CRYPTREC Report 2003

平成 16 年 3 月

通信・放送機構
独立行政法人情報処理推進機構

「暗号技術監視委員会報告」

目次

はじめに

CRYPTREC には「暗号技術監視委員会」と「暗号モジュール委員会」がある。両委員会とも暗号技術検討会の下で活動をしており、前者は電子政府推奨暗号の安全性の監視等を行い、後者は電子政府推奨暗号を実装する暗号モジュールの評価基準・試験基準の作成等を行っている。本書は、**“暗号技術監視委員会の 2003 年度の活動報告書”**である。

暗号技術監視委員会の前身とも言える暗号技術評価委員会では2000年度から2002年度の３カ年をかけて我が国の電子政府(e-Government)で利用可能な暗号技術のリストアップを目的とした暗号技術評価活動(暗号アルゴリズムの安全性評価)を推進してきた。

その結果、2002 年度末に、暗号技術検討会を主催する総務省、経済産業省が電子政府推奨暗号リストを公表する運びとなり、暗号技術評価活動も一区切りを迎えた。

暗号技術には、新しい解読方法の考案や計算機能力の向上等によりその安全性が損なわれるということもあり得る。従って、これら動向の監視が必要である。その監視活動を担うために暗号技術監視委員会が設置された。さらに暗号技術関連の学会、国際会議、あるいは関係団体のＷｅｂサイト等を監視し、電子政府推奨暗号の安全性に影響を与えかねない情報の収集、分析、等を実施する監視要員が事務局内に配置された。

暗号技術監視委員会は、通信・放送機構及び独立行政法人情報処理推進機構が共同で運営しており、技術面を中心とした活動を担当している。一方、ユーザの立場でかつ政策的な判断を加えて結論を出しているのが総務省、経済産業省主催の暗号技術検討会であり、相互に協調して電子政府の安全性及び信頼性を確保する活動を推進しているものである。

今年度は“監視活動元年”であり、先ずは暗号技術監視委員会、暗号技術調査ワーキンググループの設置、監視要員の配置等、監視体制の樹立に始まり、監視活動方針・手順の確立とそれに従った監視活動及び関連調査活動等が開始された。

電子政府推奨暗号の監視活動は今年度限りのものではない。暗号が使われ続ける限り継続していかなければならない活動である。また、暗号モジュール委員会との連携を保ちつつ、暗号技術の研究者、実装技術者等の多くの関係者の協力を得て成り立っているものである。

末筆ではあるが、本活動に様々な形でご協力下さった関係者の皆様に謝意を表する次第である。

暗号技術監視委員会　委員長　今井 秀樹

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。たとえば、電子政府において電子署名や GPKI システム等暗号関連の電子政府関連システムに関係する業務についている方などを想定している。しかしながら、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書の第１章は暗号技術監視委員会及び監視活動等について説明してある。第２章は今年度の監視活動、調査等の報告である。また、監視要員が中心になって実施した調査等の報告が第３章にある。

本報告書の内容は、我が国最高水準の暗号専門家で構成される「暗号技術監視委員会」及びそのもとに設置された「暗号技術調査ワーキンググループ」において審議された結果であるが、暗号技術の特性から、その内容とりわけ安全性に関する事項は将来にわたって保障されたものではなく、今後とも継続して評価・監視活動を実施していくことが必要なものである。

暗号技術監視委員会の事務局を務める通信・放送機構及び独立行政法人情報処理推進機構の Web サイトで、本報告書も含めた CRYPTREC 活動に関する情報を参照することができる。

http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html

http://www.ipa.go.jp/security/enc/CRYPTREC/index.html

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡いただけると幸いである。

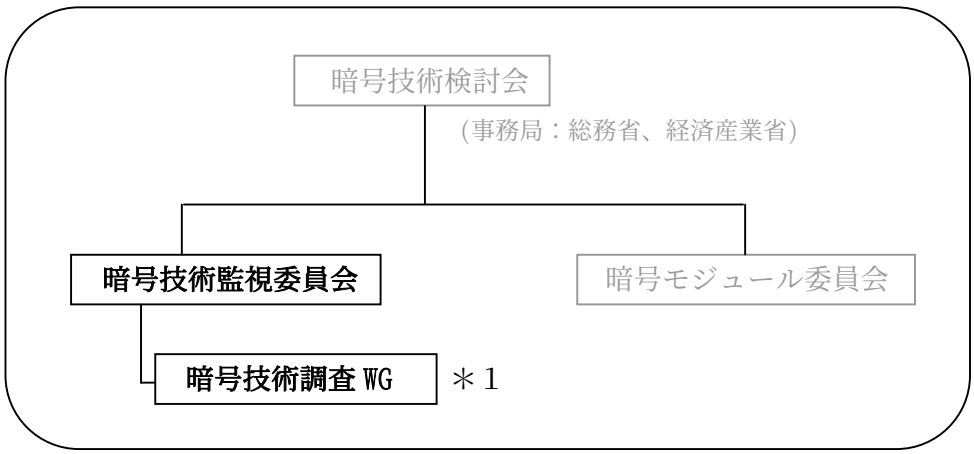
【問合せ先】　cryptrec@shiba.tao.go.jp　または　cryptrec@ipa.go.jp

委員会構成

暗号技術監視委員会(以下「監視委員会」)は、総務省と経済産業が共同で主催する暗号技術検討会の下に設置され、通信・放送機構(TAO)と独立行政法人情報処理推進機構(IPA)が共同で運営する。監視委員会は、暗号技術の安全性及び信頼性確保の観点から、電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討を適宜行う等、主として技術的活動を担い、暗号技術検討会に助言を行う。また、将来的には、電子政府推奨暗号リストの改訂に関する調査・検討を行う予定である。なお、日常的な監視業務を行う監視要員を TAO/通信総合研究所(CRL)(両機関は 2004 年 4 月 1 日統合予定)及び IPA に配置し、暗号技術関連学会や国際会議等を通じての暗号技術に関する情報収集、関係団体の Web サイトの監視等を行う。

暗号技術調査ワーキンググループ(以下「調査 WG」)は、監視委員会の下に設置され、TAO と IPA が共同で運営する。調査 WG は、監視委員会活動に関連して必要な項目について、監視委員会の指示のもとに調査・検討活動を担当する作業グループである。監視委員会の委員長は、実施する調査・検討項目に適する主査及びメンバーを、監視委員会及び調査 WG の委員の中から選出し、調査・検討活動を指示する。主査は、その調査・検討結果を監視委員会に報告する。現在、監視委員会の指示に基づき実施されている調査項目は、「擬似乱数生成系調査」、「暗号利用モード調査」の２つである。

監視委員会と連携して活動する「暗号モジュール委員会」も、監視委員会と同様、暗号技術検討会の下に設置され、TAO と IPA が共同で運営している。



＊1　今年度実施されている調査項目

1)暗号利用モードの調査　主査：古原和邦、委員：川村信一、古屋聡一

2)擬似乱数生成系調査　　主査：金子敏信、委員：荒木純道、森井昌克、栃窪孝也

図１　2003 年度の CRYPTREC の体制図

委員名簿

暗号技術監視委員会

委員長	今井 秀樹	東京大学 教授
顧問	辻井 重男	中央大学 教授
委員	太田 和夫	電気通信大学 教授
委員	金子 敏信	東京理科大学 教授
委員	佐々木 良一	東京電機大学 教授
委員	松本 勉	横浜国立大学 大学院 教授
委員	大塚 玲	独立行政法人情報処理推進機構 主任研究員
委員	田中 秀磨	独立行政法人通信総合研究所 研究員
委員	山村 明弘	独立行政法人通信総合研究所 グループリーダ
委員	渡辺 創	独立行政法人産業技術総合研究所 研究員

暗号技術調査ワーキンググループ

委員	荒木 純道	東京工業大学 大学院 教授
委員	有田 正剛	日本電気株式会社 主任
委員	小暮 淳	株式会社富士通研究所 主任研究員
委員	酒井 康行	三菱電機株式会社 主任研究員
委員	四方 順司	横浜国立大学 大学院 講師
委員	新保 淳	株式会社東芝 主任研究員
委員	洲崎 誠一	株式会社日立製作所 主任研究員
委員	藤岡 淳	日本電信電話株式会社 主幹研究員
委員	松崎 なつめ	松下電器産業株式会社 主席技師
委員	青木 和麻呂	日本電信電話株式会社 研究主任
委員	川村 信一	株式会社東芝 主任研究員
委員	香田 徹	九州大学 大学院 教授
委員	古原 和邦	東京大学 助手
委員	下山 武司	株式会社富士通研究所 研究員
委員	館林 誠	松下電器産業株式会社 参事
委員	角尾 幸保	日本電気株式会社 主任研究員
委員	時田 俊雄	三菱電機株式会社　主席研究員
委員	古屋 聡一	株式会社日立製作所 研究員
委員	森井 昌克	徳島大学 教授
委員	栃窪 孝也	東芝ソリューション株式会社 SI 技術担当

オブザーバー

奥　　隆行　　警察庁 情報通信局
富田 哲　　防衛庁 長官官房
一條 靖彦　　防衛庁 陸上幕僚監部
山本 寛繁　　総務省 行政管理局
竹之内 修　　総務省 行政管理局
藤本 昌彦　　総務省 情報通信政策局(2003 年 7 月まで)
佐藤 憲一郎 総務省 情報通信政策局(2003 年 7 月まで)
福岡 晃　　総務省 情報通信政策局(2003 年 7 月まで)
野崎 雅稔　　総務省 情報通信政策局
榎本 淳一　　総務省 情報通信政策局
黒田 崇　　総務省 情報通信政策局
石川 雅一　　外務省 大臣官房
小谷 光弘　　経済産業省 産業技術環境局
北浦 康弘　　経済産業省 商務情報政策局
滝澤 修　　独立行政法人通信総合研究所
大蒔 和仁　　独立行政法人産業技術総合研究所

事務局

通信・放送機構

喜安拓(2003 年 7 月まで)、大久保明、横山隆裕(2003 年 7 月まで)、鳥居秀行、
天野滋、高橋靖典、半澤則之

・ 監視要員

山村明弘、田中秀磨、藤田真史

独立行政法人情報処理推進機構

内藤理(2003 年 5 月まで)、早貸淳子、河内浩明、網島和博、小柳津育郎、
田中公明、矢田健一(2003 年 8 月まで)、山岸篤弘

・ 監視要員

大塚玲、黒川貴司、杉田誠

第１章　活動の目的

1.1. 電子政府システムの安全性確保

電子政府システムが2003年度に本格的に始動した。電子政府システムの安全性の確保は緊急に対処しなければならない。内閣府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)(http://www.kantei.go.jp/jp/singi/it2/index.html)はe-Japan戦略II(2003年7月)を発行し、「新しいIT社会基盤整備」において「安心・安全な利用環境の整備」を唱え、電子政府や電子自治体、重要インフラ等の公共的分野のサービスの情報セキュリティ対策の一層の充実が求めている。これらの電子政府、電子自治体における情報セキュリティ対策は根幹において暗号アルゴリズムの安全性に依存している。情報セキュリティ確保のためにはネットワークセキュリティ、通信プロトコルの安全性、機械装置の物理的な安全性、セキュリティポリシー構築、個人認証システムの脆弱性、運用管理方法の不備を利用するソーシャルエンジニアリングへの対応と幅広く対処する必要があるが、暗号技術は情報セキュリティシステムにおける基盤技術であり、暗号アルゴリズムの安全性を確立することなしに情報セキュリティ対策は成り立たない。さらに、2005年までに世界最先端のＩＴ国家になるとの目標を達成するためのe-Japan戦略II加速化パッケージ(2004年2月)においてもセキュリティ(安全･安心)政策の強化が政府として取り組むべき重点施策とされていて、各府省庁の情報セキュリティ確保において「攻撃の予兆や被害に関する情報収集・分析」が重要案件としてあげられている。暗号技術の危殆化を予見し、電子政府システムで利用される暗号技術の安全性を確保するためには最新の暗号理論の研究動向を専門家が十分に情報収集・分析することが不可欠である。

1.2 暗号技術監視委員会

電子政府システムにおいて利用される暗号アルゴリズムを評価・選択する活動が2000年度から2002年度まで暗号技術評価委員会(CRYPTREC: Cryptography Research and Evaluation Committees)において実施された。その結論を考慮して電子政府推奨暗号リスト(付録参照)が総務省・経済産業省において決定された。電子政府システムの安全性を確保するためには電子政府推奨暗号リストに掲載されている暗号技術の安全性を常に把握し、安全性を脅かす事態を予見することが重要課題となった。そのため2003年度に電子政府推奨暗号の安全性に関する継続的な評価、電子政府推奨暗号リストの改訂に関する調査・検討を行うことが重要であるとの認識の下に、暗号技術評価委員会が発展的に改組され、暗号技術検討会の下に「暗号技術監視委員会」が設置された。暗号技術監視委員会の責務は電子政府暗号の安全性を常時把握し、もし電子政府暗号技術に問題点が発覚した場合には早急な対応を行うことである。さらに暗号技術監視委員会は電子政府暗号の監視活動のほかにも暗号理論の研究動向を把握し、将来の電子政府暗号リストの改訂に技術面から支援を

行うことを委ねられている。

1.3 電子政府暗号リスト

2000 年から 2002 年の CRYPTREC プロジェクトの集大成として暗号技術評価委員会で作成された「電子政府推奨暗号リスト素案」は 2002 年に暗号技術検討会に提出され、暗号技術検討会での審議ならびに(総務省・経済産業省による)パブリックコメント募集を経て「電子政府推奨暗号リスト」(付録参照)として決定された。そして、「各府省の情報システム調達における暗号の利用方針(平成 15 年 2 月 28 日、行政情報システム関係課長連絡会議了承)」により、各府省における暗号技術の利用方針として合意された。電子政府暗号リストの技術的な裏付けについては、暗号技術評価報告書(2002 年度版)に詳しく記載されている。暗号技術評価報告書(2002 年度版)は(http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/index.html)から入手できる。

1.4 活動の指針

電子政府推奨暗号リスト掲載の暗号技術に関する研究動向を把握して、暗号技術の安全性について監視を行い、必要に応じて電子政府システムにおける暗号技術の情報収集とリストの改訂について暗号技術検討会(総務省・経済産業省)に対して助言を行う。また、暗号理論全体の技術動向を把握して、最新技術との比較を行い、電子政府システムにおける暗号技術の陳腐化を避けるため、将来のリストの改正を考慮して、電子政府推奨暗号リストに関する調査・検討を行う。監視活動は、情報収集、情報分析、審議及び決定の 3 つのフェーズからなる。

暗号技術検討会における電子政府推奨暗号の監視に関する基本的考え方は以下の通りである。

(1) 実運用環境において安全性に問題が認められた電子政府推奨暗号は原則としてリストから削除する。
(2) 電子政府推奨暗号の仕様変更は認めない。
(3) 電子政府推奨暗号の仕様変更に到らないパラメータの修正等の簡易な修正を行うことにより当該暗号の安全性が維持される場合には、修正情報を周知して当該暗号をリストに残す。

以上の指針に基づき、監視委員会ではTAO/独立行政法人通信総合研究所(CRL)(両機関は2004年4月に独立行政法人情報通信研究機構として統合予定)及びIPAに監視要員を配置した。監視要員は研究集会、国際会議、研究論文誌、インターネット上の情報等を監視し、電子政府推奨暗号の安全性に関して情報を分析し、それを監視委員会に報告する。監視委

員会のもと暗号技術調査ワーキンググループを構成し、推奨暗号の安全性に問題点の疑いがある場合には早急に検討できる体制を作った。また電子政府暗号の応募者からの自発的な情報提供を呼びかけています。監視要員は情報を参考にして情報分析を行い、電子政府推奨暗号の削除等を検討すべき事態が発生しているか否か判断する。

第２章 監視活動

2.1　監視活動状況

2.1.1　監視状況 ·

監視活動には監視委員会のもと、暗号技術調査ワーキンググループの活動、監視要員の調査活動等がある。ワーキンググループにおいては疑似乱数生成系の検定法と暗号利用モードについて調査している。また、1024ビットのRSA型合成数の素因数分解問題について計算機実験と専用ハードウェア構築の実現性の両面からの調査、及びSSL/TLSで実装されているRSA暗号の問題点を調査した。また代数的攻撃について注目し監視を行った。

監視要員は研究論文誌、インターネット上の情報や研究集会における情報を収集し、国際学会等に参加し、電子政府暗号に関する安全性を脅かす研究動向があるかどうか監視をおこなった。その結果 2003 年度においては、監視活動における３つのフェーズである「情報収集」、「情報分析」、「審議及び決定」における「審議及び決定」に至る案件はなかった。監視要員を主体に情報収集を行い、その情報を分析し、電子政府推奨暗号の安全性に懸念を持たせるような事態はなかった。

2.1.2 監視報告

検討課題と考えられたものは以下の通りである。

・いくつかの擬似乱数生成系の検定法
・暗号利用モード
・素因数分解問題の現状(TWIRL の実現性と計算機実験)
・ SSL/TLS で実装される暗号の問題点
・ 代数的攻撃

それぞれの検討課題の調査結果については該当する節を参照してほしい。また、近年研究が盛んになってきているサイドチャネル攻撃については、アルゴリズムの実装環境の安全性に大きく依存するため、暗号モジュール委員会にて文献調査が行なわれている。サイドチャネル攻撃への耐性と暗号技術の安全性について、暗号モジュール委員会から審議結果の報告が待たれるところである。

2.1.3 国際学会等参加記録

2003 年度は表 2.1 に示すような国際会議に監視要員を派遣し、最新の暗号解読技術に関する情報収集を実施した。以下では、これらの国際会議で発表された論文を中心に、暗号解読技術の最新動向について述べる。

表 2.1　国際会議への参加状況

学会名・会議名		開催国・都市	期間
EUROCRYPT 2003	Eurocrypt	Warsaw, Poland	2003/5/5 ～ 2003/5/8
SAC 2003	Selected Areas in Cryptography	Ottawa, Ontario, Canada	2003/8/13 ～ 2003/8/15
CRYPTO 2003	Crypto Conference	Santa Barbara, Ca., USA	2003/8/18 ～ 2003/8/21
CHES 2003	Workshop on Cryptographic Hardware and Embedded Systems	Cologne, Germany	2003/9/8 ～ 2003/9/10
ISO SC27	International Organization for Standardization	Saint Denis, France	2003/10/20 ～ 2003/10/24
ASIACRYPT 2003	Asiacrypt	Taipei, Taiwan	2003/12/1 ～ 2003/12/4
EIDMA-CWI WS	EIDMA-Cryptography Working Group	Utrecht, Netherlands	2003/12/12 ～ 2003/12/12
SCIS 2004	Symposium on Cryptography and Information Security	宮城県仙台市	2004/1/27 ～ 2004/1/30
FSE 2004	Fast Software Encryption	Delhi, India	2004/2/5 ～ 2004/2/7
TCC 2004	Theory of Cryptography Conference	Cambridge, MA, USA	2004/2/19 ～ 2004/2/21
CT-RSA 2004	RSA Conference 2004, Cryptographers' Track	San Francisco, Ca., USA	2004/2/23 ～ 2004/2/27
PKC 2004	International Workshop on Practice and Theory in Public Key Cryptography	Singapore	2004/3/1 ～ 2004/3/4

表 2.2 は最重要の成果が報告される IACR(International Association for Cryptographic Research: 国際暗号学会)主催の5つの国際会議に報告された暗号解読技術に関する論文件数を、暗号技術の分類に従って集計したものである。

公開鍵暗号に関する暗号解読技術については、素因数分解等の暗号学的仮定(安全性の根拠となる仮定)に対する基礎的な研究が 14 件中 10 件と多く報告されている。これは最近の証明可能安全性理論の発展により、主要な公開鍵暗号技術が暗号学的仮定に帰着する証明を備えていることから、暗号解読技術も個別のアルゴリズムに対する解読法の提案は減少し、暗号学的仮定そのものを対象にする傾向が強まっているためと考えられる。暗号学的仮定を対象とする基礎的な研究では、2003 年度は後述の TWIRL に代表される素因数分解の

ための特殊なハードウェアの構成法に関する報告や、楕円曲線暗号の定義体の違いによる強度解析が多く見られる。表 2.2 のその他の項目は、Braid 群や Lattice など、電子政府推奨暗号のアルゴリズムが依拠していない暗号学的仮定に対するものである。

共通鍵暗号に関する暗号解読技術の傾向としては、公開鍵暗号とは対照的に、個別アルゴリズムに対する攻撃法が報告されることが多い。特にストリーム暗号に関する解読技術が 19 件中 15 件と多数を占め、その中でも代数的攻撃法の研究が数多く報告されている。共通鍵暗号に特化している FSE 2004 では、代数的攻撃法に関するセッションも設けられる状況となっている。

表 2.2　暗号解読技術の分野別発表件数

	Eurocrypt	CRYPTO	Asiacrypt	FSE	PKC	計
公開鍵暗号	**4**	**4**	**3**	**0**	**3**	**14**
暗号学的仮定						
楕円曲線	1		1			2
素因数分解		2	2		2	6
その他		1			1	2
守秘	1	1				2
署名	2					2
鍵交換						0
共通鍵暗号	**3**	**3**	**1**	**12**	**0**	**19**
ブロック暗号	1		1	2		4
ストリーム暗号	2	3		10		15
その他	**1**	**1**	**1**	**0**	**0**	**3**
ハッシュ関数			1			1
擬似乱数生成系	1	1				2

(１)公開鍵暗号

(イ)暗号学的仮定に関連する報告

・素因数分解ハードウェアの構成法

素因数分解に用いられる数体篩(ふるい)法の一部で特に大きな処理コストが必要となる篩(ふるい)部分と線形代数部分に専用ハードウェアを用いる方法が盛んに研究されている。Shamir-Tromer らは篩(ふるい)部分について、Geiselman-Steinwandt らは篩(ふるい)部分および線形代数部分のそれぞれについて、特殊なハードウェアの構成法を示し、従来の見積もりよりも低いコストで RSA 合成数の素因数分解が可能であると報告した。

Shamir-Tromer らの提案は、WSI(Wafer-Scale Integration)を前提とした革新的なハードウェア構成(TWIRL)を採用することにより 1024bit の素因数分解を目指しているのに対し、Geiselman-Steinwandt らの提案は、既存の LSI 技術を多

用した回路を 4.9cm 角のシリコンチップに実装することで、768bit の素因数分解について TWIRL よりコストパフォーマンスが 1/6 程度に低下するものの実現性が高いと主張している。これらの新しい技術に関連して、3.1 において TWIRL に関する評価結果を記述している。

・楕円曲線暗号

Hess は、GHS (Gaudry-Hess-Smart) 攻撃を一般化し、標数 2 の拡大体 $\mathbf{F}_{2^n}$ を定義体とする従来より多くの楕円曲線に適用可能とした。また、Menezes-Teske-Weng らも同じく標数 2 の拡大体 $\mathbf{F}_{2^n}$ について、Pollard のρ法や GHS 攻撃法などが効率良く適用できるパラメータを考察し、いくつかの場合に攻撃に必要な計算量を 1/1000 以下に削減できると主張している。さらに、Theriault は種数が小さな超楕円曲線に対する Index Calculus の改良について考察し、例えば種数 3 の超楕円曲線ではメモリサイズで 5%程度大きな定義体を採用すべきだと主張している。いずれの攻撃法も特に電子政府推奨暗号リストの見直しを必要とする事態には至っていないが、楕円曲線暗号のパラメータを選択する際には、これらの攻撃法に対しても留意する必要があろう。

(ロ)守秘目的の公開鍵暗号アルゴリズムに関連する報告

Braid 群に基づく公開鍵暗号系及び Hidden Field Equation(HFE)に基づく公開鍵暗号系に関する解読法が報告されているが、電子政府推奨暗号リストに直接影響を与えるものではない。

Braid 群に基づく公開鍵暗号に対するものでは、Lee-Park ら及び Cheon-Jun らが解読法を提案している。特に、Cheon-Jun らの提案は多くの暗号アルゴリズムが困難性を仮定していた Braid Diffie-Hellman 共役問題と呼ばれる問題についての多項式時間アルゴリズムを与えている。

また、Hidden Field Equation(HFE)に基づく暗号システムに関しては、Faugere-Joux らがグレブナー基底の計算アルゴリズムを利用した HFE の解読法を提案している。HFE において、秘匿する多項式の次数 d が固定された場合には，この解読法は変数の数に関する多項式時間で HFE を解読でき、HFE-Challenge(d=96, n=80)が約 2 日で解けることを主張している。

(ハ)署名アルゴリズムに関連する報告

電子政府推奨暗号の一つである DSA の variant である RDSA[1]に関し、Fouque-Poupard らが RDSA に関する既知文書攻撃(known-message attack)による解読法を報告している。この解読法は非常に少ない計算量で、署名鍵を導けることを示す強力なものである。

---

[1] RDSA は Biehl らが 2002 年に論文誌 Designs, Codes and Cryptography で発表した署名アルゴリズムである。その名称は、位数が未知の群における Root problem(n 乗根を求める問題)に基づいており、かつ DSA と式の形が似ていることに由来しているが、離散対数問題に基づく DSA とは別物である。

ただし、この解読法はRDSAに固有の特殊な性質を利用しており、DSAの安全性への影響はない。

(２)共通鍵暗号

(イ)ブロック暗号に関連する報告

ブロック暗号の安全性評価手法に関する報告がBiryukovらよりなされた。ブロック暗号の解析では、線形特性や差分特性など、線形変換やアフィン変換により不変な特性を利用することがあるが、Biryukovらの報告では、任意の２つのpermutation(S-box)が線形(アフィン)等価(相互に変換可能)か否かを判定する効率のよいアルゴリズムを構成できることを示している。

(ロ)ストリーム暗号に関連する報告

ストリーム暗号に関連する暗号解読技術として、代数的攻撃法が数多く報告されている。Courtoisはoverdefined(項の数より方程式の数の方が多いこと)な連立代数方程式を解く方法を工夫し、いくつかの暗号の解読が理論的に可能であると主張している。Armknechtは、CourtoisのCRYPTO 2003の結果の一部(Precomputationに関する部分)に含まれる曖昧さを修正し、厳密に定義してさらに8倍高速化したと主張している。代数的攻撃法に関する報告の多くは理論的な結果であり、シミュレーション等による実験的な結果が示されていないことなどから、代数的攻撃法の有効性については懐疑的な意見も多い。また、現在までに示されている代数的攻撃法はLFSRに基づくストリーム暗号に対してのものであり、電子政府推奨暗号リストに掲載されているストリーム暗号は全てLFSRに基づかない方式のため、これらの安全性に関して直接的な影響はないと考えられる。

2.1.4 委員会開催記録

2.1.4.1 暗号技術監視委員会の開催

表 2.3

回	年月日	議題
第1回	2003年5月19日	委員会運営案の説明、2003年度の活動方針決定等
第2回	2003年11月19日	監視方法の説明、暗号技術調査ワーキンググループ活動報告、国際学会等の報告、暗号モジュール委員会の近況報告等
第3回	2004年2月10日	WG活動報告、調査報告、監視状況、国際学会参加報告、来年度活動計画等

2.1.4.2 暗号技術調査ワーキンググループの開催

表 2.4

回	年月日	議題
第 1 回	2003 年 6 月 23 日	WG 運営方法説明、監視要員配置説明と監視活動協力要請、WG 活動方針の説明等
第 2 回	2003 年 7 月 14 日	調査の中間報告
第 3 回	2004 年 2 月 2 日	調査結果の報告、報告書作成について、来年度活動計画案検討等

2.2　暗号技術調査ワーキンググループ

2.2.1 擬似乱数生成系調査ワーキンググループ

2.2.1.1 調査背景

擬似乱数生成系は相互運用性を確立する必要性がないことから、CRYPTREC のリストにおいては SHA-1 を使った擬似乱数生成器が例示されているのみである。しかしながらシステムの要求内容に対して、これが必ずしも十分なものとはいえず、また、適切でない擬似乱数生成器の利用は安全性を損なう可能性もあることから、少なくとも高い乱数性を持つ擬似乱数生成器が採用されるために検定ツールが必要と考えられる。乱数の検定法には種種様々なものが広く知られている。それらを複数集めて検定ツールとしてまとめられたものもいくつか存在する。代表的なものとしては、NIST FIPS PUB 140-2、NIST Special Publication (SP) 800-22、DIEHARD、”The Art of Computer programming 準数値算法” D.Knuth 著に記載されたものなどが知られている。これらはいくつかの観点から乱数検定の統計的手法がまとめられたものであるが、1)複数の検定ツールで同じ検定手法が用いられている 2)採用されている検定法と採用されていない検定法が検定ツールごとに異なるが理由が不明瞭 3)同じ検定手法でも検定ツール毎に閾値等の設定値が異なる場合がある、など曖昧な点が存在する。CRYPTREC が乱数性の検定を行うにあたっては、これまでは NIST FIPS PUB 140-2 と NIST SP800-22 を準拠にしていた。しかしながら、いくつかの検定法で不具合があることを 2002 年度版暗号技術評価報告書において指摘している上いくつかの学術論文が発表されたことと、暗号モジュールの評価においても乱数検定が必要になるという背景があり、擬似乱数生成系の調査を行う必要が暗号技術監視委員会で認められ、今年度からワーキンググループが組織され調査を行うこととなった。

2.2.1.2 活動内容

1) ワーキンググループの構成と開催状況

暗号技術監視委員会から、今年度は以下の委員と暗号技術監視要員でワーキンググループを構成することが指示された。

主査：金子　敏信　東京理科大学理工学部　教授
委員：荒木　純道　東京工業大学工学部　教授
委員：栃窪　孝也　東芝ソリューション株式会社 SI 技術開発センター
委員：森井　昌克　徳島大学工学部　教授

本調査ワーキンググループの今年度の開催状況は以下の通りである。

全体会合	6 月 23 日	東京ファッションタウン	10:03-11:41
第 1 回	7 月 14 日	メルパルク東京	14:58-16:17
第 2 回	2 月 2 日	メルパルク東京	16:00-17:50

技術的な議論は主にメーリングリストを通じて活発に行った。

2) ワーキンググループの活動目標

乱数の検定法は一般的な乱数を対象としているが、CRYPTREC が対象としているのは暗号利用用途の擬似乱数生成系であり、このような観点から CRYPTREC が推奨する乱数検定法をまとめた乱数検定ツール(以下 CRYPTREC 乱数検定ミニマムセット)を作成することを最終的な目標とする。この CRYPTREC 乱数検定ミニマムセットの導出にあたり各乱数検定法の理論的根拠を確認し、どのような観点からの検定が CRYPTREC の方針に適切かを整理する。また、必要であれば閾値等のパラメータを適切な値に修正する。

3) 今年度の活動内容

NIST SP800-22 の離散フーリエ変換検定と Lempel-Ziv 圧縮検定の問題点については、2002 年度版暗号技術評価報告書において指摘されている上、いくつかの学会等でも研究報告がなされている。今年度はこの 2 種類の検定法の問題点の追求と修正の可能性について検討することに注力した。

4) 調査概要

調査 1)「離散フーリエ変換検定と線形合同法について」

2002 年度版暗号技術評価報告書において指摘されている NIST SP800-22 の離散フーリエ変換検定の問題点について追求する。NIST SP800-22 に記述されている検定法の誤りについて調べ、修正の可能性について検討する。さらに、NIST SP800-22 に例示されている線形合同法を用いた疑似乱数生成器(linear truncated congruential generator) の未知パラメータを求めるアルゴリズムに関する調査を行う。

調査 2)「Lempel-Ziv 圧縮検定について」

2002 年度版暗号技術評価報告書において指摘されている NIST SP800-22 の Lempel-Ziv 圧縮検定の問題点について追求する。NIST SP800-22 に記述されている検定法の誤りについて調べ、修正の可能性について検討する。

これらの調査結果とワーキンググループ内における議論から、本ワーキンググループは報告書を作成した。

2.2.1.3 まとめ

今年度の調査結果について、以下に記す。

1) 離散フーリエ変換検定に関する調査

離散フーリエ変換検定では、複数の標本乱数列を離散フーリエ変換した値を 2 値系列に直し、その系列に関する p-value の一様性及び比率で乱数生成器の合否を判断する。NIST SP800-22 に示される離散フーリエ変換検定では、系列長が 10^5[bit]程度の場合、NIST が用意した 16 種類全ての例示的疑似乱数生成器が p-value の一様性の検定に合格しないという問題があり、フーリエ変換された値を 2 値系列に変換する際の閾値が理論的に誤っているという指摘がある。離散フーリエ変換検定の問題点を検証し、修正を試みた結果を表 2.1 に示す。これらの修正は、いくつかの実験結果から推定し、計算機実験により適切な値であることが確認している。今後は理論的な検証が必要と考えられる。

2)Lempel-Ziv 圧縮検定に関する調査

Lempel-Ziv 圧縮検定は、複数の標本乱数列を Lempel-Ziv 圧縮アルゴリズムで増分分解しその部分列数を、適切な閾値で 2 値系列に変換した後、その系列に関する p-value の一様性及び比率で乱数生成器の合否を判断する。増分分解系列数 $W(n)$(n:乱数系列長)は圧縮可能性を評価し、圧縮が可能な系列の場合、乱数性が悪いと判断する。NIST SP800-22 の定めた $W(n)$の平均値と分散の閾値の決定に不明瞭な点があり調査を行った。NIST は理想的な乱数の部分列に対する平均値及び分散を SHA-1 及び Blum-Blum-Shub 乱数生成器を用いた実験値で定めている。一方、Lempel-Ziv 圧縮検定については、他にも理論的な解析を行った結果があり、その解析から定まる平均値及び分散と NIST が定めた値には食い違いが生じている。評価者が計算機実験を行った結果、NIST の値でも現在知られている理論値でも評価するのに実際的でないことが分かった。さらに、評価者によって、いくつかの適当な乱数生成器を用いた実験結果から定めた値を用いても、p-value の比率検定に関し本質的に違うことはないことが明らかになった。評価者の解析によれば、検定方法の性格から片側分布のみで評価が行われているため、2 値系列に変換するための閾値の自由度が 1 であることが、このような結果の原因となっている。本ワーキンググループにおける議論の結果、Lempel-Ziv 圧縮検定はさらなる理論的解析が望まれる検定法であり、現在のところ CRYPTREC 乱数検定法のミニマムセットに加えるには検討を要すると判断した。

3)線形合同法の解析手法に関する調査

線形合同法の出力を乱数とする疑似乱数生成器は乱数性が良好な反面、暗号学的に安全でないため CRYPTREC では使用を勧めていない。しかしながら仕様が単純であり NIST SP800-22 にも例示されている状況にある。そこで本ワーキンググループでは乱数検定と同時にその乱数が線形合同法によって安易に生成されていないかをチェックする目的で線形合同法の解析手法に関する調査を行った。現在知られている解析手法には、Freize、Hastad、Kannan、Lagarias、Shamir のアルゴリズムと Knuth のアルゴリズムがある。Freize らのアルゴリズムは、出力ビットが 2[bit]より大きければ非常に有効なアルゴリズムであるが、NIST が例示する疑似乱数生成器は出力ビットが線形合同法の出力の最上位 1[bit]なので有効な検定方法にはならない。Knuth のアルゴリズムは、線形合同法の法が 2 のべき乗の時に有効であり、出力されるビット数が 2[bit]以上と仮定されている。NIST が例示する疑似乱数生成器は、これらの解析手法が仮定している条件の範囲外であるため、出力系列からそれが線形合同法による系列であるかどうかの判断を行う解析手法の開発は、現在知られているアルゴリズムの応用では、単純には解決しないことが分かった。

表 2.1 離散フーリエ変換検定の調査概要

	NIST	調査結果
周波数スペクトルの分布	・正規分布 ・95%点の閾値=$\sqrt{3n}$	・ 自由度 2 の χ^2 分布 ・95%点の閾値 =$\sqrt{(-\ln 0.05)n} = \sqrt{2.9957\cdots n}$
閾値で 2 値化した系列の分布	・2 項分布 ・平均＝$nP/2$ ・分散=$nP(1-P)/2$	・ 複数の実験結果から「2 項分布とならない」ことを確認 ・ 平均＝$nP/2$ ・ 分散 $nP(1-P)/4$ と推測

以上の議論を経て、CRYPTREC 乱数検定ミニマムセットの導出においては理論的な裏付けが無いものについては、積極的には採用しない方向に決まった。また理論的裏付けがあったとしても、計算機実験が行える程度の実際的な規模において追試を行い、閾値等の設定値が適切かどうかの確認が必要であろうとの判断となった。ただし、乱数検定法は全部で 250 種類ほど知られており、全部を確認することは非現実的であるので、今後は調査の範囲を絞ることも課題となった。今後の活動としては以下を検討している。

1) FIPS 140-2、SP 800-22、DIEHARD で採用されている各検定法の調査範囲の絞り込みと理論的根拠の確認及び計算機実験による検証
2) 以上の結果を踏まえての CRYPTREC 乱数検定ミニマムセットへの導入の判断
3) CRYPTREC 乱数検定ミニマムセットの暗号モジュール評価ツールへの組み込みの検討

2.2.2 暗号利用モード調査ワーキンググループ

2.2.2.1 調査背景

昨年度までの暗号技術評価委員会での活動では、暗号アルゴリズムの安全性の評価に注力し、暗号利用モードの調査は積極的に行われなかった。そのため、暗号利用モードの安全性に関する話題や実装性に関する記述は未整理であり、ユーザが操作モードを選択し、適切に用いるための必要な情報が提供できていなかった。

しかし、暗号利用モードはブロック暗号を実装する際には欠かせない技術である。システムの設計の際には、そのシステムに合った暗号利用モードを選択するのは重要であり、無配慮に利用モードを設計、選択、利用すると、場合によっては暗号アルゴリズムの効果が暗号処理に反映できず、安全性を脅かす場合もある。暗号利用モードの標準化状況についても、特に米国において従来の標準を見直し新たなモードを付け加える動きもある。これにはメッセージ認証のための利用モード(MAC)や、メッセージ認証機能付き暗号利用モードの標準化作業も含まれる。

上記のような背景から、電子政府の運用上、暗号利用モードに関する調査を行い調達側が適切な暗号利用モードを選べるようにすることが必要であると暗号技術監視委員会で合意が得られ、今年度からワーキンググループが組織され調査を行うことになった。

2.2.2.2 活動内容

1) ワーキンググループの構成と開催状況

暗号技術監視委員会から、今年度は以下の委員と暗号技術監視要員でワーキンググループを構成することが指示された。

主査：古原和邦　東京大学生産技術研究所　情報・システム大部門　助手
委員：川村信一　株式会社東芝 研究開発センター
　　コンピュータネットワークラボラトリー　主任研究員
委員：古屋聡一　株式会社日立製作所 システム開発研究所第 5 部　研究員

今年度のワーキンググループの開催は以下の通りである。

全体会合	6 月 23 日	東京ファッションタウン	10:03-11:41
第 1 回	7 月 14 日	メルパルク東京	13:06-13:58
第 2 回	2 月 2 日	メルパルク東京	13:15-14:15

正式な開催とはならなかったが、「暗号と情報セキュリティシンポジウム 2004(SCIS2004)」の会場やメーリングリスト上で活発な議論が行われた。

2)ワーキンググループの活動目標

暗号利用モード全般について評価方法と安全性についてまとめ、評価内容について技術的・理論的に示し、電子政府におけるシステム調達者が暗号利用モードの選定における判断材料となる資料を提供することが最終的な目標である。今年度は、既に利用されているものと新たに提案されてきたものを対象とし、現状をまとめることを目標とした。

3)今年度の活動内容

暗号利用モードは相互運用性が重視される技術であり、既に標準化されたものが採用される傾向がある。その上で、既存の利用モードに新たな機能を追加する形で新たな暗号利用モードが世界中の研究者達から学会や標準化団体等に提案されている状況がある。しかしながら暗号研究分野全体を見渡しても、暗号利用モードは暗号アルゴリズムと比較すると、多岐に渡るわけではなく、また、安全性の評価も十分なされているとは考えにくい。今年度は一般に暗号利用モードと呼ばれる技術の検証に注力することとした。また、特殊な利用環境を想定しているものや、技術公開を積極的に行っていないものについては、積極的に取り扱うことはしないこととした。これに関連して、特許の問題等が指摘されている場合は、知り得る範囲で記述することにした。

4)調査概要

調査 1)「暗号利用モードの現状と提案されている MAC の方式について」

現在利用されているもしくは提案されている暗号利用モードについて調査し、主に安全性の観点からその特徴をまとめる。また、同様に MAC についてもと調査し特徴をまとめる。

調査 2)「暗号利用モードの安全性評価について」

現在までに知られている暗号利用モードの評価の方法について、理論的な手法か、運用的な面も考慮したものか、の視点から調査しまとめる。

これらの結果を受けて、本ワーキンググループでは報告書を作成している。報告書内では MAC についても触れられているが、主眼は暗号利用モードの評価手法と現在の安全性評価の実情に置いた。MAC に関連してハッシュ関数、特に鍵付きハッシュ関数についての調査についても議論に上がったが、これらは技術的に比較的新しく未成熟な部分が多いため調査範囲が狭いので、今年度は積極的には調査を行わないことにした。

2.2.2.3 まとめ

表 2.a に示すものについて調査を行い、本ワーキンググループの報告書としてまとめた。

表 2.2 調査した暗号利用モード技術

秘匿に関するモード	認証暗号に関するモード	ディスクセクタ向けモード
ECB	CCM	EME
CBC	CWC	NR
k-CFB	EAX	
OFB	IACBC	
CTR	XCBC	
2DEM	IAPM	
ABC	OCB	
IGE	*k*-PCFB	
自己同期型利用モード		
F8@3GPP		

本報告書において、NIST、ISO/IEC、JIS、ANSI の暗号利用モードの捉え方に関する記述を第 3 章にまとめた。暗号利用モードの安全性を評価する上での手法や、証明可能安全性の議論については第 4 章に記述されている。各暗号利用モードの仕様や現時点での安全性評価に関しては第 5 章から第 7 章までに記載されている。

ここでは、相互運用性の観点と米国における標準化動向から、ECB、CBC、*k*-CFB、OFB、CTR についてのみ表 2.3 にまとめる。ECB 以外については、実運用上で現実的な脅威と考えられる問題点は指摘されていないが、ECB においても例えば数ブロックの非常に短い通信においては問題なく運用できるなど、安全に使用できる場合もある。安全性に関する詳細な解析については報告書を参照されたい。以下に表の読み方について記す。なお、「ブロック」とは 64 ビットブロック暗号を利用する場合には 64 ビット、128 ビットブロック暗号を利用する場合は、128 ビットを意味する。また、表中、*n* はブロック暗号の処理ビットサイズ、*k* は暗号利用モードの処理ビットサイズを示す。

- 秘匿に関する注意点
  実用上の安全性に問題点が指摘されているのは ECB だけであるが、その他の暗号利用モードについても現実的な脅威として捉えることができないものであっても現時点で知られている注意点について記した。
- 1[bit]エラー伝播範囲
  通信中に 1[bit]エラーが生じた場合、そのエラーが伝播する範囲。この範囲が小さい方が望ましい。
- 処理速度
  1 ブロックの出力を得るために暗号アルゴリズムを呼び出す回数。呼び出す回数が小さい方が処理速度は早い。

・ 並列実装性

暗号化および復号において、複数のブロックを同時に処理する並列処理を行うための並列実装が可能か否かについて。暗号化もしくは復号のどちらかのみが可能な場合もある。

・ 復号関数実装の必要性

暗号化と復号において処理の方法が異なる場合は、独立に暗号化用の回路と復号用の回路が必要になる。復号関数の実装が必要な場合は回路規模が、必要としない場合と比較して大きくなる。

・ コメント

以上の項目に合致しない特徴について記す。

表 2.3 秘匿に関する暗号利用モードのまとめ(1/2)

	秘匿に関する注意点	1[bit]エラー伝播範囲	処理速度	並列実装性		復号関数実装の必要性	コメント
				暗号化	復号		
ECB	・暗号文を見るだけで平文ブロックが同じ値であるか否かを判定できる。よって、特別な理由がない限り、通常のデータの暗号化等へは用いるべきでない。	1ブロック	1	有り	有り	必要	
CBC	・$2^{n/2}$ ブロック程度以上の平文を暗号化すると、暗号文一致攻撃により、暗号文を見るだけで平文に関する１ブロック分の情報が得られる可能性がある。	1 ブロック+1 ビット	1	無し	有り	必要	

表 2.3 秘匿に関する暗号利用モードのまとめ(2/2)

	秘匿に関する注意点	1[bit]エラー伝播範囲	処理速度	並列実装性		復号関数実装の必要性	コメント
				暗号化	復号		
k-CFB	・$2^{n/2}$ ブロック程度以上の平文を暗号化すると、暗号文一致攻撃により、暗号文を見るだけで平文に関する１ブロック分（k ビット）の情報が得られる可能性がある。 ・k が小さい場合、初期値と平文の組み合わせによっては、鍵ストリームの周期が極端に小さくなる恐れがある。	($\lfloor n/k \rfloor$~$\lceil n/k \rceil$) 平文ブロック+1 ビット(1 平文ブロック=k ビット)	k/n	無し	有り	不要	k[bit] の自動同期回復機能がある。
OFB	・$2^{n/2}$ ブロック程度で周期を形成。(kが小さい場合、IV によっては、暗号文から容易に鍵の候補を絞り込むことが可能。) ・初期値の運用を誤ると重大な欠陥につながる恐れがあり、注意が必要。	1 ビット	1	無し	無し	不要	
CTR	・初期値の運用を誤ると重大な欠陥につながる恐れがあり、注意が必要。	1 ビット	1	有り	有り	不要	

第3章 その他調査

3.1 TWIRL 調査

TWIRL(数体ふるい法専用のハードウェアデザイン)[8]の調査について報告を行う。

3.1.1 背景

2003 年に、Shamir と Tromer は TWIRL と呼ばれる、数体ふるい法におけるふるい処理部分を効率的に行うための計算機アーキテクチャの提案を行なった。TWIRL は汎用的な ASIC 技術を用いることで，ふるいと呼ばれる処理を高い並列度で処理することを特徴とする。これはシストリックアレイと呼ばれる巨大な並列計算のための計算機構造であって、0.13 μm プロセスの VLSI テクノロジーで実現し、1Ghz のクロックサイクルで動作させた場合に、1024 ビットの RSA 型合成数を分解する時間と費用の見積もりが 1 年未満で 10M ドル(約 10 億円)と、提案者達は彼らの論文の中で見積もっている。しかしこれは材料のみの費用であり、開発･設計費用は含まれていない。

主要な公開鍵暗号である RSA 暗号の標準的な鍵の長さは現時点(2004 年 3 月)において 1024 ビットであり、もしも TWIRL が現実に製造・動作可能となると、 RSA 暗号が解読可能であることを意味することになる。そこで、TWIRL 構築の実現性とそのための開発･設計費用について推測を行い、暗号技術の安全な利用のためのパラメータ設定において検討が必要になっていた。実際の実現性と現在の公開鍵暗号の安全性について論じた報告もある[5]。また TWIRL 以外にも類似の研究[1,2,3,4,6]が行なわれつつあるため素因数分解問題への専用ハードウェアの構成について十分な調査が必要であることは 2002 年度の CRYPTREC 活動でも指摘されており、Bernstein の研究[1]については調査を行なった[9]。

3.1.2 調査事項

TWIRL装置に関する技術を調査し、前提(仮定)および想定しているハードウェアの機能、開発費用、実現時期、ブレークスルーが必要な技術課題について分類し、整理し妥当性を検証し、技術的な可能性と課題の洗い出し、および基本ブロック図レベルの基本構成検討を行う。

3.1.3 評価1

TWIRL が1024-bit 合成数を素因数分解するのに必要なコストは、1000万ドル(約10 億円)

の費用と約 1 年の計算時間であると提案者は試算している。この試算の妥当性を検討するために、 TWIRL の動作内容を詳細に調査し、 基本回路設計を行うことで、 提案者の主張するハードウェアデザインと回路規模の見積もりの妥当性について検証を行った。

3.1.3.1 提案技術の各ブロックの説明

提案技術の各ブロックについて調査した。各ブロックについて、ブロック図、インターフェース、機能、サブブロック、評価者の見直しと提案論文との相違、動作概要について詳細に調査をおこなった。いくつかのブロックにおいては提案論文における仕様が十分でなく、パラメータ設定等で独自の判断をとらなければならない部分も多かった。

動作原理については、TWIRL を構成する大部分のユニットについては提案者の主張するハードウェアデザインおよび回路規模の見積もりは妥当であるが、配送機構 (Largish Station の Buffer と Smallish Station の Funnel) ユニットについては、提案者の見積もりよりも大規模な回路が必要である。

3.1.3.2 評価結果

評価で検討した基本回路設計をもとに検討を行った結果、現時点(2004 年 1 月)のテクノロジーを用いた場合、提案者が想定する性能を持つ TWIRL の実現は不可能であるとの結論に至った。その主な理由は以下の 3 点である。

・提案者の主張通り TWIRL を単一の LSI に実装するには、 直径 100 mm 以上の巨大ウェハーを欠損なく製造する技術が必要となる。 しかしこのような巨大なウェハーは現在の技術では製造不可能である。

・TWIRL を複数の LSI に分割して実装したとしても必要 LSI 数が膨大となり、単一のボードには実現不可能である。

・分割した LSI を複数のボードに実装したとしても,提案者が主張する周波数 (1 GHz) を前提とした場合、ボード間の IO 数が多数であることから、現在の技術では実現不可能である。

3.1.4. 評価2

評価は、アルゴリズム技術者による解析のグループと、装置自体の実装を評価するハード

ウェア技術者による評価グループとで行ない評価作業をまとめた。TWIRL の提案論文の紹介といくつかのその他のモデルについても考察している。TWIRL デバイスの面積評価、そう素部品に対する回路設計、Verilog 記述言語による評価、消費電力評価をおこなった。

3.1.4.1 結論

結論１：現状の提案はアイデアのレベルにとどまっており、詳細な装置仕様を記述するに至っていない。詳細な仕様を作成することは自明な作業ではなく、多くの障壁を乗り越えなければならないことが予想される。

結論２：30 ㎝ ウェハ規模の巨大な論理回路自体が非現実的である。その製造費用を考える以前に、その製造方法が存在しない。また、その代替案も困難であることが予想され、初期費用以前の問題である。仮に製造したとしても(主要な面積部分に対して) 1 GHz クロックによる動作を期待することはできない。
結論３：故障耐性については原著にて付録として扱っている。しかし、独立性の低い高並列な回路構成ゆえに、多くの出力に故障が起こることが想定されるなど、原著の検討で故障耐性が十分であるとは考えない。さらに、現状の半導体技術の経験から、今回の評価対象に適切な故障耐性を持たせる場合、全体でもかなりの部分を占めるパートについては、場合により大規模な冗長回路構成とする必要がある。すなわち、30 ㎝ ウェハに原著者が主張する機能を搭載するのは困難と考えるのが妥当である。

結論４：電力消費からくる発熱に対する冷却、および動作中のメンテナンスなども動作のコストとして計上されるべきであるが、これらは 30 ㎝ ウェハという大きな回路であり、現実的にどう克服してよいか、ノウハウがない。

結論５：その他、クロックツリーの構築、冗長回路の埋め込み、試運転段階の動作検査用論理などサポート技術、製造上のサイズマージンなど実世界での実装を試みた場合に回路規模の増加が強く見込まれる。

結論６：以上の懸念の多くは装置が占めるウェハ上の面積に関わる部分であり、半導体技術が進歩し、集積度があがればこれらは克服できる可能性がある。

3.1.5 参考文献

[1] D.J.Bernstein, Circuits for integer factorization: a proposal, 2000.
Available at http://cr.yp.to/papers.html
[2] W.Geiselmann, R.Steinwandt, A dedicated sieving hardware, PKC 2003, LNCS 2567, pp.254-266, Springer-Verlag, 2003.
[3] W.Geiselmann, R.Steinwandt, Hardware to solve sparse systems of linear equations over GF(2), CHES 2003, LNCS, 2779, pp.51-61, Springer-Verlag, 2003.
[4] W.Geiselmann, R.Steinwandt, Yet Another Sieving Device, CT-RSA 2004, LNCS 2964, pp.278-291, Springer-Verlag, 2004.
[5] B.Kaliski, TWIRL and RSA Key Size,
2003. Available at http://www.rsasecurity.com/rsalabs/
[6] A.K.Lenstra, A.Shamir, Analysis and optimization of the TWINKCLE factoring device, EUROCRYPT2000, LNCS 1807 pp35-52 Springer-Verlag, 2000
[7] A.K.Lenstra, A.Shamir, J.Tomlinson, E.Tromer, Analysis of Bernstein's factorization circuit, Asiacrypt 2003, LNCS 2501, pp.1-26, Springer-Verlag, 2002.
[8] A.Shamir, E.Tromer, Factoring Large Numbers with the TWIRL Device, CRYPTO 2003, LNCS 2729, pp.1-26, Springer-Verlag, 2003.
[9] Bernstein及びA.K.Lenstraらの素因数分解(行列計算ステップ)回路に関する調査報告書
CRYPTREC調査報告書 2002-0039, Available at
http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec20030424_outrep.html

3.2 SSL 調査

3.2.1 背景

2001年度、暗号技術検討会により電子政府システム等に暗号技術を組み入れる際に利用される可能性が高いと判断された暗号プロトコルであるSSL/TLSに関して、これまでに報告されてきた脆弱性に関して、

- 暗号方式そのものの安全性、
- プロトコル(メカニズム)としての安全性、
- 実装に関する安全性、
- 運用上の安全性

といった観点から調査を行った[7]。その後約2年が経過し、その間に方式や実装に関わる新たな攻撃や改良された攻撃が提案されている。このような背景から、前回の調査後から現在におけるSSL/TLSについて調査を行うこととした。

3.2.2 調査目的

2001年度におけるSSL/TLSの調査では「最新版で修正プログラムを当てている限り安全である」という結論であった。最近ではOpenSSLについて、Bleichenbacherの攻撃の拡張、VaudenayのCBCパディング攻撃、ASN.1ライブラリにおける脆弱性等、サイドチャネル攻撃や実装上の問題点等が指摘されており、こういったSSLの現状を把握しておく必要があると考えた。そのため、監視作業の一環としてSSLの現状を把握する追加調査および修正プログラムに関する運用方法についての調査を実施すべきと判断した。

具体的には、調査対象としてはSSLVer3.0/TLS Ver1.0以上とし、前回の調査後から2004年1月時点までに新たに発見・指摘された脆弱性の分析と対処法を調査項目とした。

3.2.3 脆弱性調査の結果要約

(1) サイドチャネル攻撃

(a) SSL/TLSで用いられる暗号化のパディング(CBCパディング)に関して、バイト単位の固定のパディングパターンを使用している場合、パディングの正当性チェックの結果を利用して、平文をバイト単位で逐次求めることが可能であるという攻撃手法が存在する。

(b) RSA Encryptionについては、これまで報告されたBleichenbacher のPKCS#1 v1.5に対する適用的選択暗号文攻撃を改良した実用的な攻撃手法や、PKCS#1 v.2.1に従う

EME-OAEP-DECODE 手法による復号プロセスにおいて、攻撃者が平文の一部のハミング重みを集めることにより、平文の最下位ビットを露呈させ、さらにその情報から所望の平文を得るという新たな攻撃法も提案されている。

(c) SSL のソフトェアで用いられている RSA 実装において、高速化を目的として用いられる Montgomery reduction や Karatsuba 乗算法に起因し、RSA 復号処理においてその入力値の大きさにより処理ロジックが異なり、タイミング攻撃が成功する報告もなされている。

いずれの攻撃法についても、対策が提案され、最新のソフトウェアでは対処がなされている。

(2) 実装上、その他の問題点

(a) 通信プロトコルを記述するために用いられる ASN.1 (Abstract Syntax Notation 1) は、SSL/TLS 以外にも SNMP (Simple Network Management Protocol)、SIP (Session Initiation Protocol)や S/MIME (Secure/Multipurpose Internet Mail Extensions) 等のエンコードに用いられている。その中の BER (Basic Encoding Rules)エンコードは可変長をサポートした汎用性のある方法であるが、注意深く実装しなければバッファオーバーフロー等の脆弱性を誘発する危険性がある。実際、OpenSSL における ASN.1 の BER エンコードにおける脆弱性は複数回報告されている。今後も発生する可能性があるので注意が必要である。

(b) その他、SSL/TLS プロトコルに付随するものとしては、ルート証明書の更新手法における証明書管理技術に関する課題や、ブラウザのセキュリティホールによるアドレスバーの詐称の問題等があった。

なお、種々のセキュリティホールについては、パッチによる対策がなされているが、アドレスバーの脆弱性については、現時点でパッチが公開されていない(2004 年 1 月末現在)。

3.2.4 修正プログラムの管理･運用方法について

SSL 機能を持つサーバ及びクライアントを使用する上での各種設定方法等運用方法と、それに伴うセキュリティについて考察を行った。サーバプログラムとしては、Web サーバである Apache に SSL 機能を追加する代表的な OpenSSL モジュールである mod_ssl を対象とし調査を行った。また、クライアントプログラムとしては、代表的なブラウザである Internet Explorer、Netscape Navigator を調査対象とした。

また、SSL/TLS と直接関係はないが、運用上の対策として最新パッチを管理する技術が重要となるため､一般的なソフトウェアの運用の課題として､米国の NIST(National Institute of Standards and Technology)から発行されている、セキュリティ上の問題を修正するパッチの運用指針を定めた“(SP 800-40) Procedures for Handling Security Patches” ([4])

に関する調査を行った。たとえば、この文書では、組織内に PVG (Patch and Vulunerability Group)というグループを設けて、

- 脆弱性やパッチの情報を収集して、組織固有のパッチ・データベースを作成する。
- パッチのテストを行い、システム管理者に脆弱性とパッチを提供する。
- スキャニングによって、パッチの適用状態を検証する。

といった業務等を行う方針を打ち出している。

3.2.5 結論

SSL/TLS はある種、完成されたセキュリティプロトコルと考えられているが、2001 年度の調査後も、バッファオーバーフロー等の実装上の問題点に加えて、タイミング攻撃等において新たなサイドチャネル攻撃が提案されているのが実状である。

これらの攻撃に対しては実装上で対策が取られており、最新の修正プログラムを当てている限り安全であるが、利用者は常に最新の状態に保つことが必要となる。

そのため、電子政府等の各種システムで暗号プロトコルである SSL/TLS を安全に利用するためには、今後も継続的に SSL/TLS の安全性について監視を行い、脆弱性に関する正確な情報を入手していくとともに、ソフトウェアに最新の対策を施すための運用にまで目を配らせることが望まれる。

3.2.6 参考文献

[1] J. Black, and H.Urtubia. “Side-Channel Attacks on Symmetric Encryption Schemes: The Case for Authenticated Encryption”, In Proc. of 11th USENIX Security Symposium 2002, pp. 327338, 2002.

[2] D. Brumley, and D. Boneh, “Remote Timing Attacks are Practical”, In Proc. of the 12th Usenix UNIX Security Symposium, USENIX, 2003.

[3] B. Canvel, A.Hiltgen, S.Vaudenay, and M.Vuagnoux. “Password Interception in a SSL/TLS Channel”, CRYPTO 2003, LNCS, No.2729, pp.583-599, 2003.

[4] NIST Special Publications, http://csrc.nist.gov/publications/nistpubs/index.html.

[5] S. Vaudenay, “Security Flaws Induced by CBC Padding – Applications to SSL, IPSEC, WTLS...”, EUROCRYPT 2002, LNCS, No.2332, pp.534-545, 2002.

[6] K. G. Paterson, and A. Yau. “Padding Oracle Attacks on the ISO CBC Mode Encryption Standard”, In, Proc. of CT-RSA04, 2004.

[7]CRYPTREC 暗号アルゴリズム及び関連技術の評価報告 http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec20030424_outrep.html.

3.3 素因数分解問題と計算機実験

この節では、素因数分解問題に関する計算機実験プロジェクトについて報告し、ビット数が大きな数の素因数分解が有する困難性に関する安全性について述べる。

3.3.1 調査の背景とその目的

本計算機実験プロジェクト開始当時においても、高度情報通信ネットワーク社会形成基本法に基づく e-Japan 重点計画 (平成 13 年 3 月 29 日高度情報通信ネットワーク推進戦略本部決定) に基づき、国内の高度情報通信ネットワークの安全性及び信頼性を世界最先端の IT 国家にふさわしいものにするために、高度情報通信ネットワークにおける脅威に起因するサービス提供機能の停止が最小限となるような各種の施策を実施することとなっており、特に、電子署名等の電子認証の普及、電子政府の構築等に向けて、高度情報通信ネットワークの安全性及び信頼性を確保するためには、基盤技術である暗号技術について、客観的な評価が重視されていた。

2001 年度から施行された、「電子署名及び認証業務に関する法律」では、その第 33 条において、特定認証業務に関する認定の制度の円滑な実施を図るため、電子署名及び認証業務に係る技術の評価に関する調査及び研究を行うことが記されている。また、「電子署名及び認証業務に関する法律施行規則」では、その第 2 条第 1 項において、電子署名の安全性に適合する基準の 1 つとして、「ほぼ同じ大きさの 2 つの素数の積である 1024 ビット以上の整数の素因数分解」が有する困難性を挙げている。さらに、電子署名及び認証業務に関する法律の施行の円滑化を図ることを目的として定められている「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」では、その第 3 条第 1 項において、モジュラスとなる合成数が 1024 ビット以上の RSA 方式 (及び RSA-PSS 方式[1]) を挙げている。

これらを受けて、2001 年度、暗号技術検討会では、電子署名法等に基づいて利用される暗号技術の評価 (電子署名に用いる暗号技術等への助言) を実施することが決められた。暗号技術検討会からの要請を受け、公開鍵暗号評価小委員会では 2000 年度に実施された評価を踏まえて、さらに詳細な安全性評価を実施すべく調査・研究を開始した。数論的問題の困難性に依拠して暗号プリミティブの安全性を主張する暗号スキームを横断的に評価するため、2002 年度までに調査された内容については、CRYPTREC Report 2002[3, 2.4 節] にまとめられている。本計算機実験プロジェクトは、素因数分解問題の困難性の調査・研究の一環として挙げられ、実施されたものの中の 1 つであって、素因数分解を実行するソフトウェアを開発し、実際に素因数分解を行うことにより、いろいろな論文等の評価でいわれている 1024 ビット素因数分解の難しさが妥当かどうか実験的に検証することが主な目的である。

[1] 平成 14 年総務省 法務省 経済産業省告示第 13 号 (平成 14 年 11 月 21 日官報第 3492 号) のよる一部改正。

3.3.2 素因数分解問題に関する背景

素因数分解問題の困難性、すなわち、同程度の大きさの 2 つの異なる素数 p, q の積である合成数 N が与えられたときにその素因数 p, q を知ること、を評価する方法には大きく分けて 3 種類ある。

(a) 現在存在しているハードウェア上でプログラムを作成し実験を行う。

(b) 現在の技術で作成可能だが実際には作られていないハードウェアを用いて思考実験を行う。

(c) 現在の技術では実現不可能なハードウェアを用いて思考実験を行う。

(b) に属するものとしては、TWIRL[15] 等があり、(c) の代表としては、量子計算機があるが、これらの実現可能性を含めた議論は本節では扱わないものとする。(a) の方法は昔からさまざまな方法が考案されてきたが、それらは実行時間の関数を決める主要因に応じて 2 種類に大別される。一方は、N に含まれる最小素因数のサイズに依存して実行時間が決まるものであり、他方は、N のサイズに依存して実行時間が決まるものである。前者に属するアルゴリズムのうち最高速のものは楕円曲線法 (ECM) であり、後者に属するもので最高速は一般数体ふるい法 (General Number Field Sieve method)(以下、GNFS と略記する) である。どちらも準指数関数時間を要する。つまり、$L_x[r, \alpha]$ を、$x \to \infty$ のときの漸近的振る舞いが、

$$\exp((\alpha + o(1))(\log x)^r (\log\log x)^{r-1}) \quad (\alpha, r \text{ は共に実数で、} 0 \le r \le 1 \text{ を満たす。} \log \text{は自然対数とする。}) \tag{3.1}$$

と同等な任意の関数とするとき、これらのアルゴリズムの実行時間はどちらもある $\alpha, r\ (0 < r < 1)$ に対して $L_x[r, \alpha]$ に属する。

GNFS の概要　GNFS は、非自明な関係式

$$x^2 \equiv y^2 \pmod{N} \tag{3.2}$$

を見つけ、$\gcd(x \pm y, N)$ を計算することにより N の素因数を見つける一連のアルゴリズムを指す。GNFS を大きく分けると、

(1) 多項式選択　(2) 関係式収集　(3) フィルタリング　(4) 行列計算　(5) 平方根計算

の 5 つのステップに分かれる。以下のパラグラフにおいてそれぞれのステップについて簡単に説明する。詳細については、[6, 12, 1, 13, 14, 2, 16] 等を参照のこと。

多項式選択　大量の関係式 (relation) を効率良く収集するという観点から、$f(m) \equiv 0 \pmod{N}$ を満たす整数係数の既約多項式 f (と整数 m) を 1 つ選択するステップ。多項式の選び方により全体の実行時間が左右される。現在の素因数分解実験の世界記録程度だと、多項式の次数 d は 5 次くらいが有効であると考えられている。

関係式収集　f の 1 つの根を θ とするとき、決められた範囲内の有理整数 $a+bm$ およびイデアル $(a+b\theta)$ $(a,b$ は互いに素) がそれぞれ、決めれた上限以下の素数および素イデアル (factor base) で割り切れるかどうか (smooth) を判定するステップ。代表的な方法として、線ふるい (line sieve) と格子ふるい (lattice sieve) の 2 つがある。factor base の上限よりも大きい範囲の素数あるいは素イデアルも数個、因子として許容する変形版 (variation) がいくつか提案されていて、よく利用されている。本ステップの実行時間は、上述のパラメータを適当に取ることによりある α に対して $L_N[1/3, 2\alpha]$ に属し、GNFS の実行時間において支配的であるが、多くの処理が独立に計算可能なので並列化の効果が大きい。

フィルタリング　行列計算ステップへ進む前に、大量に収集された関係式を整理して、行列サイズを縮小するステップ。非自明な関係式を構成するのに寄与しない無駄なデータを積極的に排除することにより、次のステップである行列計算を高速化する。

行列計算　大規模な疎行列を M としたとき $Mv = 0$ を満たす解 $v(\neq 0)$ を求めるステップ。本ステップの実行時間 (及び行列の行数) は、上述のパラメータを適当に取ることによりある β に対して $L_N[1/3, 2\beta]$ (及び $L_N[1/3, \beta]$) に属し、GNFS の実行時間において支配的であるが、現在知られている方法では処理の独立性が低くく、並列化の効果はそれほど大きくはない。言い換えると、効率的な並列・分散処理には計算機 (CPU) 間の密結合が要求される。

平方根計算　有理整数と代数的数の平方根を計算し、式 (3.2) を満たす x, y を求めるステップ。有理整数側は平方根を直接的に求められるのに対して、代数的数側ではイデアルの積しか求められていないため直接的にとはいかない。代表的な方法としては、格子基底簡約アルゴリズムを利用して平方根イデアルから平方根を近似するという計算テクニックを用いる方法が知られている。

最近の素因数分解記録　参考のため、近年、GNFS によって素因数分解された結果を以下の表 3.1 に示す。なお、RSA-576 に関しては、Bonn 大の Jens Franke 氏が [9] と同じワークショップにて、関係式収集時間 13.2 年 (Pentium III 1GHz 換算)、収集した relation 数は 635M、行列計算時間は 12 日 (64 × Alpha 660MHz) という処理概要を速報している。

表 3.1: 近年の GNFS による分解記録 [5, 1]

合成数	ビット数	分解者	分解発表日
RSA-155	512	CWI ら	1999 年 8 月
Simon Singh	512	Granlund ら	2000 年 10 月
c158 in $2^{953}+1$	524	Bonn 大ら	2002 年 1 月
RSA-160	530	Bonn 大ら	2003 年 4 月
RSA-576	576	Bonn 大ら	2003 年 12 月

3.3.3 素因数分解計算機実験プロジェクトにおける調査結果の概要

2002 年 1 月から 2004 年 3 月までの 2 年強の間、素因数分解計算機実験プロジェクトが実施され、その間に、大きな数の素因数分解に必要な計算量について従来より信頼性の高い見積りを出すべく、統一された環境で数多くの RSA のモジュラスの素因数分解が行なわれた。すなわち、世界水準の GNFS 実装を用い、90 桁から 150 桁までの 10 桁刻の合成数の分解実験をいくつか行ない、得られた実験データを理論的に予想される評価式に当てはめ、それを外挿 (extrapolation) することにより 1024 ビットの素因数分解の実行時間の見積りを行い、現在、市販されている汎用のハードウェア (パソコン等) を用い、2 年程度 (関係式収集および行列計算にそれぞれ 1 年位) で分解を完了するためには、一企業や一研究グループでは集められないような数の計算機資源を要することが推測されるとの見積りを得た。なお、これらの見積りについては以下のパラグラフにおいて要約して紹介する。

また副産物として、表 3.3 にあげる従来因子の知られていなかった合成数の分解に成功した。特に、この表中、c164 in 2,1826L は GNFS で分解された合成数の大きさでは世界 2 位であり、c248 in 2,1642M は特殊数体ふるい法 (SNFS) で分解された合成数の大きさで世界 1 位であった[2]。これらの結果は、実際に利用された GNFS 実装が世界水準に達していることを示しており、そこから得られる実験データが現時点でベストに近いものであることを保証している。

主なスケジュール　本計算機実験プロジェクトの主なスケジュールは以下の表 3.2 の通りであった。

主な素因数分解記録　本計算機実験プロジェクト等によって素因数分解された結果[3]を以下の表 3.3 に示す [1]。c164 in 2,1826L に関しては、関係式収集時間は約 7 年 (Pentium 4 2.53GHz 換算)、収集した relations 数は 458M、行列計算時間は約 12 日 (16× Pentium 4 2.6GHz) と報告されている [1]。

選択する多項式の次数と関係式収集時間の外挿　上述の評価式 (3.1) は x が大きくなるときの漸近的な評価であるが、今回対象となる大きさの範囲の N については選択する多項式の次数 d は 4,5,6 と非常に小さい。そこで、今回は [10, Section 3.1] の指摘を採用し、実行時間 (単位 CPU・年) を理論から予想される次数別の評価式

$$C_d \exp\left((1+o_d(1))\left(d\log d + \sqrt{(d\log d)^2 + 4\log(n^{1/(d+1)})\log\log(n^{1/(d+1)})}\right)\right) \tag{3.3}$$

を用いて近似する。

[2]分解対象は Cunningham 数から選択されている。後者は 2004 年 4 月 4 日付の記録である (http://www.rkmath.rikkyo.ac.jp/~kida/snfs248.htm)。Cunningham プロジェクト全般については、http://www.cerias.purdue.edu/homes/ssw/cun/ を参照のこと。

[3]素因数分解に使った計算資源、及びその実装に用いた稼働は中心となって活動したメンバ及びその所属組織に帰属する場合もあり本成果は必ずしも CRYPTREC だけのものでない。

表 3.2: 主なスケジュール

2001 年度末	立教大学で勉強会を 4 回開催。プロジェクトの進め方及び数体ふるい法に関する報告書 [6] が提出される。
2002 年度	不定期に勉強会を数回開催。line sieve プログラム実装における高速化の解説や、関連論文の解説等が行なわれる。
2003 年度	8 月頃までに block Lanczos 法の実装が終了し、特殊数体ふるい法で line sieve を用いて、Cunningham 数をいくつか分解することに成功する。引き続き、lattice sieve 及び、平方根の実装完了にともない、いくつかの Cunningham 数、及び 90〜150 桁の分解実験を行なった。また、いくつかの未分解 Cunningham 数や分割数の分解に成功した。これらの分解実験を通じて、ビット数の大きな数の計算量の見積りを行なった。SCIS や ISEC 等へ結果等が論文発表された (本節の参考文献を参照)。

表 3.3: 本計算機実験プロジェクト等で分解した合成数 [1]

c161 in 3, 409+	SNFS	$3146556580457915284319008046876542171617718876815478513 \times p107$
c173 in 3, 419+	SNFS	$655637289610437314600881201740188993708411415076269 49 \times p120$
c163 in p(29675)	ECM	$22397255528160225411990840248205316 97 \times p126$
c163 in p(22733)	ECM	$45211894866667804086453435775564396429676244467 \times p116$
c164 in 7, 316+	ECM	$88170017041631125909548421501685554015451 29 \times p122$
c165 in 2,2030L	ECM	$87678355175652250615083617929401084618044201 \times p121$
c198 in 3, 431−	SNFS	$5327475339364876749276709275805059852090562839012167 \times p147$
c164 in 2,1826L	GNFS	$34334644886182446546273008924242084634327089789559771215864092254849 \times p97$
c249 in 2, 827+	ECM	$69787377067722881486602094502761253930262932578924438539 \times p193$
c248 in 2,1642M	SNFS	$75052937460116417664924678548932616036640381023147128390479077762437 \backslash 12148179748450190533 \times p160$

p(·) は分割数を示す。例えば「Factorization of Partition Numbers」(`http://www.asahi-net.or.jp/~KC2H-MSM/mathland/part/index.htm`) では分割数の素因数分解結果を収集している。

図 3.1: 関係式収集時間の外挿結果

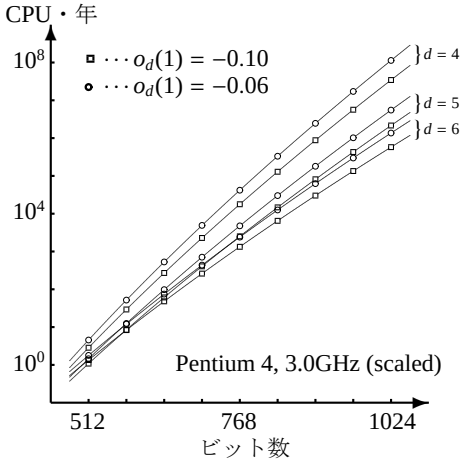
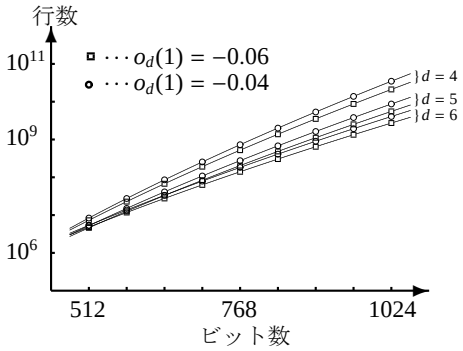


図 3.2: 大規模疎行列の行数の外挿結果



得られた実験データから定数 C_d, o_d を決定しそれらを外挿した結果、以下の図 3.1 のような結果を得た [7, 11]。

したがって、今回採用した外挿法が妥当であるならば、1024 ビットの合成数を GNFS で素因数分解するには 6 次式を使うのが良く、そのとき関係式収集ステップを 1 台の PC で行うと 50 万年から 140 万年かかるものと推測される。つまり、50 万台から 140 万台の PC を同時に稼動させれば 1 年で関係式収集ステップを終える計算になる[4]。ただし、実行時間は Pentium 4, 3.0GHz の PC におけるものとする。

選択する多項式の次数と大規模疎行列のサイズの外挿　関係式収集時間の場合と同様に、評価式を外挿した結果、以下の図 3.2 のような結果を得た [7, 11]。

したがって、今回採用した外挿法が妥当であるならば、1024 ビットの合成数を GNFS で素因数分解するには 6 次式を使うのが良く、そのとき、大規模疎行列の行数は 2.7×10^9 から 4.0×10^9 程度になると見積もられる。

行列計算の実行時間の評価　実験例が少ないことから評価式による外挿に基づいた行列計算時間の見積りはせず、行列計算時間を行列の行数の 2 乗で下から押さえることで評価を行った [7]。

表 3.3 中の c164 in 2,1826L の分解のとき、行列の行数は 7×10^6 で、16 台の PC をギガビット・イーサネットで接続した PC クラスタ上での行列計算時間は約 12 日、そのときのネットワークの通信時間が全体の 1/3 ほどであったことを用いる [13, 8 節]。

計算機の台数を $\lambda = \mu^2$ とすると計算時間は $1/\lambda$ に比例して減るが、通信時間は $1/\mu$ に比例してしか減らないことに注意すれば、1024 ビットの素因数分解に必要な行列計算時間は、その行数を上述のように 4×10^9 と見積もった場合、今回採用した外挿法が妥当であるならば、4096 台の PC を 10 ギガビット・イーサネットで接続したクラスタで 50 年以上、または、227 万台の PC を 10 ギガビット・イーサネットで接続したクラスタで 1 年以上かかるものと見積もられる。ただし、実行時間は Pentium 4, 2.53GHz の PC におけるものとする。

3.3.4　補足

Lenstra らの報告 [8, Section 4] でも指摘されているように、式 (3.1) を用いて単純に外挿する見積りでは、N のビット数による $o(1)$ 項の違いを考慮しないので誤った結果を導く可能性があり、注意が必要である。実際、彼らはこれらを避けるため、smooth さを与える確率の関数を基礎にして別の評価方法を提案して見積りを行っている。

[4] 1024 ビットでは factor base の素数の大きさも 32 ビットを越えて 37 ビットほどになるので、seti@home(`http://setiathome.ssl.berkeley.edu/`) のような Internet による分散計算に直ちに乗せることはできないものと考えられる。

なお、Lenstra の報告 [9] では 1024 ビットの関係式収集時間を上述のおよそ 200 倍から 600 倍多く見積もっている。

3.3.5 まとめ

(i) 2002 年 1 月から 2004 年 3 月までの 2 年強の間実施された素因数分解計算機実験プロジェクトについて概要を報告した。理論的に予想される次数別の評価式を得られた実験データから外挿 (extrapolation) することにより 1024 ビットの素因数分解の実行時間の見積りを行った。その結果、今回採用した外挿法が妥当であるならば、当面の間、1024 ビット以上の整数の素因数分解が有する数論的困難性の安全性基準には問題がないことがわかった。

(ii) 1024 ビットの素因数分解における関係式収集に関しては、Lenstra らの報告 [8, 9] があり、今回の素因数分解計算機実験プロジェクトの外挿結果よりも大きい見積りを提出しているので、これらの点についてはさらなる検討が必要であると考えられる。

(iii) 近年、専用のハードウェアによる素因数分解を行う提案がいくつか行われている。ハードウェアの進歩は非常に速いことから、今後の発展状況を継続して注意深く監視していくことが必要であると考えられる。

参考文献

[1] 青木和麻呂, 植田広樹, 木田祐司, 下山武司, 園田裕貴, “一般数体篩法実装実験 (1) －概要,” SCIS2004 予稿集, 講演番号 2B1-3, 2004.

[2] 青木和麻呂, 伊豆哲也, 植田広樹, 下山武司, “一般数体篩法実装実験 (2) －ミニ素因数分解・ミニ素数判定,” 信学技報 Vol.103 No.711, IT-2003-112, pp.229–234, 電子情報通信学会, 2004.

[3] CRYPTREC, “CRYPTREC Report 2002,” CRYPTREC, 2003. Available at http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec20030512_report044.htm

[4] 富士通株式会社, “数体ふるい法における多項式選択部分・線形代数部分・イデアル平方根計算部分についての調査研究,” CRYPTREC 暗号技術関連の調査報告 No.0203, CRYPTREC, 2004. Available at http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec20040331_outrep.html

[5] 伊豆哲也, 木田祐司, “素因数分解の現状について,” 日本応用数理学会論文誌, Vol.13, No.2, pp.289–304, 2003.

[6] 木田祐司, “暗号アルゴリズムの詳細評価に関する報告書,” CRYPTREC 暗号アルゴリズム及び関連技術の評価報告 No.0021, CRYPTREC, 2002. Available at http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec20030424_outrep.html

[7] 木田祐司, “素因数分解計算機実験 研究調査報告書,” CRYPTREC 暗号技術関連の調査報告 No.0201, CRYPTREC, 2004. Available at http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec20040331_outrep.html

[8] Arjen K. Lenstra, Eran Tromer, Adi Shamir, Wil Kortsmit, Bruce Dodson, James Hughes, Paul Leyland, “Factoring estimates for a 1024-bit RSA modulus,” proc. Asiacrypt 2003, LNCS 2894, pp.55–74, Springer-Verlag, 2003.

[9] Arjen K. Lenstra, “SNFS versus GNFS, and the feasibility of factoring a 1024-bit number with SNFS,” EIDMA-CWI Workshop, Factoring large integers with the Number Field Sieve, December, 2003. Available at http://db.cwi.nl/projecten/project.php4?prjnr=84

[10] Brian A. Murphy, “Polynomial Selection for the Number Field Sieve Integer Factorisation Algorithm, Ph. D thesis, Australian National University, 1999. Available at http://web.comlab.ox.ac.uk/oucl/work/richard.brent/ftp/Murphy-thesis.ps.gz

[11] 日本電信電話株式会社, “素因数分解問題調査報告書,” CRYPTREC 暗号技術関連の調査報告 No.0202-1, CRYPTREC, 2004. Available at http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec20040331_outrep.html

[12] 日本電信電話株式会社, “「素因数分解問題に関する研究調査」素因数分解問題調査報告書～SQUFOF 法の実装報告～,” CRYPTREC 暗号技術関連の調査報告 No.0202-2, CRYPTREC, 2003. Available at http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/fy15/cryptrec20040331_outrep.html

[13] 下山武司, 植田広樹, 青木和麻呂, “$GF(2)$ 上の巨大疎行列に対する並列計算法,” SCIS2004 予稿集, 講演番号 2B1-4, 2004.

[14] 下山武司, 青木和麻呂, 植田広樹, 木田祐司, “一般数体篩法実装実験 (4) －線形代数,” 信学技報 Vol.103 No.711, IT-2003-114, pp.241–246, 電子情報通信学会, 2004.

[15] Adi Shamir, Eran Tromer, “Factoring Large Numbers with the TWIRL Device,” proc. CRYPTO 2003, LNCS 2729, pp.1-26, Springer-Verlag, 2003.

[16] 植田広樹, 青木和麻呂, 木田祐司, “一般数体篩法実装実験 (3) － Filtering,” 信学技報 Vol.103 No.711, IT-2003-113, pp.235–240, 電子情報通信学会, 2004.

付録

電子政府推奨暗号リスト

平成１５年２月２０日
総　　務　　省
経　済　産　業　省

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注 1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注 2)
共通鍵暗号	64 ビットブロック暗号(注 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注 4)
	128 ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注 5)
その他	ハッシュ関数	RIPEMD-160(注 6)
		SHA-1(注 6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注 7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

注釈：

(注 1)　SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

(注 2)　KEM（**Key Encapsulation Mechanism**）-DEM(Data **Encapsulation Mechanism**)構成における利用を前提とする。

(注 3)　新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。

(注 4)　3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。

1)　FIPS46-3 として規定されていること

2)　デファクトスタンダードとしての位置を保っていること

(注 5)　128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。

(注6)　新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。

(注7)　擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

電子政府推奨暗号リスト掲載暗号の問い合わせ先一覧

１．１　公開鍵暗号技術

暗号名	DSA
関連情報	仕様 ・ANSI X9.30:1-1997, Public Key Cryptography for The Financial Services Industry: Part 1: The Digital Signature Algorithm (DSA) で規程されたもの。 ・参照 URL <http://www.x9.org/>　なお、同規格書は日本規格協会(http://www.jsa.or.jp/)から入手可能である。

暗号名	ECDSA (Elliptic Curve Digital Signature Algorithm)
関連情報	公開ホームページ 和文：　http://www.labs.fujitsu.com/techinfo/crypto/ecc/ 英文：　http://www.labs.fujitsu.com/en/techinfo/crypto/ecc/
問い合わせ先	富士通株式会社 電子政府推奨暗号 問合わせ窓口 E-MAIL：crypto-ml@ml.soft.fujitsu.com

暗号名	RSA Public-Key Cryptosystem with Probabilistic Signature Scheme (RSA-PSS)
関連情報	仕様　公開ホームページ ・PKCS#1 RSA Cryptography Standard (Ver.2.1) ・参照 URL <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/ 和文：　なし 英文：　http://www.rsasecurity.com/rsalabs/submissions/index.html
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 デベロッパ営業本部 部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

暗号名	RSASSA-PKCS1-v1_5
関連情報	仕様　公開ホームページ ・PKCS#1 RSA Cryptography Standard (Ver.2.1) ・参照 URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html 和文：　なし 英文：　http://www.rsasecurity.com/rsalabs/submissions/index.html
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 デベロッパ営業本部 部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

暗号名	RSA Public-Key Cryptosystem with Optimal Asymmetric Encryption Padding (RSA-OAEP)
関連情報	仕様　公開ホームページ ・PKCS#1 RSA Cryptography Standard (Ver.2.1) ・参照 URL http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html 和文：　なし 英文：　http://www.rsasecurity.com/rsalabs/submissions/index.html
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 デベロッパ営業本部 部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

暗号名	RSAES-PKCS1-v1_5
関連情報	仕様 ・PKCS#1 RSA Cryptography Standard (Ver.2.1) ・参照 URL <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html>
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 デベロッパ営業本部 部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

暗号名	DH
関連情報	仕様 ・ANSI X9.42-2001, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography で規定されたもの。 ・参照 URL <http://www.x9.org/>　なお、同規格書は日本規格協会(http://www.jsa.or.jp/)から入手可能である。

暗号名	ECDH (Elliptic Curve Diffie-Hellman Scheme)
関連情報	公開ホームページ 和文： http://www.labs.fujitsu.com/techinfo/crypto/ecc/ 英文： http://www.labs.fujitsu.com/en/techinfo/crypto/ecc/
問い合わせ先	富士通株式会社 電子政府推奨暗号 問合わせ窓口 E-MAIL：crypto-ml@ml.soft.fujitsu.com

暗号名	PSEC-KEM Key agreement
関連情報	公開ホームページ 和文： http://info.isl.ntt.co.jp/ 英文： http://info.isl.ntt.co.jp/
問い合わせ先	〒239-0847 神奈川県横須賀市光の丘 1-1-609A 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所 セキュリティプラットフォームグループ 主任研究員 神田雅透 TEL：046-859-2437, FAX：046-855-1533, E-MAIL：kanda@isl.ntt.co.jp

１．２ 共通鍵暗号技術

暗号名	CIPHERUNICORN-E
関連情報	公開ホームページ 和文： http://www.hnes.co.jp/products/security/index.html 英文： http://www.hnes.co.jp/products/security/index-e.html
問い合わせ先	〒108-8558 東京都港区芝浦 2-14-22 日本電気株式会社 インターネットソフトウェア事業部 TEL：03-3456-6436, FAX：03-3456-5819, E-MAIL：soft@security.jp.nec.com

暗号名	Hierocrypt-L1
関連情報	公開ホームページ 和文： http://www.toshiba.co.jp/rdc/security/hierocrypt/ 英文： http://www.toshiba.co.jp/rdc/security/hierocrypt/
問い合わせ先	〒212-8582 神奈川県川崎市幸区小向東芝町 1 (株) 東芝 研究開発センターコンピュータ・ネットワークラボラトリー 研究主務 秋山浩一郎 TEL：044-549-2156, FAX：044-520-1841 E-MAIL:crypt-info@isl.rdc.toshiba.co.jp

暗号名	MISTY1
関連情報	公開ホームページ 和文： http://www.security.melco.co.jp/misty 英文： http://www.security.melco.co.jp/misty
問い合わせ先	〒100-8301 東京都千代田区丸の内 2-2-3 (三菱電機ビル) 三菱電機株式会社 インフォメーションシステム事業推進本部情報セキュリティ推進センター センター長 小松田敏二 TEL：03-3218-3221, FAX：03-3218-3221 E-MAIL： Binji.Komatsuda@hq.melco.co.jp

暗号名	Triple DES
関連情報	仕様 ・FIPS PUB 46-3, Data Encryption Standard (DES) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkencryption.html>

暗号名	AES
関連情報	仕様 ・FIPS PUB 197, Advanced Encryption Standard (AES) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkencryption.html>

暗号名	Camellia
関連情報	公開ホームページ 和文： http://info.isl.ntt.co.jp/camellia/ 英文： http://info.isl.ntt.co.jp/camellia/
問い合わせ先	・〒239-0847 神奈川県横須賀市光の丘 1-1-609A 日本電信電話株式会社　NTT 情報流通プラットフォーム研究所 セキュリティプラットフォームグループ　主任研究員　神田雅透 TEL： 046-859-2437, FAX：046-855-1533, E-MAIL：kanda@isl.ntt.co.jp ・〒104-6212 東京都中央区晴海 1-8-12 オフィスタワーZ13 階 三菱電機株式会社　通信システム事業本部 NTT 事業部　NTT 第一部第一課　課長 富田文隆 TEL:03-6221-2634, FAX:03-6221-2771 E-MAIL: fumitaka.tomita@hq.melco.co.jp

暗号名	CIPHERUNICORN-A
関連情報	公開ホームページ 和文： http://www.hnes.co.jp/products/security/index.html 英文： http://www.hnes.co.jp/products/security/index-e.html
問い合わせ先	〒108-8558 東京都港区芝浦 2-14-22 日本電気株式会社 インターネットソフトウェア事業部 TEL：03-3456-6436, FAX：03-3456-5819, E-MAIL：soft@security.jp.nec.com

暗号名	Hierocrypt-3
関連情報	公開ホームページ 和文： http://www.toshiba.co.jp/rdc/security/hierocrypt/ 英文： http://www.toshiba.co.jp/rdc/security/hierocrypt/
問い合わせ先	〒212-8582 神奈川県川崎市幸区小向東芝町 1 (株) 東芝 研究開発センターコンピュータ・ネットワークラボラトリー 研究主務 秋山浩一郎 TEL：044-549-2156, FAX：044-520-1841 E-MAIL:crypt-info@isl.rdc.toshiba.co.jp

暗号名	SC2000
関連情報	公開ホームページ 和文： http://www.labs.fujitsu.com/techinfo/crypto/sc2000/ 英文： http://www.labs.fujitsu.com/en/techinfo/crypto/sc2000/
問い合わせ先	富士通株式会社 電子政府推奨暗号 問合わせ窓口 E-MAIL：crypto-ml@ml.soft.fujitsu.com

暗号名	MUGI
関連情報	公開ホームページ 和文： http://www.sdl.hitachi.co.jp/crypto/mugi/ 英文： http://www.sdl.hitachi.co.jp/crypto/mugi/index-e.html
問い合わせ先	〒244-8555 神奈川県横浜市戸塚区戸塚町 5030 番地 (株) 日立製作所 ソフトウェア事業部 システム管理ネットワーク管理ソフト設計部 部長 松永和男 TEL： 045-866-8111, FAX： 045-865-9010 E-MAIL： matsun_k@itg.hitachi.co.jp

暗号名	MULTI-S01
関連情報	公開ホームページ 和文： http://www.sdl.hitachi.co.jp/crypto/s01/index-j.html 英文： http://www.sdl.hitachi.co.jp/crypto/s01/index.html
問い合わせ先	〒244-8555 神奈川県横浜市戸塚区戸塚町 5030 番地 (株) 日立製作所 ソフトウェア事業部システム管理ネットワーク管理ソフト設計部 部長 松永和男 TEL： 045-866-8111, FAX： 045-865-9010 E-MAIL： matsun_k@itg.hitachi.co.jp

暗号名	RC4
関連情報	仕様 ・問い合わせ先 RSA セキュリティ社(http://www.rsasecurity.co.jp/) ・仕様 RC4 のアルゴリズムについては、RSA Laboratories が発行した CryptoBytes 誌(Volume5, No.2, Summer/Fall 2002) に掲載された次の論文に記載されているもの。Fluhrer, Scott, Itsik Mantin, and Adi Shamir, "Attacks On RC4 and WEP", CryptoBytes, Volume 5, No.2,Summer/Fall 2002 ・参照 URL <http://www.rsasecurity.com/rsalabs/cryptobytes/index.html>

１．３　ハッシュ関数

暗号名	RIPEMD-160
関連情報	仕様 ・参照 URL <http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html>

暗号名	SHA-1, SHA-256, SHA-384, SHA-512
関連情報	仕様 ・FIPS PUB 186-2, Secure Hash Standard (SHS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkhash.html>

１．４　擬似乱数生成系

暗号名	PRNG in ANSI
関連情報	仕様 ・ANSI X9.42-2001, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography ・参照 URL <http://www.x9.org/> なお、同規格書は日本規格協会(http://www.jsa.or.jp/) から入手可能である。

暗号名	PRNG in ANSI X9.62-1998 Annex A.4
関連情報	仕様 ・ANSI X9.62-1998, Public Key Cryptography for The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) ・参照 URL <http://www.x9.org/> なお、同規格書は日本規格協会(http://www.jsa.or.jp/) から入手可能である。

暗号名	PRNG in ANSI X9.63-2001 Annex A.4
関連情報	仕様 ・ANSI X9.63-2001, Public Key Cryptography for The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography ・参照 URL <http://www.x9.org/> なお、同規格書は日本規格協会 (http://www.jsa.or.jp/) から入手可能である。

暗号名	PRNG for DSA in FIPS PUB 186-2 Appendix 3
関連情報	仕様 ・FIPS PUB 186-2, Digital Signature Standard (DSS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkrng.html>

暗号名	PRNG for general purpose in FIPS PUB 186-2 (+ change notice 1) Appendix 3.1
関連情報	仕様 ・FIPS PUB 186-2, Digital Signature Standard (DSS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkrng.html>

暗号名	PRNG in FIPS PUB 186-2 (+ change notice 1) revised Appendix 3.1/3.2
関連情報	仕様 ・FIPS PUB 186-2, Digital Signature Standard (DSS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkrng.html>