CRYPTREC Report 2008

平成 21 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 2008 年度活動報告である。

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

本年度は、「暗号技術監視委員会」とともに、2003 年 3 月に公表した「電子政府推奨暗号リスト」の見直し作業に着手した。「電子政府推奨暗号リスト」の見直しに当たっては、現行の「電子政府推奨暗号リスト」に掲載された暗号技術を再評価するだけでなく、CRYPTREC Report 2007 に述べられた通り、技術の進歩や使用環境の変化に対応する必要があるため、新たな暗号技術の公募を行うことになった。

そこで、本委員会では、「暗号技術監視委員会」と共同で、新たな暗号技術を公募する為の公募要項（案）の作成を行った。本委員会では、応募される暗号技術が実際にソフトウェアやハードウェアとして実装可能であることの確認や関連する各種データの正当性の効率的な検証を可能とするために参照ソースコードを作成するための条件などの検討を行った。また、2007 年度までの活動を引き継ぎ、暗号モジュールに対するサイドチャネル攻撃などの暗号モジュールに対する攻撃法や対策の調査研究を、暗号モジュール委員会の傘下にある電力解析実験 WG にて実施し、将来のセキュリティ要件への適用の準備を進めた。

本委員会の活動が、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。

2009 年 3 月

暗号モジュール委員会　委員長　松本　勉

本報告書の利用にあたって

本報告書は、一般的な情報セキュリティの基礎知識を有している読者を想定している。例えば、電子署名やGPKI[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活動内容と成果概要、第3章には暗号モジュール委員会の委員会開催状況を記述した。

2007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[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。

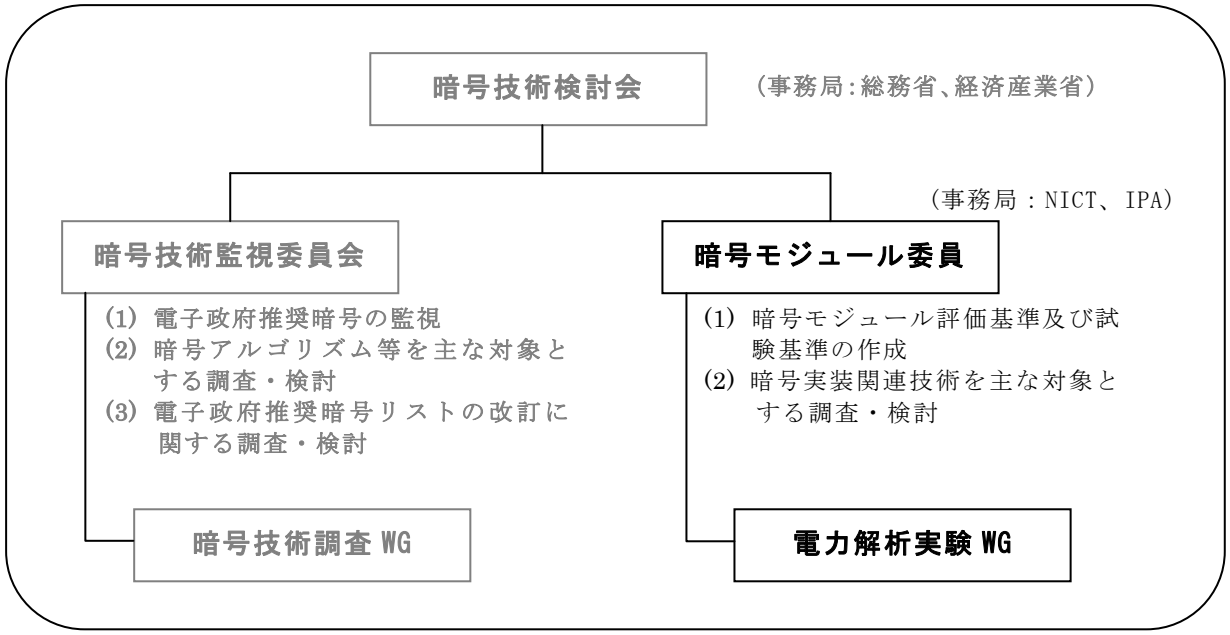

図１　2008 年度の CRYPTREC の体制

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

委員名簿

暗号モジュール委員会 （2009 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	太田　和夫	国立大学法人電気通信大学　教授
委員	亀田　繁	財団法人日本情報処理開発協会　センター長
委員	佐伯　稔	三菱電機株式会社　主席研究員
委員	佐藤　証	独立行政法人産業技術総合研究所　研究チーム長
委員	高橋　芳夫	株式会社 NTT データ　シニアエキスパート
委員	角尾　幸保	日本電気株式会社　主席研究員
委員	栃窪　孝也	日本大学　専任講師
委員	鳥居　直哉	株式会社富士通研究所　部長
委員	福永　利徳	日本電信電話株式会社　研究主任
委員	古屋　聡一	株式会社日立製作所　主任研究員
委員	森岡　澄夫	日本電気株式会社　主任研究員
委員	松崎　なつめ	パナソニック株式会社　チームリーダ

オブザーバ

氏原　正勝	警察庁　情報通信局
谷川　健	警察庁　情報通信局（2008 年 7 月まで）
赤澤　康之	警察庁　情報通信局（2008 年 7 月から）
伊東　信孝	警察大学校　警察情報通信研究センター
山本　寛繁	総務省　行政管理局
荻原　直彦	総務省　情報通信政策局
川崎　光博	総務省　情報通信政策局
増子　喬紀	総務省　情報通信政策局(2008 年 7 月まで)
梶原　亮	総務省　情報通信政策局(2008 年 7 月から)
山崎　浩史	総務省　情報通信政策局(2008 年 7 月まで)
齊藤　修啓	総務省　情報通信政策局(2008 年 7 月から)
東山　誠	外務省　大臣官房

山元　明裕　　外務省　大臣官房
森田　信輝　　経済産業省　産業技術環境局
小野塚　直人　経済産業省　商務情報政策局（2008 年 5 月まで）
下里　圭司　　経済産業省　商務情報政策局（2008 年 5 月から）
花田　高広　　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
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
　山田　安秀
　山岸　篤弘
　伊東　徹
　星野　文学
　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
　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いる。従来の公開鍵暗号評価小委員会及び共通鍵評価小委員会は暗号技術調査 WG に再編され、監視委員会で必要と判断した個別テーマに関する調査を実施している。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。

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 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

---

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）
9 CSE：Communications Security Establishment
10 CMVP：(Cryptographic Module Validation Program)

制度における暗号モジュールに対するセキュリティ要件である FIPS（Federal Information Processing Standard）PUB 140-2 が、米国より、国際標準化機関である ISO[11]（International Standard Organization）に、国際標準として提案され審議が始まったため、2004 年度からは、ISO/IEC[12] JTC[13]1 SC[14]27/WG[15]3 における標準化作業に対するコメント作成等の活動や 2006 年度に検討が開始された FISP 140-3 に対する検討作業を行ってきた。

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。

1.1.2 暗号モジュール委員会を取り巻く環境の変化

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

また、2006 年度に検討が開始された FIPS 140-3 の作成作業は、2007 年 7 月に Draft が公開された。2007 年 10 月のコメント募集を経て、FIPS 140-3 が制定される予定である。一方、ISO/IEC JTC1 SC27 では、FIPS 140-3 をベースとして ISO/IEC 19790 の改訂も提案される予定となっている。

このような環境の変化に合わせ、暗号モジュール委員会では FIPS 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、

---

[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
[18] SASEBO: サイドチャネル攻撃実験用標準評価ボード（Side-channel Attack Standard Evaluation BOard）で 2 種類の Xilinx Virtex-II Pro FPGA である xc2vp7 と xc2vp30 を搭載。

電力解析に対する技術的な蓄積を実施してきた。

1.2 暗号モジュールの試験及び認証に関する国際標準化動向

安心できる実用的な情報セキュリティシステムの構築において、安全で実装性能の高い暗号アルゴリズムの選択は不可欠の条件である。しかし、それだけでは不十分であり、暗号アルゴリズムを適切な方法で実装することが不可欠である。暗号アルゴリズムをソフトウェア及びハードウェアとして実装したもの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/カナダ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。この規格の関連文書としては、試験要件(DTR[22])と運用ガイダンス(IG[23])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。

また、NIST/CSE[24]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 に制定作業を開始している。2007 年 7 月には、FIPS 140-3 の草案が公開された。

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

2007 年 7 月に公開された草案に対するコメントは、2007 年 10 月 11 日に締め切られ、現在 NIST で、各国から寄せられたコメントを検討の上、修正が施されている。この修

SASEBO ボードに関しては、平成 19 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新たに開発を行った、Xilinx 社製 FPGA を実装した SASEBO-G、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 3 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] Derived Test Requirements
[23] Implementation Guidance
[24] Communication Security Establishment

正案は、大幅に遅れ、2009 年 3 月末現在 FIPS 140-3 草案に対する改訂版は公開されていない。その後、再度コメント募集が行われた後、米商務省に提出され、正式な FIPS 140-3 として発行されると考えられる。また、FIPS 140-3 に対応する DTR も 2009 年 3 月末現在公開されていない。

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。

2006 年 3 月に制定された ISO/IEC 19790 は、米国 NIST で進められている FIPS 140-2 の改訂をにらみ、FIPS 140-2 の後継標準となる FIPS 140-3 をベースに、早期改訂に着手することが決まっている。

なお、この ISO/IEC 19790 は、2007 年 3 月に JIS[25] X 19790 として、日本工業標準調査会(JISC[26])から日本工業規格(JIS）として制定された。また、JIS X 19790 に対応する試験規格としては、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 JIS となり、2008 年 6 月に制定された ISO/IEC 24759 は、2009 年 3 月現在、日本工業標準調査会にて、JIS 化の作業が進行中である。

さらに、ISO/IEC JTC1 SC27/WG3 では、米国 NIST における FIPS 140-3 の開発を受け、FIPS 140-3 をベースとして ISO/IEC 19790 の早期改訂を 2007 年 10 月会合で議決している。しかし、2009 年 3 月末現在改訂案の WD は提出されていない。

1.3 暗号モジュール委員会の活動状況

1.3.1 過去の経緯

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

この目的のためには、実装が適切に行われていることを確認する仕組みが必要であり、米国・カナダでは CMVP として試験及び認証の制度が実施されている。CRYPTREC では、このような制度の基となる暗号モジュールに対するセキュリティ要件等の素案作成、

[25] JIS：Japanese Industrial Standards（日本工業規格）
[26] JISC：Japanese Industrial Standards Committee（日本工業標準調査会）

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。

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

[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

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 のドラフト WD 及び 1st CD に対するコメント案を作成し、SC 27 国内委員会経由で国際事務局に提案した。

(2) 電力解析実験ワーキンググループの立ち上げ

米国では FIPS 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 の最終ドラフト案を審議し、SC 27 の国内委員会に対し、コメント案の作成に協力した。

(2) FIPS 140-3 へのコメント提出

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

(3) 電力解析実験ワーキンググループの活動

米国では FIPS 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。

(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。

---

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

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

1.3.2　2008 年度の活動概要

2008 年度暗号モジュール委員会の成果

今年度の暗号モジュール委員会の主要成果としては、次の 4 つが挙げられる。

(1) 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の公募要件作成

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）」について暗号技術検討会の依頼を受け、暗号モジュールの実装に関する第一次評価と第二次評価の評価項目について検討を行った。

(2) サイドチャネル攻撃のセキュリティ要件と NIST FIPS 140-3 DTR 等への標準化への協力

NIST による暗号モジュールセキュリティ要件 FIPS 140-3 の改訂作業が大幅に遅れ、2009 年 1 月末現在 FIPS 140-3 草案に対する改訂版は公開されていない。また、FIPS 140-3 に対応する DTR も公開されていない。

さらに、FIPS 140-3 に基づき早期改訂が予定されている ISO/IEC 19790 検討に関しては WD が提出されていない。そのため、これらの標準化に関する検討は、来年度以降に先送りすることとなった。

(3) 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。

(4) 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

第 2 章　2008 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、ハードウェア及びソフトウェア実装性評価の公募要件作成

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「暗号技術公募要項（2009 年度）（案）」について、暗号技術検討会の依頼を受け、暗号モジュールの実装性に関する第一次評価と第二次評価の評価項目の検討を行った。図 2.1 に実装性評価の位置づけの概念図を示す。

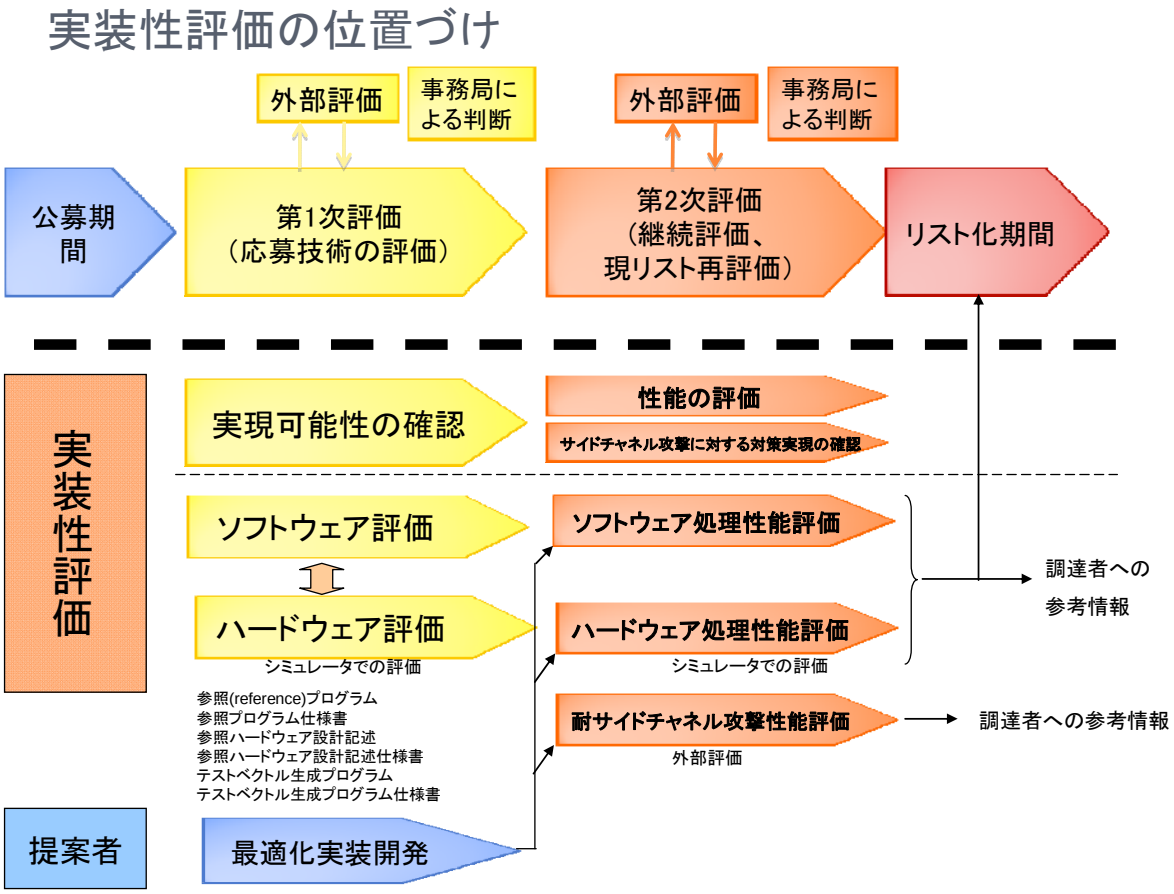

図 2.1　実装性評価の位置づけ

ア　第一次評価（2010 年 4 月～2011 年 3 月）

・　評価の目的は、応募された暗号技術が、実装ができることの確認であり、公

募要項では「実現可能性の確認」と表現する。

・ 「実現可能性の確認」は、ソフトウェア、ハードウェアの両面で確認する。

・ 「実現可能性の確認」は、アルゴリズム評価と並行して実施する。

イ 第二次評価（2011 年 4 月～2012 年 3 月）

・ 第二次評価の目的は、「性能評価」とし、ソフトウェア、ハードウェアの両面で評価を行う。

・ 評価対象：第一次評価をパスした暗号及び現リスト掲載暗号

(i) ソフトウェア処理性能評価

・ 標準的なプラットフォーム上で提案者が実装した最適化コードを用いて、処理速度、リソースの使用量等を評価する。

・ 評価結果は、リスト作成に利用するとともに、調達者へプラットフォーム選定上の参考情報（処理性能の見積もり、必要なリソース量の見積もり）として提供する。

(ii) ハードウェア処理性能評価

・ FPGA 上で、提案者が実装した最適化コードを用いて、処理速度、リソースの使用量等を評価する。

・ 評価結果は、リスト作成に利用するとともに、調達者へプラットフォーム選定上の参考情報（処理性能の見積もり、必要なリソース量の見積もり）として提供する。

(iii) サイドチャネル攻撃に対する対策実現の確認

・ 提案者による、サイドチャネル攻撃対策を施した実装を対象として、処理性能やリソースの使用量などを計測するとともに、サイドチャネル攻撃対策の有効性を確認する。

・ ソフトウェア実装／ハードウェア実装の両方を対象とする。

・ 結果を調達者へ、暗号技術を決める際の参考情報として提供する。

・ 想定するサイドチャネル攻撃としては、電力解析攻撃やタイミング攻撃とする。

2.1.2 実装性評価の詳細

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

ア ソフトウェア評価

(i) 実現可能性の確認

・ 参照プログラム、テストベクタを用いて、参照プログラムが、テストベクタを処理できることを確認する。

(ii) 性能評価

・ 評価対象：提案者が作成した最適化実装を対象とする。

・ 最適化実装コードについては、非公開とし、評価は事務局立ち会いの下で実施する。
・ 処理速度、メモリ等の使用状況（コードサイズ、作業領域サイズ）等を評価
・ インターフェース情報等に関しては、2010 年 10 月頃を目処に、事務局より提供する（Web 等での公開）。
・ 提案者からの追加の情報（最適化実装）は、2011 年 3 月頃に提出を求める。

イ　ハードウェア評価

(i) 実現可能性の確認

・ テストベクタを用いて、参照ハードウェア設計が、テストベクタを処理できることをシミュレータ上で確認する。

(ii) ハードウェア処理性能評価

・ 性能評価を行うプラットフォームとしては FPGA とする。
・ 性能評価の対象は、提案者が提出する最適化実装を用いる。
・ 最適化実装コードについては、非公開とし、評価は事務局立ち会いの下で実施する。
・ 評価項目としては､処理速度評価(クリティカルパス遅延､レイテンシー等)、リソース使用量（使用セル数）をシミュレータにより評価する。
・ インターフェース情報等に関しては、2010 年 10 月頃を目処に、事務局より提供する（Web 等での公開）。
・ 提案者からの追加の情報（最適化実装）は、2011 年 3 月頃に提出を求める。

ウ　サイドチャネル攻撃に対する対策実現の確認

・ 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。
・ 提案者から、サイドチャネル攻撃に対する対策を組み込んだ実装情報の概要情報を提供してもらう。
・ 対策を組み込んだ実装に関しては、非公開とする。
・ 提案者が提出した実装を用いて、中立の第三者（外部評価者）にサイドチャネル攻撃の実施を委託する。
・ 評価結果は暗号技術を決める際の参考情報として提供する。
・ インターフェース情報等に関しては、2010 年 3 月頃を目処に、事務局より提供する（Web 等での公開）。
・ 対策を組み込んだ実装は、2011 年 10 月頃に提出を求める。

エ　現時点で想定している実装プラットフォーム

（ア） ソフトウェアでの実現可能性の確認

・ CPU: Intel x86 アーキテクチャ互換のプロセッサ
・ Memory: 2GB 以上
・ OS: Microsoft Windows のいずれかのエディション
・ 言語：C 言語

（イ）ハードウェアでの実現可能性の確認

(i) FPGA

- Xilinx FPGA XC5VLX30 もしくは、XC5VLX50
- 言語：Verilog-HDL

(ii) 論理合成

- Xilinx 社 ISE Foundation の論理合成機能

(iii) 配置配線

- Xilinx 社 ISE Foundation の配置配線機能

(iv)論理シミュレーション

- ModelSIM XE-Ⅲ

2.2 サイドチャネル攻撃のセキュリティ要件の検討

NIST による暗号モジュールセキュリティ要件 FIPS 140-3 の改訂作業が大幅に遅れ、2009 年 1 月末現在 FIPS 140-3 草案に対する改訂版は公開されていない。また、FIPS 140-3 に対応する DTR も公開されていない。

さらに、FIPS 140-3 に基づき早期改訂が予定されている ISO/IEC 19790 検討に関しては WD が提出されていない。そのため、これらの標準化に関する検討は、来年度以降に先送りすることとなった。

2.3 暗号モジュールへの攻撃の監視と分析

暗号モジュール委員会に関連する活動としては、2008 年度も監視要員が CHES[32]および FDTC[33]へ参加し、情報収集を行い、国際会議等の報告として監視委員会にて監視状況の報告を行った。

2008 年度の監視状況は、CRYPTREC レポート 2008 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 2008 年度電力解析実験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]

[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）

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未だ具体的に決められていない。

そこで、電力解析実験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する。

2.4.2 今年度の成果概要

本ワーキンググループでは平成 18 年度の開始当時から、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]等が開発されたため、これらを利用し、FPGA と ASIC の暗号モジュールにおける実験結果の違いを調べることを主要課題として活動を行い、比較実験結果とそれに関連する実験データの統一化、標準評価方法の検討を今年度の成果とした。

(1) サイドチャネル攻撃に関する比較実験

委員が行った実験成果についてワーキンググループで検討を行った。

3 種類のサイドチャネル攻撃実験用標準評価ボード SASEBO（Xilinx 版）、SASEBO-G（Xilinx 版）、SASEBO-R（LSI 版）搭載の各 AES 暗号モジュールについて、電力相関解析(CPA[39])の比較実験を行った結果、Xilinx の FPGA と ASIC ではどちらも類似した結果となり、採取する波形データの数が多ければ攻撃は成功することが確認された。

それらは、それぞれＳボックスの作り方による実装の違いによって測定結果に違いが存在することが確認できた。

また、動作クロック周波数が低い場合と時間当たりの波形データのサンプル数が多い場合の方が、そうでない場合より攻撃成功確率が高いことが確認

[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/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。

[39] CPA：Correlation Power Analysis

され、オシロスコープの性能による、クロック周波数、サンプル間隔の条件によって攻撃の成功確率が異なることが判明した。

(2) 採取データの形式の統一化

実験で採取した波形のデータを委員等の間で共有し、相互での評価が可能となる様にデータファイルの互換性についての検討を行い、波形データ交換標準フォーマット(WXF[40])として波形データの形式の統一化を行った。

この標準フォーマットには付属情報が記述出来る様になっており、波形データの利用者は、その波形データの特性がどのようなものか参考情報として利用可能となっている。

(3) 標準評価方法の検討

電力解析の評価において最も有効な方法として、ピアソンの積率相関係数を用いた CPA について検討し、この方法を電力解析実験ワーキンググループでの標準評価方法の一つとして定めた。

また CPA の評価結果の表示方法として、縦軸を相関係数の平均とし横軸を波形数としたグラフを標準の表示方法に決めた。

結果のグラフにおいては無相関のグラフと有意なハミング重み(HW[41])／ハミング距離(HD[42])のグラフに分離できた点を正解鍵が求まる波形数の位置とし、これを判定基準として決めた。この点については、電力解析攻撃の未対策版の暗号モジュールでの相関は分離可能であるが、対策版ではその点を求めるには膨大な波形数が必要と推定した。

(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

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、2008 年度の発表についてまとめた。

2.4.3 委員構成

電力解析実験ワーキンググループ （2009 年 3 月現在）

[40] WXF : Waveform data eXchange Format
[41] HW : Hamming Weight
[42] HD : Hamming Distance

委員長	松本　勉	国立大学法人横浜国立大学　教授
委員	今福　健太郎	独立行政法人産業技術総合研究所　研究チーム長
委員	黒川　恭一	防衛大学校　教授
委員	後藤　敏	早稲田大学　大学院　教授
委員	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　チームリーダー
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	栃窪　孝也	日本大学　専任講師
委員	鳥居　直哉	株式会社富士通研究所　部長
委員	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	古屋　聡一	株式会社日立製作所　主任研究員
委員	本間　尚文	国立大学法人東北大学　大学院　助教
委員	森岡　澄夫	日本電気株式会社　主任研究員
委員	山越　公洋	日本電信電話株式会社　研究主任

事務局

独立行政法人　情報処理推進機構
- 山岸　篤弘
- 伊東　徹
- 鈴木　幸子

独立行政法人　情報通信研究機構
- 黒川　貴司
- 金森　祥子

2.4.4　サイドチャネル攻撃に関する比較実験

(1) 防衛大学校による FPGA と ASIC の CPA の比較実験結果の報告

防衛大学校から SASEBO(Xilinx)に搭載された、電力解析攻撃への対策が行われていない AES の暗号モジュールと、SASEBO-R(ASIC)に搭載された、S ボックスの作り方による実装の異なる、電力解析攻撃への対策が行われていない 5 種類の AES の暗号モジュール[43]について CPA を行った実験結果のデータについて説明が行われた。(図 2.2)

ASIC の結果の波形データのグラフは FPGA の場合と類似の結果となった。これらの、攻撃への対策が行われていない暗号モジュールでは、採取する波形数を増やした場合に鍵の情報は取得可能となったが、それぞれの S ボックスの作り方による実装の違いで測定結果に違いが存在することが確認された。

また、東北大学からの同様の実験に関する参考意見として、SASEBO(Xilinx)に搭載された AES について、ハミング重み(HW)モデルを用いた評価を行った場合では鍵の推定が出来なかった。ASIC について、CPA では 500 波形位から鍵の推定が可能であった。AND-XOR 1 段（PPRM[44]1[45]に相当）の場合では 4000 波形位で全ての鍵が推定出来た。ハミング距離(HD)でも同じ程度であったが、ハミング重みでは更に早く相関が収束した。全般的な傾向として、CPA では他の評価方法より、少ない波形数で全ての回路構成で全ての鍵を推定出来た。

---

[43] 5 種類の暗号モジュール：①Normal(enc/dec)（合成体（暗号化/復号実装)），②case（CASE 文記述（暗号化のみ実装)），③AND-XOR1 段（暗号化のみ実装），④AND-XOR3 段（暗号化のみ実装），⑤FPGA ネットリスト（①の FPGA 用ネットリストを使用）について実験を行った。

[44] PPRM：Positive Polarity Reed-Muller

[45] PPRM1：Positive Polarity Reed-Muller 理論による 1 段の AND-XOR ロジックで S-box を記述した AES 実装。(暗号化のみ実装)

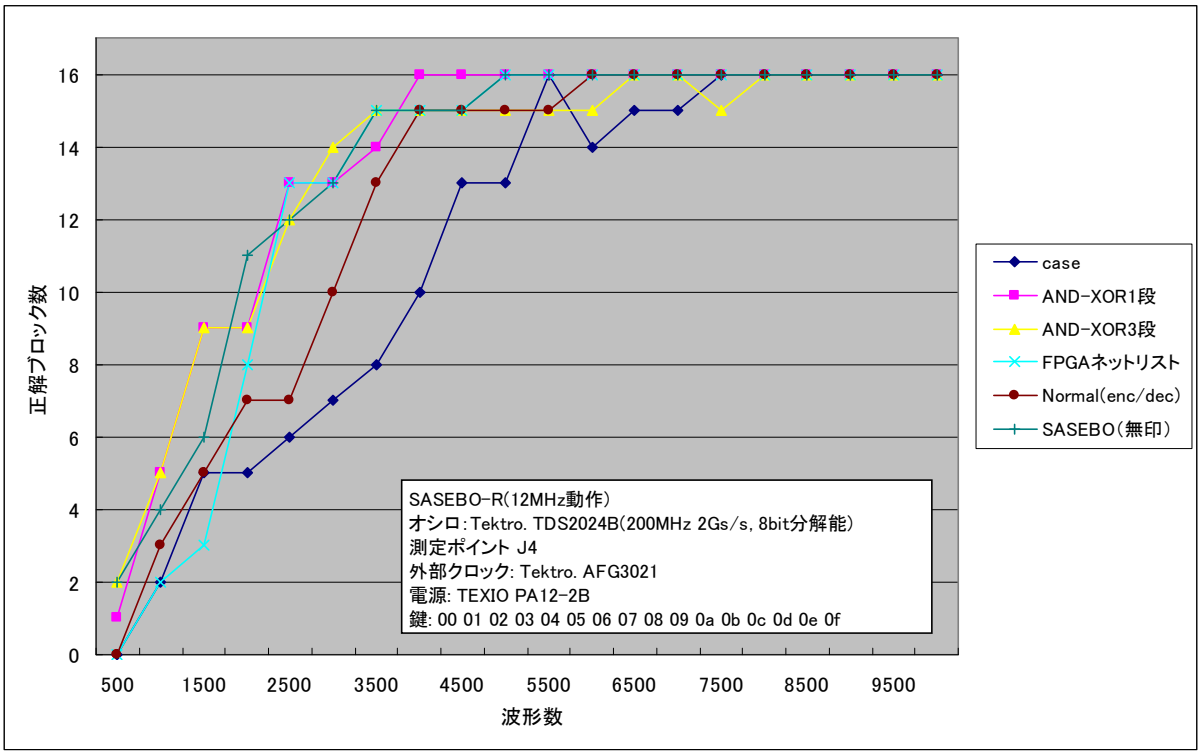

図 2.2　実装による実験データの差異

(2) 横浜国立大学／NTT データよる実験と比較の報告

横浜国立大学／NTT データより SASEBO-R(ASIC)の防衛大学校、東北大学／産業技術総合研究所との CPA についての 3 種類の実験結果の比較について報告された。(図 2.3)

実験結果を比較すると、横浜国立大学／NTT データの実験では動作クロック周波数が 6MHz と他の実験より低く設定されており、更に波形データのサンプル間隔も 5GS/s と時間あたりのサンプル数が他の実験より多くなっており、この場合において、実験結果の表から TBL[46],PPRM1、PPRM3[47]の何れのモジュールの場合でも他の実験結果[48]よりエラーの数が少なくなっている。また、防衛大学校と東北大学／産業技術総合研究所の結果の比較においても、クロック周波数とサンプル数の関係は同様の傾向になっており、クロック周

[46] TBL : S-box を CASE 文で記述した実装。(暗号化のみ実装)

[47] PPRM3 : Positive Polarity Reed-Muller 理論による 3 段の AND-XOR ロジックで S-box を記述した AES 実装。(暗号化のみ実装)

[48] 他の実験結果:Comp(ENC/DEC)は合成体による S-box を用いた実装(暗号化/復号実装), Comp(ENC)は合成体による S-box を用いた実装（暗号化のみ実装), S1（FPGANET）は合成体による S-box を用いたのと同じ RTL(Register Transfer Level)ソースで FPGA と同等のノードのネットリストとなる様に論理合成したもの（暗号化/復号実装)。

波数が低く、時間当たりのサンプル数も多い方が、攻撃成功確率が高いことが確認された。

波形数3000個のTBL，PPRM1，PPRM3の3つに注目してみると
・防衛大はTBLが他よりもエラーが多く，　TBLが1番目にエラーが多い，
・東北大はPPRM1=4だけがエラーが少なく，　TBLは2番目にエラーが多い．
・横浜国大はTBLが一番エラーが少なく，　TBLは3番目である．

	防衛大学校（黒川研究室）	東北大/産総研	横浜国大
SASEBO設定	12MHz　J7経由で外部クロックを使用	24MHz　制御FPGAからクロック供給	6MHz　制御FPGAからクロック供給
	測定ポイント:J4	GND側を測定，シャント抵抗:2.2Ω （他のシャント抵抗はショート）	GND側を測定
	平文:128bitの乱数 鍵:00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f	平文:カウンタ（0x0～0x493df） 鍵:2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c	平文：カウンタ（0x1～0x10000） 鍵:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
測定	TDS2024B（200MHz，2GS/s，8bit） 垂直軸:10mV/DIV 時間軸:2GS/s	MSO6104A（1GHz，4GS/s） 時間軸:1GS/s	WR6050A（500MHz，5GS/s,8bit） 時間軸:5GS/s
		Agilent 1130A with SMA probe head （差動プローブを使用）	
	1万波形	30万波形	6万5千波形（1024*64）→ WEB公開中
分析	CPAを実施（HDで1万波形）	CPAを実施（HDで3万波形，HWで30万）	HW，HDで相関係数をグラフ化，CPA実施

	#3k	#5k	#10k
Comp（ENC/DEC）	6	1	0
Comp（ENC）	-	-	-
TBL	9	3	0
PPRM1	2	0	0
PPRM3	3	1	0
S1（FPGANET）	3	0	0
SASEBO（初代）	3	1	0

	#3k	#5k	#10k
Comp（ENC/DEC）	16	16	9
Comp（ENC）	16	15	14
TBL	14	12	2
PPRM1	4	1	0
PPRM3	15	8	1
S1（FPGANET）	-	-	-
SASEBO（初代）	2	1	1

	#3k	#5k	#10k
Comp（ENC/DEC）	-	-	-
Comp（ENC）	最大8	最大4	0
TBL	0	0	0
PPRM1	最大1	0	0
PPRM3	最大1	0	0
S1（FPGANET）	-	-	-
SASEBO（初代）	-	-	-

数値は，16ブロック中のエラーブロック数

図 2.3　横浜国大／NTT データよる実験と比較

2.4.5　採取データの形式の統一化

横浜国立大学と防衛大学校より、暗号モジュールの測定データの測定環境の違いによる影響の切り分けを行うため、採取波形のデータベースの構築が考案された。（図 2.4）

そして、波形データの形式の共通化が検討され、横浜国立大学からサイドチャネル攻撃実験データ交換用標準フォーマット(WXF)として提案された。この標準フォーマットはサイドチャネル攻撃実験を行うための測定データを対象にして測定データを評価者の間で共有可能とするための標準形式にすることを目的としてワーキンググループで検討を行った。

この標準フォーマットは波形データの採取時の特性等を付属情報として開示可能な範囲で記述することとしており、そのデータがどの様な採取波形なのか、波形データ

の利用者に評価のための参考情報として利用出来るようにしている。

尚、このフォーマットは横浜国立大学の web サイトで公開されている。
交換用標準フォーマット(WXF)の URL：
http://ipsr.ynu.ac.jp/wxf/index.html

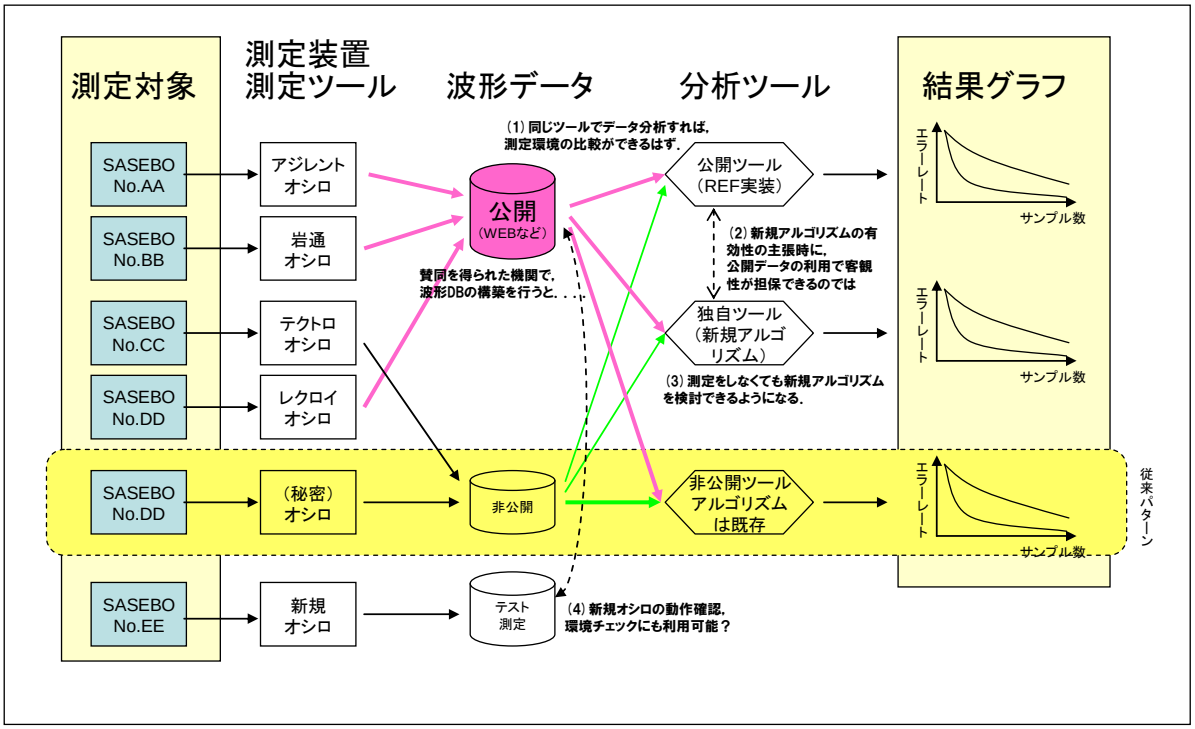

図 2.4　波形データ（DB）の共有化について標準フォーマットの検討

2.4.5.1 データ交換用標準フォーマット(WXF)の概要

「１セットの波形」と「付属情報」を“ZIP ファイル”に収め、波形と付属情報を参照する方法（ファイル名など）をZIP ファイル内の“CATALOG.txt”ファイルに記述する。

(1) １セットの波形

・オシロスコープ等の機器で測定した一区切りの時系列データを「1 波形」、ある複数(1 個以上)の波形の集まりを「1 セットの波形」、とする。

・1 波形＝1 ファイルに収める形式に対応することを必須とし、他の形式はオプ

ションとして別途検討する。

（他の形式の例： 複数波形＝1 ファイル、1 波形＝複数ファイル。）

(2) 付属情報

・平文/暗号文、鍵、波形のスケール（垂直，水平）などの関連する情報をまとめて「付属情報」とする。

・付属情報はプレーンテキストで 「名前(TAG)： 値」 等の形式で記述する。

例) SamplingRate: 5000000

2.4.5.2 ZIP ファイルの例

ZIP ファイルの例（図 2.5）

・測定データそのものである mat ファイルのほかには、3 つのテキストを同封すればよい。（mat ファイルは Matlab のデータファイル）

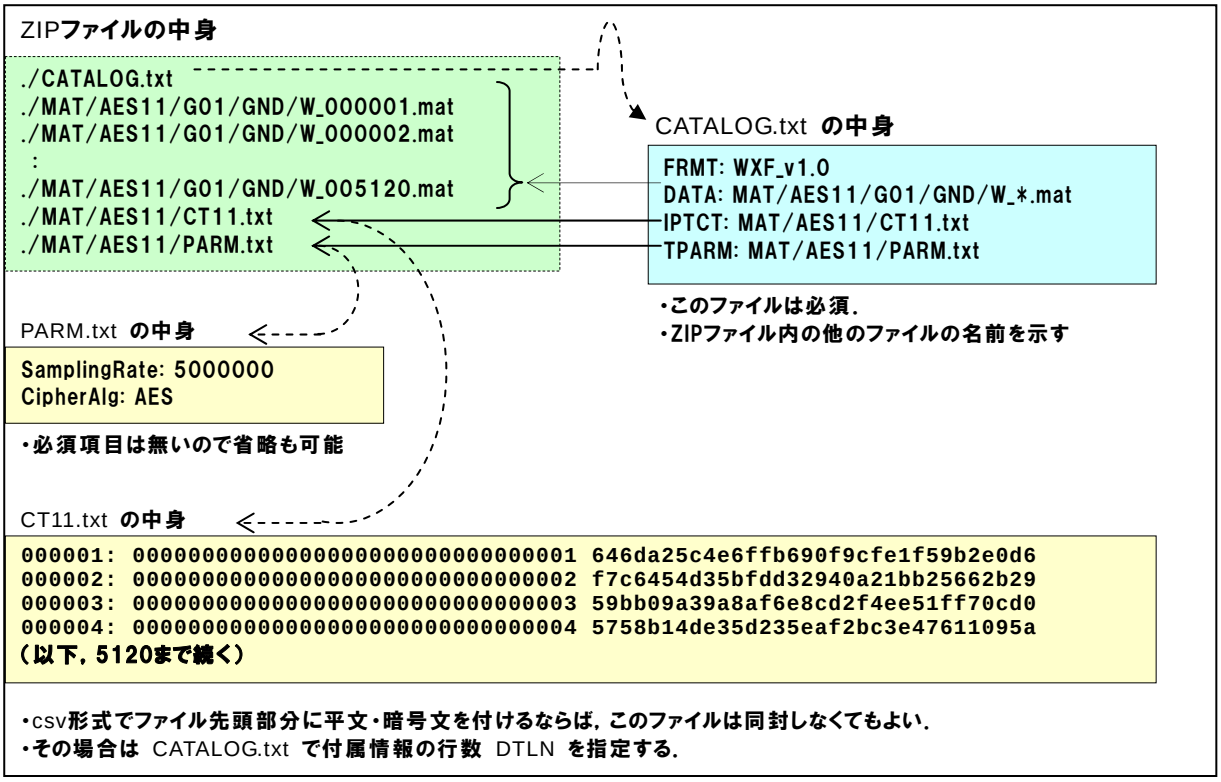

図 2.5　ZIP ファイルの例

2.4.5.3 波形データの形式

波形データの種類は mat, csv, bin の 3 種類とした。

(1) mat 形式：

・変数名 w のベクトルデータを、matlab の save コマンドでファイル出力し

た matlab 独自形式のバイナリ。

・付属情報を記載するために struct array 型の変数 s を mat 形式のファイルに入れてもよい。

その場合、TAG 部をフィールド名に、VAL 部をその値に対応させる。

・倍精度浮動小数点（8byte）でも圧縮されるためファイルサイズは bin 形式と同程度になる。Octave でも利用可能。

(2) csv 形式：

・CRLF で区切られた 1 行に 1 サンプルの値を、整数あるいは浮動小数点表示でファイル出力したプレーンテキスト。

・オプションでファイルの先頭に付属情報を記載可能とする。
（matlab では save –ascii –double で出力、txtread コマンドで指定行数をスキップして読み込める）

・1 レコード（=1 行)には 1 フィールドのみがあり（","を含まない)、CSV としてのヘッダ行は無いものとする（RFC4180 を参照)。

・フィールドは文字列の場合でも、ダブルコーテーションで括らない。最後のレコードにも CRLF を付ける。

・double 型のデータをファイル出力するとサイズが大きめ（10 倍以上）になり、HDD に展開するには具合が悪い。

・ZIP 圧縮したまま使用するならば問題はない。

(3) bin 形式：

・8bit or 16bit or 64bit のデータをヘッダや構造無しに単純に並べたバイナリファイル。

・8bit は int8 型 または uint8 型とする。

・16bit は int16 型 または uint16 型で Low byte を先にする（little-endian)。

・64bit は double 型で IEEE754 の little-endian とする。

・オシロから取り出したデータを Offset や Gain などのスケール変換をせずに保存した値として入れることを想定。

2.4.5.4 今後の課題

(1) 波形データの特性等の付属情報の記述のための名称（TAG）の拡張性について（XML 記述の採用の要否)。

(2) ブロック暗号以外の暗号についての名称（TAG）の追加や、値（VAL）で使用する単語やフレーズの整理。

(3) 複数波形＝1 ファイルの導入の検討として、どのような波形を 1 ファイルとするか。

また委員からの意見として、波形データフォーマットの統一化だけでは解決できな

い問題点について、選択平文での攻撃等によるインターラクティブな分析を行う場合では、単に実験データを交換するだけでは追試が出来ず、他の実験条件も揃えねばならない。この点は実験上での制約事項となっているため、どのように対処するかが今後の課題である。

2.4.6 実験データの標準評価方法の検討

暗号モジュールの電力解析の評価において最も有効な方法として、CPA が上げられるが、ピアソンの積率相関係数を用いた評価方法について横浜国大／NTT データから標準化が提案された。

$$\text{ピアソンの相関係数} = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i-\bar{y})^2}}$$

この方法を検討し、電力解析実験ワーキンググループでの標準評価方法の一つとして定めた。

また、CPA の評価結果について、縦軸を相関係数の平均とし横軸を波形数としたグラフを電力解析実験ワーキンググループでの標準の表示方法の一つとした。（図 2.6）

結果のグラフにおいては無相関のグラフ（HD9[49]）と有意なハミング重み／ハミング距離のグラフ（HW10[50]，HW11[51]，HD11[52]）に分離できた点（HD11 と HD9 の分離点）を正解鍵が求まる波形数の位置とし、判定基準とすることとした。この分離点に関しては、電力解析攻撃の未対策版の暗号モジュールでの相関は分離可能であるが、対策版ではその点を求めるには膨大な波形数が必要と思われるため、今後の検討課題である。

尚、この評価方法は「相関係数について -- WXF データの分析」として横浜国立大学の web サイトで公開されている。

「相関係数について -- WXF データの分析」の URL：

http://ipsr.ynu.ac.jp/wxf/wxf_CORR_v9.pdf

[49] HD9：AES の PPRM1 の 9 ラウンドのハミング距離
[50] HD10：AES の PPRM1 の 10 ラウンドのハミング距離
[51] HW11：AES の PPRM1 の 11 ラウンドのハミング重み
[52] HD11：AES の PPRM1 の 11 ラウンドのハミング距離

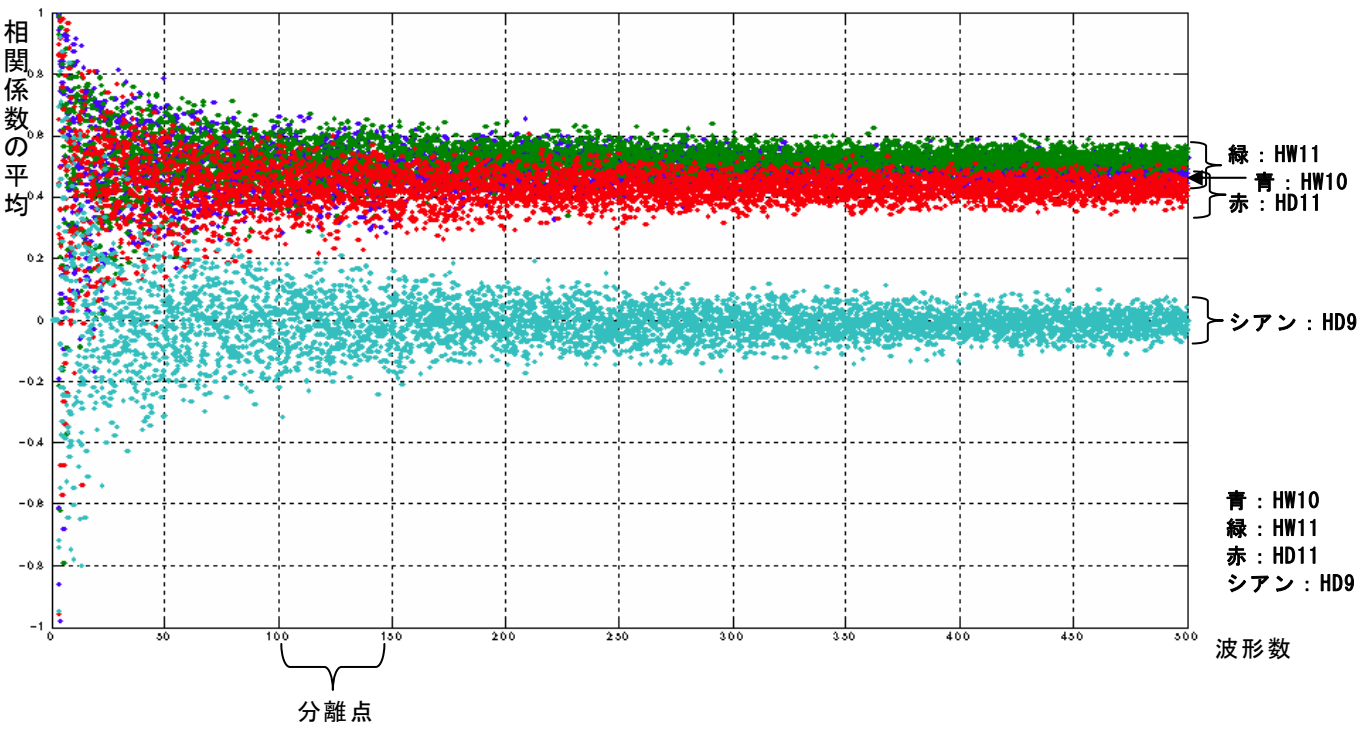

図 2.6　電力解析攻撃の未対策の AES 暗号モジュール(PPRM3)に対する CPA の結果の表示

2.4.7　電力解析攻撃実験のための評価ボードを利用した研究の調査

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、電力解析実験ワーキンググループの委員による、2008 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	SASEBO ボードに搭載された AES 回路へのサイドチャネル攻撃とその検証	ISEC[53]	2008.5.16	南崎 大作，岩井 啓輔，黒川 恭一（防衛大学校）	SASEBO
2	サイドチャネル攻撃評価用自動測定ソフトウェアの開発	ISEC	2008.5.16	岩井 啓輔，南崎 大作，黒川 恭一（防衛大学校）	SASEBO
3	Collision-Based Power Analysis of Modular Exponentiation Using Chosen-Message Pairs	CHES2008	2008.8.11	本間 尚文，宮本 篤志，青木 孝文（東北大学），佐藤 証（産業技術総合研究所），Adi Shamir(ワイツマン研究所)	SASEBO
4	High-Performance Concurrent Error Detection Scheme for AES Hardware	CHES2008	2008.8.11	佐藤 証（産業技術総合研究所），本間 尚文，菅原 健，青木 孝文（東北大学）	SASEBO
5	鍵候補の篩い分けによる CPA の	CSS2008 D5-1[54]	2008.10.9	片下 敏宏，佐藤 証(産業技術総	SASEBO

[53] ISEC：情報セキュリティ研究会（電子情報通信学会）
[54] CSS：Computer Security Symposium（情報処理学会）

	高速化と鍵推定精度の向上			合研究所),菅原 健, 本間 尚文, 青木 孝文(東北大学)	
6	電源ライン上の漏洩情報を用いたサイドチャネル攻撃	CSS2008 D5-2	2008.10.9	林 優一, 菅原 健, 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
7	標準評価基板上の ASIC への差分電力解析実験	CSS2008 D5-3	2008.10.9	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
8	暗号モジュールへの信号ラインからのサイドチャネル攻撃(2)- 詳細実験結果	CSS2008 D5-4	2008.10.9	渡部 良太, 高橋 芳夫, 松本 勉(横浜国立大学)	SASEBO
9	SASEBO における FPGA に対する電力解析/電磁波解析実験	ISEC	2008.11.13	庄司 陽彦(株式会社ワイ・デー・ケー/情報セキュリティ大学院大学), 野澤 晃, 木村 隆幸(株式会社ワイ・デー・ケー), 洲崎 智保, 山下 哲孝, 角尾 幸保(日本電気株式会社)	SASEBO
10	FPGA & ASIC Implementation of Differential Power Analysis Attack on AES	INSCRYPT[55]	2008.12.15	Guoyu QIAN, Yibo FAN(早稲田大学), 角尾 幸保(日本電気株式会社), 池永 剛,後藤 敏(早稲田大学)	SASEBO-G SASEBO-R
11	CPA 攻撃用実験環境の構築	ISEC	2008.12.17	南崎 大作, 岩井 啓輔, 黒川 恭一(防衛大学校)	SASEBO
12	テーブルネットワーク型AES実装の新手法の提案(2)	SCIS[56]	2009.1.20	山口 晃由, 佐藤 恒夫(三菱電機株式会社)	INSTAC-8
13	自己完結型テンプレート攻撃	SCIS	2009.1.20	鈴木 大輔(三菱電機株式会社/横浜国立大学), 佐伯 稔(三菱電機株式会社), 松本 勉(横浜国立大学)	SASEBO-R
14	ブロック暗号の回路アーキテクチャに対するサイドチャネル耐性評価(1)	SCIS	2009.1.20	鈴木 大輔(三菱電機株式会社/横浜国立大学), 佐伯 稔, 清水 孝一(三菱電機株式会社)	SASEBO-R
15	ブロック暗号の回路アーキテクチャに対するサイドチャネル耐性評価(2)	SCIS	2009.1.20	佐伯 稔(三菱電機株式会社), 鈴木 大輔(三菱電機株式会社/横浜国立大学), 清水 孝一(三菱電機株式会社)	SASEBO-R
16	RSL技術を用いた耐DPA暗号LSIの設計手法 ープロトタイプ LSI に対する DPA 評価結果ー	SCIS	2009.1.20	佐伯 稔(三菱電機株式会社), 鈴木 大輔(三菱電機株式会社/横浜国立大学)	SASEBO-R
17	サイドチャネル攻撃評価用 ISO/IEC 標準暗号プロセッサの開発	SCIS	2009.1.21	本間 尚文, 宮本 篤志, 菅原 健, 青木 孝文(東北大学), 佐藤 証(産業技術総合研究所)	SASEBO-R
18	べき乗剰余演算に対する比較電力解析の応用	SCIS	2009.1.21	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
19	電磁波を利用した故障利用攻撃の実験手法に関する一考察	SCIS	2009.1.21	田中 秀磨(情報通信研究機構)	SASEBO
20	高周波クロックによる RSL 技術を用いた AES へのフォールト攻撃実験	SCIS	2009.1.21	八木 達哉, 崎山 一男, 太田 和夫(電気通信大学)	SASEBO-R
21	フォールト混入時における RSL 技術による暗号回路モデルを用い	SCIS	2009.1.21	泉 雅巳, 太田 和夫, 崎山 一男(電気通信大学)	SASEBO-R

[55] INSCRYPT : International Confernces on Information Security and Cryptology (Chinese Association for Cryptologic Research and The State Key Laboratory of Information Security (SKLOIS) of China)

[56] 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)

	た安全性解析				
22	電力解析と電荷の充放電に関する考察	SCIS	2009.1.22	品川 宗介，市川 哲也（三菱電機エンジニアリング株式会社），佐藤 恒夫（三菱電機株式会社）	SASEBO-R
23	SASEBO における FPGA に対する電力解析／電磁波解析実験	SCIS	2009.1.22	庄司 陽彦（株式会社ワイ・デー・ケー／情報セキュリティ大学院大学），野澤 晃，木村 隆幸（株式会社ワイ・デー・ケー），洲崎 智保，山下 哲孝，角尾 幸保（日本電気株式会社）	INSTAC-32 SASEBO
24	信号処理を利用した SASEBO における差分電力解析	SCIS	2009.1.22	山下 哲孝，洲崎 智保（日本電気株式会社），庄司 陽彦，野澤 晃，木村 隆幸（株式会社ワイ・デー・ケー），角尾 幸保（日本電気株式会社）	SASEBO
25	波形選別による差分電力解析の改善について	SCIS	2009.1.22	野澤 晃，庄司 陽彦，木村 隆幸（株式会社ワイ・デー・ケー），洲崎 智保，山下 哲孝，角尾 幸保（日本電気株式会社）	SASEBO
26	最近傍から計測した磁界を用いた差分電磁波解析	SCIS	2009.1.22	菅原 健，鳥塚 英樹，本間 尚文（東北大学），佐藤 証（産業技術総合研究所），青木 孝文，山口 正洋（東北大学）	SASEBO-R
27	サイドチャネル解析研究に役立つ波形データ交換用標準フォーマット WXF の提案	SCIS	2009.1.22	松本 勉（横浜国立大学），高橋 芳夫(横浜国立大学/株式会社 NTT データ）	SASEBO-R
28	CPA に対するデカップリングキャパシタの影響の予備検証	SCIS	2009.1.22	片下 敏宏，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-R

(1) SASEBO ボードに搭載された AES 回路へのサイドチャネル攻撃とその検証

南崎 大作，岩井 啓輔，黒川 恭一（防衛大学校）

ISEC 2008-1（2008 年 5 月 16 日）

サイドチャネル攻撃に関する研究が盛んに行われている昨今、INSTAC32 に準拠した SASEBO ボードが開発された。この論文では、SASEBO に東北大学より提供された ECB モードの AES を搭載してサイドチャネル攻撃の一種である CPA(Correlation Power Analysis)を試みた結果を示した。

(2) サイドチャネル攻撃評価用自動測定ソフトウェアの開発

岩井 啓輔，南崎 大作，黒川 恭一（防衛大学校）

ISEC 2008-2（2008 年 5 月 16 日）

サイドチャネル攻撃の評価のためのハードウェア環境は、INSTAC の策定により整いつつあるのに対して、測定環境や、解析ソフトウェアについての標準化はなされておらず、依然として個々の実験環境に大きく依存している。

この研究では、デジタルオシロスコープの制御、大量の動作波形の自動収集、データの解析等を簡単なユーザインタフェースで操作可能な、サイドャネル攻撃評価用ソフトウェアを開発した。サイドチャネル標準評価ボード SASEBO に実装された AES 暗号に対して

このソフトウェアを用いて CPA 攻撃を試みた結果を示した。

(3) Collision-Based Power Analysis of Modular Exponentiation Using Chosen-Message Pairs

本間 尚文，宮本 篤志，青木 孝文（東北大学），佐藤 証（産業技術総合研究所），Adi Shamir(ワイツマン研究所)

CHES2008 （2008 年 8 月 11 日）

この論文は、二箇所の異なった位置での電力検出による、自乗演算の間の衝突を生成するための特定の入力対を用いた冪剰余に基づく公開鍵暗号系に対して新たな選択文電力解析攻撃を提案した。新たな攻撃法は、バイナリー(左から右と、右から左の)法、m-ary 法、およびスライディングウィンドウ法の冪法プロセスのすべての標準実装に適用できた。また、提案した攻撃を使用することによって、幾つかの場合でダミーの乗算を挿入する SPA 対策を破ることができた。FPGA とパワーPC プロセッサの上に RSA のハードウェアとソフトウェア実装で、攻撃の有効性は本実験によってそれぞれ示された。新しい衝突生成法に加えて、記録された信号にノイズが存在しクロックにいくつかのジッタが有る場合でも衝突を検出する、高精度波形適合の技法を示した。

(4) High-Performance Concurrent Error Detection Scheme for AES Hardware

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

CHES2008 （2008 年 8 月 11 日）

この論文はブロック暗号 AES のハードウェア実装での効率的な同時発生の誤り検出方法を提案した。提案方法は、追加演算装置を必要とせず、単にラウンド関数ブロックを 2 つのサブブロックに分割して、暗号化(または、復号)と誤り検出に交互にサブブロックを使用した。クロック周期の数は倍になったが、最大動作周波数はサブブロックの短くされたクリティカルパスにより増加した。提案方法にはサイズと速度に関してハードウェア性能に限定的な影響があった。提案方法による AES ハードウェアは、サイズと速度に最適化のオプションがある 90nm の CMOS 標準セルライブラリを使用することで設計構成された。コンパクトと高速な実装はそれぞれ 2.21Gbps@16.1Kgates と 3.21Gbps@24.1Kgates の性能を実現した。それに対して、誤り検出のない AES ハードウェアの性能はコンパクトなバージョンでは 1.66Gbps@12.9Kgates で、高速なバージョンでは 4.22Gbps@30.7Kgates であった。誤り検出の有無にかかわらず性能の間には、わずかな違いしかなかった。誤り検出による性能のオーバーヘッドは、サイズと速度の間の最適バランスで評価して、最大で 14.5%と見積った。逆に、提案手法の AES ハードウェアでは、幾つかの場合では、より良い性能となった。パイプライン演算が CTR モードのように行われた場合、さらにサブブロックを分割することによって、容易にスループットを上げることができた。提案された誤り検出方法はこの研究における AES に適用されたが、また、他のアルゴリズムにも効率的に適用可能である。

(5) 鍵候補の篩い分けによる CPA の高速化と鍵推定精度の向上

片下 敏宏，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)

CSS 2008 D5-1 （2008 年 10 月 9 日）

本論文では、CPA(Correlation Power Aalisys) による電力解析に鍵候補の篩い分けを適用し、高速化と鍵推定の精度を向上させる手法を提案した。また、サイドチャネル標準評価ボードSASEBO(Side-channel Attack Standard Evaluation Board) 上のFPGA に搭載したAES モジュールの電力解析実験を実施し、提案手法と従来手法の比較を行った。その結果、提案手法は5,000 個の電力波形のとき約26%の処理時間が削減され、また鍵推定の精度も向上させることができた。

(6) 電源ライン上の漏洩情報を用いたサイドチャネル攻撃

林 優一，菅原 健，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)

CSS 2008 D5-2 （2008 年 10 月 9 日）

サイドチャネル攻撃は、暗号モジュールが発生する電力波形等に漏洩している鍵情報を解析する攻撃法である。これまでの多くの論文では電力観測専用の端子を設けるなどした実験専用の基板等が用いられ、その取得波形の解析アルゴリズムにおける推定鍵の精度や処理速度向上が議論の中心となっていた。本論文では，暗号モジュールに改造をほどこすことなく、本体から離れた電源線や通信線上で暗号処理の電力波形を観測する手法を提案し、CPA (Correlation Power Analysis) において正しく鍵が導出できることを示した。そして、EMC (Electro-Magnetic Compatibility) の研究の視点から、その波形取得の原理を説明した。

(7) 標準評価基板上の ASIC への差分電力解析実験

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)

CSS 2008 D5-3 （2008 年 10 月 9 日）

この論文では、ASIC(専用LSI)実装した暗号モジュールを搭載した評価基板SASEBO-Rを用いた電力解析実験について述べている。SASEBO-R の構成を述べるとともに、ASIC実装された共通鍵暗号AES 回路に対する差分電力解析を示した。ASIC に搭載されたS-box の実装方式が異なる複数のAES 回路全てに差分電力解析を適用し、それらの結果の違いを考察した。また、FPGA実装したAES 回路を用いた場合の解析結果との比較を示した。

(8) 暗号モジュールへの信号ラインからのサイドチャネル攻撃（２）- 詳細実験結果

渡部 良太，高橋 芳夫，松本 勉(横浜国立大学)

CSS 2008 D5-4 （2008 年 10 月 9 日）

サイドチャネル攻撃の一つに、暗号処理中のハードウェアの消費電力を分析することにより暗号鍵などの秘密情報を暴露しようとする電力解析攻撃がある。消費電力の測定は電源ラインで行えることがよく知られており、論文等で報告される結果はほとんど電源ラインからの測定を用いている。しかし、電源ラインと電気的に関連のある測定ポイントであれば、電源ラインで測定した消費電力から得られる情報と同様な情報が得られる可能性がある。筆者らはそのような消費電力の測定ポイントとして信号ラインに注目していた。既に、2008 年 2 月の電子情報通信学会情報セキュリティ研究会において、FPGA に実装した AES を対象として、信号ラインからでも電力解析攻撃ができることを報告されているが、本論文では信号ラインからのサイドチャネル攻撃について SASEBO 上に FPGA 実装した AES を例として詳細に検討した結果を報告した。

(9) SASEBO における FPGA に対する電力解析/電磁波解析実験

庄司 陽彦（株式会社ワイ・デー・ケー/情報セキュリティ大），野澤 晃，木村 隆幸（株式会社ワイ・デー・ケー），洲崎 智保，山下 哲孝，角尾 幸保（日本電気株式会社）

ISEC 2008-77（2008 年 11 月 13 日）

INSTAC-32 準拠ボード上で動作する暗号処理に対してサイドチャネル攻撃の手法である「電力解析」と「電磁波解析」の実験を行った際は、電力においてはビット単位で着目した場合に得られるサイドチャネル情報がほぼ均等となるのに対して、電磁波においてはビット単位で着目した場合に得られるサイドチャネル情報に偏りが存在するという結果が得られた。この論文では、サイドチャネル攻撃用標準評価ボード SASEBO 上の FPGA で動作する暗号処理に対して電力解析と電磁波解析を実施し、同様の偏りが見られるかを確認した。しかしながら、SASEBO において得られた電力／電磁波のサイドチャネル情報を、ビット単位に分類を行い、得られるレベルの比較をしたが、双方の偏りの大きさに違いがほとんど見られない結果となった。この結果より、偏りに違いがみられなかった原因について考察した。

(10) FPGA & ASIC Implementation of Differential Power Analysis Attack on AES

Guoyu QIAN，Yibo FAN(早稲田大学)，角尾 幸保(日本電気株式会社），池永 剛，後藤 敏(早稲田大学)

Inscrypt2008 （2008 年 12 月 15 日）

Advanced Encryption Standard (AES)は米国政府によって採用された新たなブロック暗号の標準である。相関係数を基にした差分電力解析(DPA)攻撃は暗号装置と秘密鍵導出への効果的な手法である。近年、更により多くの人々がこの研究分野に興味を持ち始めている。本論文では、筆者らはAES暗号と相関DPA攻撃の実験環境を構築した。筆者らはFPGAとASICボードの双方で攻撃に成功した。実験結果より筆者らは2種類のボードにおいてその効果と正確性を解析した。更に、筆者らはFPGAとASICの消費した電力のデータを比較し、その詳細について述べた。FPGAでの攻撃は困難ではなかったが、ASICでの攻

撃については消費電力の関係から、より困難で成功率が低かった。筆者らの方法はまた詳細な電力消費測定の攻撃の効果に結び付く最初の一歩であった。

(11) CPA 攻撃用実験環境の構築

南崎 大作，岩井 啓輔，黒川 恭一（防衛大学校）

ISEC 2008-99（2008 年 12 月 17 日）

サイドチャネル攻撃の統一された評価手法の確立を目的として、サイドチャネル攻撃標準評価ボード(SASEBO)が開発された。

この論文では SASEBO に対して電力解析攻撃の一種である CPA(Correlation Power Analysis)攻撃を行い、測定条件が CPA の結果に与える影響を検証し、最良な攻撃結果を得られるような実験環境について考察した。

(12) テーブルネットワーク型 AES 実装の新手法の提案(2)

山口 晃由，佐藤 恒夫（三菱電機株式会社）

SCIS 2009　1A1-1（2009 年 1 月 20 日）

差分電力解析の対策としてソフトウェアベースでのテーブルネットワークを用いる手法が提案されている。これは、設計者のみが知り得る全単射変換処理を組み込んだテーブルを用いて暗号処理を行うことで、暗号本来の中間変数と、実際に演算される中間変数との相関をなくし、差分電力解析を不可能にするものである。しかし、従来のテーブルネットワーク実装では各拡大鍵に対応してテーブルを再構築する必要があり、大量のメモリを消費し、鍵変更のために多大な演算コストを必要とする。筆者らは、これまでに各拡大鍵に応じたテーブルを必要としないテーブルネットワーク化手法を提案した。この論文では、これを鍵スケジュール部にも拡張し、未対策時に比べ暗号処理の演算時間の増加を抑えた対策法を提案した。また、提案法にCPA (Correlation Power Analysis) を適用した結果についても示した。

(13) 自己完結型テンプレート攻撃

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

SCIS 2009　1A1-2（2009 年 1 月 20 日）

この論文では、CMOS 回路に対してサイドチャネル攻撃を実行する際に、テンプレート攻撃のような強い仮定がなくとも、攻撃精度のよい選択関数を判別できる新しい攻撃手法“自己完結型テンプレート攻撃”を提案した。自己完結型テンプレート攻撃では、攻撃対象とするデバイスからのサイドチャネル情報のみで、回路の弱点をピンポイントに抽出することができた。これにより、攻撃効率を大幅に改善することができた。この論文では、提案手法によるASIC への攻撃結果も併せて示し、提案手法の有効性を示した。

(14) ブロック暗号の回路アーキテクチャに対するサイドチャネル耐性評価(1)

鈴木 大輔（三菱電機株式会社/横浜国立大学)，佐伯 稔，清水 孝一（三菱電機株式会社）

SCIS 2009　1A1-3（2009 年 1 月 20 日）

この論文では、回路アーキテクチャがサイドチャネル攻撃に与える影響を評価し、アーキテクチャによってとり得る攻撃手法とその効果を詳細に議論した。この結果、回路アーキテクチャに依存してサイドチャネル耐性が大きく異なることを示した。また、評価の過程で得られた攻撃効率の高い解析手法についても述べた。

(15) ブロック暗号の回路アーキテクチャに対するサイドチャネル耐性評価(2)

佐伯 稔（三菱電機株式会社)，鈴木 大輔（三菱電機株式会社/横浜国立大学)，清水 孝一（三菱電機株式会社）

SCIS 2009　1A1-4（2009 年 1 月 20 日）

著者らは、ブロック暗号の回路アーキテクチャに応じて、暗号回路に適用可能なサイドチャネル攻撃の解析手法は変わり、サイドチャネル耐性がその回路アーキテクチャに大きく依存すると考えており、この論文では、SASEBO-R を用いた実機評価により、SCIS2009 1A1-3 で示した著者らの検討結果について検証した。

(16) RSL 技術を用いた耐 DPA 暗号 LSI の設計手法 －プロトタイプ LSI に対する DPA 評価結果－

佐伯 稔（三菱電機株式会社)，鈴木 大輔（三菱電機株式会社/横浜国立大学）

SCIS 2009　1A1-5（2009 年 1 月 20 日）

この論文では、著者らが提案した“RSL技術を用いた耐DPA暗号LSIの設計手法"に基き開発した擬似RSL-AES回路に対するDPA評価について報告した。100万波形を用いた評価の結果、当該回路の高いDPA 耐性が確認され、提案手法が実際のLSI開発において有効であることが示された。

(17) サイドチャネル攻撃評価用 ISO/IEC 標準暗号プロセッサの開発

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

SCIS 2009　2A1-1（2009 年 1 月 21 日）

サイドチャネル攻撃実験用暗号プロセッサを開発した。プロセッサは、ISO/IEC18033全ての標準ブロック暗号とRSA暗号をそれぞれ専用回路として有し、選択的に実行可能である。AESについてはS-boxの回路方式が異なる7種類が含まれる。このプロセッサをTSMC 0.13μm CMOSの標準セルライブラリを用いて実装するとともに、このASICを搭載したサイドチャネル攻撃標準評価ボード(SASEBO-R)を開発した。この論文では、そのAESに対する差分電力解析およびRSAに対する単純電力解析への耐性評価結果を示した。

(18) べき乗剰余演算に対する比較電力解析の応用

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）
SCIS 2009　2A1-2（2009 年 1 月 21 日）

この論文では、べき乗剰余演算に対する比較電力解析の応用について述べた。比較電力解析では、特殊な入力ペアから得られた2つの消費電力波形の比較により、べき乗剰余演算中に発生する自乗算を同定し、鍵を推定する。従来のバイナリ法やwindow法だけでなく、ダミー演算や乱数マスクによる対策を施した多くのアルゴリズムに対しても適用可能である。それら対策手法に対する比較電力解析の適用を示すとともに、解析対象のモジュールの他に参照用モジュールが存在した場合、より強力な比較電力解析が実現できることを明らかにした。

(19) 電磁波を利用した故障利用攻撃の実験手法に関する一考察

田中 秀磨（情報通信研究機構）
SCIS 2009　2A3-1（2009 年 1 月 21 日）

暗号モジュールを意図的に誤動作させその入出力情報から秘密情報を導きだす故障利用攻撃は、アルゴリズムを解析する攻撃手法に比べ攻撃者が有利な状況を仮定している。誤動作を発生させる条件は、攻撃アルゴリズムの発展により徐々に緩くなっているが、実際の暗号モジュールがどのように誤動作を発生できるかについては明らかになっていない。この論文では電磁波を用いた故障利用攻撃を仮定し、暗号モジュールとしてSASEBOを対象とした場合、どのような誤動作を発生させることができるかについて紹介した。

(20) 高周波クロックによる RSL 技術を用いた AES へのフォールト攻撃実験

八木 達哉，崎山 一男，太田 和夫（電気通信大学）
SCIS 2009　2A3-2（2009 年 1 月 21 日）

DPA対策法としてRandom Switching Logic (RSL)が2004年に鈴木らによって提案された。その後、鈴木らは改良を重ね、RSLを用いたAESを評価用LSIに実装した。この論文では、その評価用LSIに対してフォールト攻撃を用いた安全性評価を行った。評価用LSIが搭載されているSASEBO-Rを用いた実験により、高周波クロック供給時に出力されるフォールト入り暗号文と1組の正常な平文・暗号文を用いることで、秘密鍵の導出が可能であることを示した。

(21) フォールト混入時における RSL 技術による暗号回路モデルを用いた安全性解析

泉 雅巳，太田 和夫，崎山 一男（電気通信大学）
SCIS 2009　2A3-3（2009 年 1 月 21 日）

サイドチャネル攻撃の1つであるDPA攻撃に対するロジックレベルの対抗方式として、RSL技術が提案されている。この論文では、フォールト混入時におけるRSL技術による暗号回路モデルを用いて安全性解析を行った。この暗号回路モデルのデータフローから暗号回路の出力は簡略化されたものとなった。また、RSLを用いた暗号回路のモデルをAESに

適用し、フォールトを第10ラウンド目および第9ラウンド目に混入した場合を考えた。このときRSL-AESのアーキテクチャのデータフローから得られる出力を解析し、秘密鍵を特定した。

(22) 電力解析と電荷の充放電に関する考察

品川 宗介，市川 哲也（三菱電機エンジニアリング株式会社），佐藤 恒夫（三菱電機株式会社）

SCIS 2009　3A1-1（2009 年 1 月 22 日）

専用暗号 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）を用いて ASIC に実装された AES 暗号演算時の消費電力を 4 種類の測定位置から測定した。測定した結果に対して、AES 最終段の部分鍵を CPA にて推測し、消費電力の標準偏差と漏洩情報について考察した。その結果，CPA 結果と消費電力の標準偏差との関係をハードウェアの充放電現象で説明できることを示すとともに，CPA 対策方針について考察を行った。

(23) SASEBO における FPGA に対する電力解析／電磁波解析実験

庄司 陽彦（株式会社ワイ・デー・ケー／情報セキュリティ大学院大学），野澤 晃，木村 隆幸（株式会社ワイ・デー・ケー），洲崎 智保，山下 哲孝，角尾 幸保（日本電気株式会社）

SCIS 2009　3A1-2（2009 年 1 月 22 日）

INSTAC-32準拠ボード上で動作する暗号処理に対して電力解析と電磁波解析の実験を行った際は、電力においてはビット単位で着目した場合に得られるサイドチャネル情報が、ほぼ均等となるのに対して、電磁波においてビット単位で着目した場合に得られるサイドチャネル情報に偏りが存在するという結果が得られた。この結果からサイドチャネル攻撃用標準評価ボードSASEBO上のFPGAで動作する暗号処理に対して、ビット単位のサイドチャネル情報の偏りがどのように現れるかを確認した。その結果、電力解析と電磁波解析において偏りの違いは殆ど見られなかったが、双方の解析において特定のビットにおいて偏りが見られた。その考察を行うため、レイアウトの違いによる影響と、サイドチャネル情報に対するハミング距離の関係についての実験を行った。

(24) 信号処理を利用した SASEBO における差分電力解析

山下 哲孝，洲崎 智保（日本電気株式会社），庄司 陽彦，野澤 晃，木村 隆幸（株式会社ワイ・デー・ケー），角尾 幸保（日本電気株式会社）

SCIS 2009　3A1-3（2009 年 1 月 22 日）

この論文では、サイドチャネル攻撃標準評価ボードSASEBOに搭載した128bitAESに対し、信号処理を利用した差分電力解析手法であるFrequency-based DPAとバンドパスフィルタを用いたDPAによる解析を行った。それにより、従来のDPAでは解析が困難である場合でも、信号処理を利用した方法を用いることで解析が可能となることを実験的に確認した。

(25) 波形選別による差分電力解析の改善について

野澤 晃，庄司 陽彦，木村 隆幸（株式会社ワイ・デー・ケー），洲崎 智保，山下 哲孝，角尾 幸保（日本電気株式会社）

SCIS 2009　3A1-4（2009 年 1 月 22 日）

この論文では、偏差などを使用して解析に悪影響を及ぼす波形を除外することで、差分電力解析における解析成功率を改善させる手法を提案した。差分電力解析を行うため、攻撃対象となるデバイスより漏洩情報を測定する際、外部からのノイズの影響によって攻撃者の意図しない波形を取得する場合がある。統計処理によって解析に不要となる情報を削除し、秘匿情報を導出する差分電力解析では、処理に用いる消費電力の中に秘匿情報をマスクするような波形が含まれると、解析における成功率が減少する。解析に悪影響を及ぼす波形が含まれている場合、提案手法を用いてそれを除外することで解析成功率を改善できることを示した。

(26) 最近傍から計測した磁界を用いた差分電磁波解析

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

SCIS 2009　3A1-5（2009 年 1 月 22 日）

この論文では、暗号LSIのパッケージを開封して行った差分電磁波解析（DEMA）について述べた。この手法では、開封したLSIの表面から100 μmほどの高さに配置した磁界プローブにより局所的な磁界を計測した。この手法は従来手法と比べて計測の難易度が上がる一方、(i)少ない波形数で鍵推定に成功し、(ii)LSI内の暗号コアの配置に依存する磁界の局所性が利用できることを示した。また、計測した磁界波形では、信号の立上りと立下りを区別するスイッチングディスタンスモデルが成り立つことを示すことで、レジスタや組み合わせ回路を乱数でプリチャージする対策が無効化できること明らかにした。

(27) サイドチャネル解析研究に役立つ波形データ交換用標準フォーマット WXF の提案

松本 勉（横浜国立大学），高橋 芳夫(横浜国立大学/株式会社 NTT データ）

SCIS 2009　3A4-1（2009 年 1 月 22 日）

暗号モジュールのサイドチャネル解析実験データの交換に広く適用できる波形データ交換用標準フォーマット Waveform data eXchange Format (WXF_v1.0)を作成した。これによりデータの配布や公開とその活用に関する技術的コストが軽減し、サイドチャネルセキュリティの研究開発や暗号モジュールの試験・認証などの環境整備の促進に役立つことが期待される。測定ツールは WXF_v1.0 に従ってデータを整形して出力すれば、少なくとも DPA 型の実験に必要な情報を提供でき、その他のオプションの情報を添付してもそれが分析ツールを阻害しないようにできる。分析ツールは、DPA 型の実験に必要な情報を取り込むことができ、必要に応じてその他の情報を参照することができる。

(28) CPA に対するデカップリングキャパシタの影響の予備検証

片下 敏宏，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）
SCIS 2009　3A4-2（2009 年 1 月 22 日）

筆者らが開発したサイドチャネル攻撃の評価のための標準ボードSASEBO（Side-channel Attack Standard Evaluation BOard）は、微細な電力波形の測定を可能とするためデカップリングキャパシタを搭載していないが、実際の暗号モジュールではキャパシタの有無が攻撃の成否に大きく影響する。この論文では、ISO/IEC 標準ブロック暗号モジュールを実装したLSI を搭載するSASEBO-Rにおいて、キャパシタの有無によるAES、Camellia、SEED、MISTY-1、CAST-128、DESの動作電力波形の違いを調べるとともに、AES に対してCPA(Correlation Power Analisys)を実施した。その結果、キャパシタを搭載しない場合は4000波形で全ての鍵が導出可能であったが、搭載した場合は10万波形でもまったく攻撃できないことがわかり、電力解析攻撃への対策として非常に効果の高いことが確認された。

2.4.8　今後の検討項目

暗号モジュールへの最適な電力解析の実験方法の検討

今年度の実験用標準評価ボードの比較実験結果から、暗号モジュールの動作クロック周波数を低く設定することと、波形のサンプリング間隔を短くすることで、攻撃の成功確率が向上することが確認されている。これらを基に評価のための測定環境や測定ポイント等の条件について検討し、実験結果の改善を行い、電力解析攻撃が成功するための測定コストと測定時間条件を意識して、最適な試験方法を検討することが今後の課題である。

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」に対する評価環境（インタフェース情報）の検討
(2) 「性能の評価」における評価内容、評価基準の検討
(3) 「サイドチャネル攻撃に対する対策実現の確認」におけるプラットフォームの検討
(4) 「サイドチャネル攻撃に対する対策実現の確認」における確認環境の検討
(5) 「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

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　電力解析実験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電力解析の実験方法の検討

第 3 章　開催状況

3.1　暗号モジュール委員会の開催状況

2008 年度の暗号モジュール委員会は、計 4 回開催された。各回会合の概要は表 3.1 のとおりである。

表 3.1　2008 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 20 年 8 月 1 日 10:00～11:30	暗号モジュール委員会活動計画 電力解析実験ワーキンググループ活動計画 電子政府推奨暗号リスト改訂と関連した活動について
第 2 回	平成 20 年 10 月 31 日 14:00～16:00	電子政府推奨暗号リスト改訂と関連した活動について 電力解析実験ワーキンググループ中間報告 規格・標準化動向等についての報告
第 3 回	平成 20 年 12 月 15 日 10:00～12:00	電子政府推奨暗号リスト改訂と関連した活動について CRYPTREC シンポジウム 2009「リスト改訂に向けて」の告知
第 4 回	平成 21 年 2 月 20 日 18:00～20:00	2008 年度電力解析実験ワーキンググループの活動報告 2008 年度暗号モジュール委員会の活動報告（案）について

3.2　電力解析実験ワーキンググループの開催状況

2008 年度の電力解析実験ワーキンググループは、計 4 回開催された。各回会合の概要は表 3.2 のとおりである。

表 3.2　2008 年度電力解析実験ワーキンググループの開催状況

回	開催日時	主な議題
第 1 回	平成 20 年 9 月 3 日 14:00～16:00	電力解析実験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 20 年 10 月 3 日 15:00～17:00	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 20 年 11 月 26 日 15:00～17:00	実験データの標準評価方法について 実験環境等についての検討
第 4 回	平成 21 年 2 月 4 日 14:30～16:30	2008 年度電力解析実験ワーキンググループの活動のまとめ 暗号モジュール委員会への報告書の作成 2009 年度の活動計画(案)について

発行日　2009 年 4 月 25 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