本電気株式会社)，板倉 征男(情報セキュリティ大学院大学)
SCIS2010　3B3-2　(2010 年 1 月 21 日)

本論文では、まず、局所的な解析が可能であることを示し、次に、この解析結果を利用することによってサイドチャネル攻撃対策手法である DRL(Dual Rail Logic)に対する攻撃が可能であることを示した。局所的な解析とは、漏洩電磁波の発生位置と強度から演算回路の位置情報やビット単位の変化を識別することである。DRL は相補的な回路を利用することで、消費電力を一定にするサイドチャネル対策であるが、漏洩電磁波の局所的な解析を使うことで解析対象の回路を特定することで防御を無効にする。以上の結果は、FPGA 上に DES を実装した SASEBO を使った実験によって確認されている。

(30) High security countermeasure method against differential power analysis attack

Ying Zhou，Guoyu Qian，Yueying Xing，Hongying Liu(早稲田大学)，角尾 幸保(日本電気株式会社)，後藤 敏(早稲田大学)
SCIS2010　3B3-3　(2010 年 1 月 21 日)

本論文は、AES の実装に対する低コストで効果の高い DPA 対策として、レジスタと乱数生成器のセットを追加する方法を提案する。この対策を SASEBO の FPGA に実装したところ、

動作周波数 200MHz で 2.56Gbps のスループットを達成し、DPA 耐性を持つことが確認できた。ただし、この対策にでは、保存するデータの長さがが異なると処理時間も変化するのでタイミング攻撃が有効な可能性があるので、さらなる解析と改良が必要である。

(31) 暗号機器の物理形状を考慮したサイドチャネル情報の評価

林 優一，菅原 健，池松 大志，本間 尚文，水木 敬明，青木 孝文，曽根 秀昭(東北大学)
SCIS2010　3B3-4 （2010 年 1 月 21 日）

従来の電力解析攻撃の多くは、消費電力波形を暗号モジュールの近傍で観測するものだったが、近年、暗号モジュールを搭載した機器の遠方にも電源線等を通じて秘密鍵情報が漏洩する事が指摘されている。この秘密鍵情報の漏洩は、機器全体の形状やデバイスに接続された線路によって構成されるフィルタによってその周波数特性が大きく変化すると考えられる。本論文では、同一の暗号モジュールを用いた場合でも、機器を構成する基板の大きさや、基板に接続される線路の長さ等に依存して、外部に漏洩する情報量が変化することを示す。この結果は、サイドチャネル攻撃対策において、暗号モジュール単体だけでなく、それを含む機器やシステム全体での評価が必要であることを示唆する。上記の結果は、AES モジュールを用いた暗号機器モデルによる理論解析及び AES モジュールを FPGA 上に搭載した SASEBO による実験により確認した。

(32) サイドチャネル標準シミュレーションモデル構築に向けた標準評価ボードの DPA 特性測定

片下 敏宏，佐藤 証(産業技術総合研究所)，永田 真，藤本 大介(神戸大学大学院)，菊地 克弥，仲川 博，青柳 昌宏(産業技術総合研究所)
SCIS2010　4B2-1 （2010 年 1 月 22 日）

暗号モジュールの開発には大きなコストが必要となるため、製造前に実装の安全性を精度良く評価することが必要となる。近似モデルを用いたシミュレーションによってサイドチャネル攻撃耐性を評価する既存研究はあるが、独自の実装環境を用いたモデルの構築がほとんどで、第三者が検証することが困難であった。このような状況を改善するため、著者らはサイドチャネル攻撃用標準評価ボード SASEBO-GII を開発し、それを用いた測定で得られた特性から近似モデルを構築し、サイドチャネル攻撃耐性を評価するための標準環境と標準モデルの整備を進めている。本論文では、モデル構築に向け、基板のデカップリングキャパシタの有無よるインピーダンス変化の特性と AES 回路の電力波形の測定、サイドチャネル情報の SNR の算出、CPA 攻撃を行いた電源ネットワークのインピーダンス変化の影響の解析などを行った。

(33) DPA 攻撃の成功率向上のためのノイズ検出手法

Yueying Xing，Ying Zhou，Guoyu Qian，Hongying Liu(早稲田大学)，角尾 幸保(日本電気株式会社)，後藤 敏(早稲田大学)

SCIS2010　4B2-2　（2010 年 1 月 22 日）

ノイズ検出フィルタの有効性は ASIC に本論文では、DPA による鍵推定の成功率(SR)を改善する方法として、測定電力波形に含まれるノイズ成分を除去するノイズ・フィルタの利用を検討する。最初にこの研究の背景を述べた後に、有効性の理論的証明を伴なうノイズ検出フィルタを提案する。ノイズ検出フィルタの有効性は ASIC にノイズ検出フィルタの有効性は ASIC 上に AES を実装した SASEBO-R を用いた実験で確認した。

(34) 暗号モジュールの信号ラインに着目した電力解析攻撃に関する考察

渡部 良太，高橋 芳夫，松本 勉(横浜国立大学)

SCIS2010　4B2-3　（2010 年 1 月 22 日）

従来行われてきた電力解析では、電源ラインで電力波形を測定するものがほとんどだったが、電源ラインと電気的に関連のある信号ラインにおける電力波形を用いても同様に鍵が推定できる可能性がある。本論文では、SASEBO-R 上の LSI と SASEBO 上の FPGA に実装された複数の AES に対し、信号ラインと電源ラインで測定した電力波形を用いて計算した相関値を比較した。測定の結果、実装方法による違いはあるものの、複数の信号ライン及び電源ラインにおける相関値に大差はないという結果が得られた。

(35) 故障利用攻撃に必要な信号出力の見積もりに関する一考察

田中 秀磨(情報通信研究機構)

SCIS2010　4B2-4　（2010 年 1 月 22 日）

本論文では、故障利用攻撃において、任意の誤りを発生させるのに必要な信号出力を評価した。攻撃対象は SASEBO-GII 上の FPGA として、基盤上の回路線に直接過電圧をかける方法で誤り発生の有無を観測した。実験の結果、この手法により見積もられた攻撃信号電圧によって、ほぼ確率 1 で任意の信号へ改変することが確認できた。

(36) 暗号モジュールへのサイドチャネル攻撃とその安全性評価の動向

本間 尚文，青木 孝文(東北大学)，佐藤 証(産業技術総合研究所)

電子情報通信学会 論文誌 J-93A　（2010 年 2 月 1 日）

代表的なサイドチャネル攻撃である SPA と DPA の解説。攻撃対象は SASEBO 上に実装された RSA 暗号と AES であり、RSA 暗号に SPA、AES に DPA を適用した例が示されている。

(37) Biasing power traces to improve correlation in power analysis attacks

金 用大，菅原 健，本間 尚文，青木 孝文(東北大学)，佐藤 証(産業技術総合研究所)

COSADE 2010　（2010 年 2 月 5 日）

本論文では、測定した電力波形から適切な部分集合を選択することにより、CPA による鍵推定の効率が改善することを 2 種類のデバイス、SASEBO と SecmatV3 SoC(DPA Contest

で利用)を使った実験によって確認した。ほとんどの電力解析の研究は、鍵の成否を判断する識別子(distinguisher)の改良に集中しているが、著者らは測定波形における SN 比に注目し、SN 比を改善するための具体的な測定波形の選択法を開発し、CPA の効率の改善を実現した。

(38) 異なる実装方法による暗号モジュールに対する離散フーリエ変換を用いた CPA の適用

櫻井 敦規，黒川 恭一，岩井 啓輔（防衛大学校）

情報処理学会 全国大会 （2010 年 3 月 10 日）

本論文では周波数領域での CPA を 2 種類の異なる AES 実装に対して適用し、回路の動作周波数とシャント抵抗値の違いによる影響を検証した。AES の S-box では合成体による回路を採用し、SASEBO-G の FPGA への実装と、FPGA と同様のノードを持つネットリストとなるように制約を与えて論理合成された AES-S を使った SASEBO-R での実装で実験を行った。実験の結果、回路の動作周波数が大きいほど相関値が大きくなる傾向は両方の実装で共通するものの、相関が最大となる周波数は大きく異なる結果が得られた。

(39) 相関値の変化傾向に着目した篩い分けの CPA への適用

若林 邦爾，黒川 恭一，岩井 啓輔（防衛大学校）

情報処理学会 全国大会 （2010 年 3 月 10 日）

CPA は、DPA に比べて正解鍵の特定に必要な電力波形数が多くなり、演算量も膨大になる欠点がある。この欠点を解消するため、CPA の途中での各鍵候補の相関値の変化傾向を使って不正解の可能性が高い鍵を篩い落とすことによって、CPA の計算量を削減する方法を提案した。AES を実装した SASEBO-R で実験を行ったところ、7 波形以上で篩い分けの効果が出る傾向が見えた。

(40) SASEBO-R の電源ラインへの電磁波解析

菅野 哲太郎，岩井 啓輔，黒川 恭一（防衛大学校）

ISEC2009-112 （2010 年 3 月 5 日）

電磁波解析は電力解析と比べ、測定場所が自由に選べる点に長所があり、暗号モジュールから伸びる電源ライン等の電線は漏洩電磁波の測定箇所として特に有効であると考える。しかし、SASEBO-R に実装した AES を対象に、ほぼ抵抗を無視出来る電線ラインからの電磁波を測定し、相関電磁波解析(Correlation ElectroMagnetic Analysis) を行った結果、全鍵ビットの特定に必要な波形数は、電力解析の数倍になった。これは、電磁波解析の欠点である、電磁波測定におけるノイズの混入が大きな要因になっていると考えられる。そこで解析の効率を改善するため、測定した波形データにデジタルフィルタを適用し、解析に要する波形数が約 1/2 以下に低減できることを実験的に確認し、有効性を検証した。

(41) アセンブリコードレベルの電力解析攻撃への対策

川村 和範，岩井 啓輔，黒川 恭一（防衛大学校）

ISEC2009-111 （2010 年 3 月 5 日）

AES のソフトウェア実装に対する電力解析攻撃への対策として、中間値が生で表れないように乱数でマスクし、Sbox の入力マスクは乱数でなく固定値 0xFF とすることで、Sbox を暗号化の度に作り替えるコストを節約する方法提案している。ただし、マスクを 1 回で掛けると高次 DPA で攻撃可能となるため、さらに 8 次 DPA 対策を施す。この提案方法を SASEBO 上の MicroBlaze 及び PowerPC に実装し、CPA への耐性を評価した。10 万波形取得して CPA を実施した結果、部分鍵は全く特定されなかった。

(42) Improved Countermeasure against Address-bit DPA for ECC Scalar Multiplication

泉 雅巳，池上 淳，崎山 一男，太田 和夫(電気通信大学)

DATE 2010 （2010 年 3 月 10 日）

Messerges らは USENIX 1999 において、ECC のスカラー倍算に対する攻撃法として、DPA を使ってレジスタのアドレス値を解析する ADPA (Address-bit DPA)を提案した。伊藤らは CHES 2003 においてアドレスビットをランダム化する ADPA に対する防御対策を提案した。本論文は、伊藤らの対策は ADPA を改良することで攻撃可能となることを指摘し、改良版 ADPA に対しても安全な改良版対策を提案した。伊藤らの対策の問題点は、データの書き換えを同じアドレスに対して行うため、上書きされるデータが元のデータと同じか否かを電力消費によって判別でき、アドレスの推定が可能となることである。この改良型攻撃に対する防御法では、データの書き換えの際、同じアドレスでなく、ランダム化したアドレスを利用する。

(43) Power Variance Analysis Breaks a Masked ASIC Implementation of AES

李 陽，崎山 一男，Lejla Batina，中津 大介，太田 和夫(電気通信大学)

DATE 2010 （2010 年 3 月 10 日）

実用的な DPA 対策では、全ビットに独立のランダムマスクをかけるといったコストの大きなことは行われず、S-box のような繰り返し利用される設計要素に対して同じマスクを適用してコストを節約する実装が行われる。本論文はこういった実装に対する有力な攻撃法である Power Variance Analysis (PVA)の基本原理を説明し、SASEBO-R 上に実装されたプロトタイプの RSL-AES に適用することによってその有効性を確認した。PVA が有効であるのは、マスクがランダムであっても繰り返し同じものが使われることであり、プロトタイプの RSL-AES では S-box のマスクが共通であることが著者らによって指摘されている。

2.5　今後の課題

2.5.1　電子政府推奨暗号リスト改訂のための、ハードウェア及びソフトウェア実装性評価

(1)「性能の評価」における評価内容、評価基準の検討

(2)「サイドチャネル攻撃に対する対策実現の確認」における確認内容の検討

(3) 現電子政府推奨暗号リスト掲載暗号に対する評価方法の検討

2.5.2　サイドチャネル攻撃のセキュリティ要件の検討

(1) FIPS 140-3 対応試験要件案に対するコメント検討

(2) ISO/IEC 19790 早期改定案へのコメント作成

2.5.3　サイドチャネルセキュリティワーキンググループよる実験

(1) 暗号モジュールへの最適なサイドチャネル攻撃の実験方法の検討

第 3 章　開催状況

3.1　暗号実装委員会の開催状況

2009 年度の暗号実装委員会は、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　2009 年度暗号実装委員会の開催状況

回	開催日時	主な議題
第 1 回	平成 21 年 8 月 5 日 15:30～17:30	CRYPTREC の体制変更について 委員長互選 暗号実装委員会活動計画 サイドチャネルセキュリティワーキンググループ活動計画
第 2 回	平成 21 年 10 月 2 日 10:00～12:00	応募暗号技術の実装性能評価法に関する詳細検討 応募暗号技術のサイドチャネル攻撃対策可能性の確認法に関する詳細検討 サイドチャネル攻撃の学会動向調査報告
第 3 回	平成 22 年 2 月 24 日 10:00～12:00	応募暗号技術のハードウェア実装性能評価用参照コードの検討 公募状況報告 事務局提案方式に関する検討
第 4 回	平成 22 年 3 月 2～3 日 16:00～17:00	2009 年度 CRYTREC 合同委員会 ＊CRYPTREC シンポジウム 2010 に合わせて開催

3.2　サイドチャネルセキュリティワーキンググループの開催状況

2009 年度のサイドチャネルセキュリティワーキンググループは、計 3 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　2009 年度サイドチャネルセキュリティ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 21 年 9 月 2 日 14:00～16:00	サイドチャネルセキュリティワーキンググループ活動計画 データの交換用標準フォーマットについて
第 2 回	平成 22 年 2 月 5 日 14:00～16:00	データの交換用標準フォーマットについて 実験の進め方について FPGA と ASIC の比較実験結果の検討
第 3 回	平成 22 年 3 月 2～3 日 16:00～17:00	2009 年度 CRYTREC 合同委員会 ＊CRYPTREC シンポジウム 2010 に合わせて開催

付録

付録１　早期改訂 ISO/IEC 1st WD 19790 に対するコメント

CRYPTREC comments on ISO/IEC 1st WD 19790

Date: 2010-MM-DD	Document: **SC 27 N7866**

1	2	(3)	4	5	(6)	(7)
NB[1]	**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 the NB**	**Proposed change by the NB**	**Resolution on each comment**
JP 1 [	3.133		te	It would be better to specify explicit operations of Zeroisation.	Please add the following sentence to the definition of zeroisation. “Zeroisation is not limited to zero clear of stored data and CSPs, and may include other operations such as writing constants or random numbers, and breaking data storage.”	
JP 2	7.1	Table 1	ed	Line “Life-cycle Assurance”. No separation in the second column.	Add separations.	
JP 3	7.1	Table 1	te	Line “Operational Environment”. This line is confusing. Especially the meaning of “Not applicable” in the right-down box is hard to understand.	The description in FIPS140-3 (Revised DRAFT 09/11/09) seems more adequate. "The OVERALL Security Levels 3 and 4 are NOT offered for software cryptographic modules, therefore no requirements for modifiable environment are provided."	
JP 4	7.1	5 th paragraph	ed	“shall be”	“Shall [01.04] be”	
JP 5	7.2.3	2nd and 3rd paragraphs	ed	“others services”	“other services”	
JP 6	7.3	1st paragraph	ed	interfaces(s).	interface(s).	
JP 7	7.3.2	Items 1 and 2	ed	The term SSP is used in Item 1 and CSP and PSP are used instead of SSP in Item 2.	Use SSP for both items, or use CSP and PSP for both items.	
JP 8	7.3.2	Item 2	ed	zeroization	zeroisation	

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

CRYPTREC comments on ISO/IEC 1st WD 19790

Date: 2010-MM-DD	Document: **SC 27 N7866**

1	2	(3)	4	5	(6)	(7)
NB[1]	**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 the NB**	**Proposed change by the NB**	**Resolution on each comment**
JP 9	7.3.2	The last paragraph	ed	sise	size	
JP 10	7.4.3.	Para 2	te	1) The paragraph is described. "Except for the Trusted Role(s) and Trusted Channel establishment, services using approved security functions shall[04.30] not be available to an operator until the operator's authentication is completed successfully. " 2) The paragraph says "services using approved security functions shall[04.30] not be available until the operator's authentication is completed successfully" 3) However, the next paragraph says, "Authentication data within a cryptographic module shall [04.32] be protected against unauthorised use, disclosure, modification, and substitution." 4) This means that the authentication data must be operated with cryptographic function. 5) Hence, operator's authentication will involve the services using approved security functions for protecting the authentication data. 6) It looks like contradiction. It will be better to add that the authentication services may use approved security functions.	Please rewrite as follows. "Except for the Trusted Role(s) and Trusted Channel establishment, services using approved security functions shall[04.30] not be available to an operator until the operator's authentication is completed successfully. **Whereas the operator's authentication mechanism may use approved security functions**."	
JP 11	7.5	SECURITY LEVEL 2, 2nd bullet	te	1) The second bullet is written as follows. " there shall [05.14] be no services via the HMI, SFMI, HFMI or HSMI interface to allow the operator to examine the executable code;" 2) It is not clear what "examine the executable code" means. It can be interpreted as following cases, but reader will not be sure what is correct.	Please describe the exact meaning of "examine the executable code".	

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

1	2	(3)	4	5	(6)	(7)
NB[1]	**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 the NB**	**Proposed change by the NB**	**Resolution on each comment**
				- Check the integrity of the code by checking the digital signature of the code? - Check the functional correctness of the executable code? - Or any other action of the operator to the executable code when the code is exploitable to the operator? 3) Exact meaning of the “examine the executable code” should be added.		
JP 12	7.5	SECURITY LEVEL 2 , 3rd bullet , 7th line	te	1) In the third bullet, there is the following sentence. “The digital signature or keyed message authentication code technique may consist of a single encompassing signature or keyed message authentication code or multiple disjoint signatures of which failure of any disjoint signature or keyed message authentication code shall [05.19] cause the module to enter the error state.” 2) Two new terms, “encompassing signature” and “disjoint signature” are described. 3) But the definitions of the terms are not given.	Please add the definitions of “encompassing signature” and “disjoint signature” in Clause 3 Terms and definitions.	
JP 13	7.10.1	Para 7	ed	“Clause 7.3.1” seems to be a misprint of “Clause 7.3.2.”	Please replace “Clause 7.3.1” with “Clause 7.3.2”.	
JP 14	7.10.3.7		te	Two phrases “At Security Levels 1 and 2” and “At Security Levels 3 and 4” are redundant. It is ambiguous whether the requirements for Security Levels 3 and 4 include those for Security Levels 1 and 2.	Please remove the redundant phrase “At Security Levels 1 and 2,” and replace “At Security Levels 3 and 4” with “In addition to the requirements for Security Levels 1 and 2”.	
JP 15	A.1.2 to A.1.10		te	There are bulleted requirements which lack Security Levels to be specified.	Please assign Security Levels to all requirements.	

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

CRYPTREC comments on ISO/IEC 1st WD 19790

Date: 2010-MM-DD	Document: **SC 27 N7866**

1	2	(3)	4	5	(6)	(7)
NB[1]	**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 the NB**	**Proposed change by the NB**	**Resolution on each comment**
JP 16	A.1.11	last bullet followed by "all user responsibilities..."	ed	The shape and the indentation of the bullet seem wrong. "44" seems to be a misprint of "4".	Please replace the bullet with a circular one and adjust the indent. Please replace "44" with "4".	
JP 17	F.4	Para 2	ed	There is an error message "Error! Reference sources not found" after "The associations are listed in …".	Please add an appropriate reference.	
JP 18	F.4	Table F-1	te	As Authentication mechanisms are associated with only TA, the test can be passed by adding a process making the response time fixed or randomised, which is not effective against attacks. SPA and SEMA should be associated with Authentication mechanisms, because PIN can be attacked effectively by SPA/SEMA rather than TA.	Please add the following security function to the row of "SPA and SEMA"; "Authentication mechanisms that control access to the module".	
JP 19	F.4	Table F-1	te	An RSA-CRT implementation without countermeasure is easily attacked with Fault Analysis (FA), which is not included in non-invasive attack methods. The specification of TPM requires FA countermeasure.	Please add a row for FA, with the following security function. "Approved asymmetric cryptographic algorithms" at least as a security function.	
JP 20	F.4	The last line	ed	"Annex B" seems to be a misprint of "Annex C".	Please replace "Annex B" with "Annex C".	

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

発行日　2010年5月28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