CRYPTREC Report 2004

平成 17 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

「暗号技術監視委員会報告」

目次

はじめに

現在のCRYPTREC活動は2003年度に発足された「暗号技術監視委員会」と「暗号モジュール委員会」を中心に行われている。両委員会とも総務省及び経済産業省が主催している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、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2004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。

しかし，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って、その安全性が損なわれることがあるため、暗号技術に係わる研究開発動向の監視が必要である。この監視活動を担うために2003年度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、関係団体のＷｅｂサイト等から、電子政府推奨暗号の安全性に影響を与えかねない情報を収集し、分析するための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、独立行政法人情報通信研究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。

昨年（2003年）度は“監視活動元年”であり、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を開始した。今年（2004）度は、引き続き監視活動及び関連調査活動等を実施している。その中で、2004年8月のハッシュ関数SHA-0、SHA-1に対する衝突（collision）発見方法についての学会発表は、暗号の安全性に係わる注目すべき事項であった。SHA-1は積極的には推奨してはいないものの電子政府推奨暗号リストに掲載されており、監視活動の一環として調査を実施することとした。

電子政府推奨暗号の監視は、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、この活動は、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ことを改めて強調しておきたい。

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。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独立行政法人情報通信研究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://cryptrec.nict.go.jp/

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。

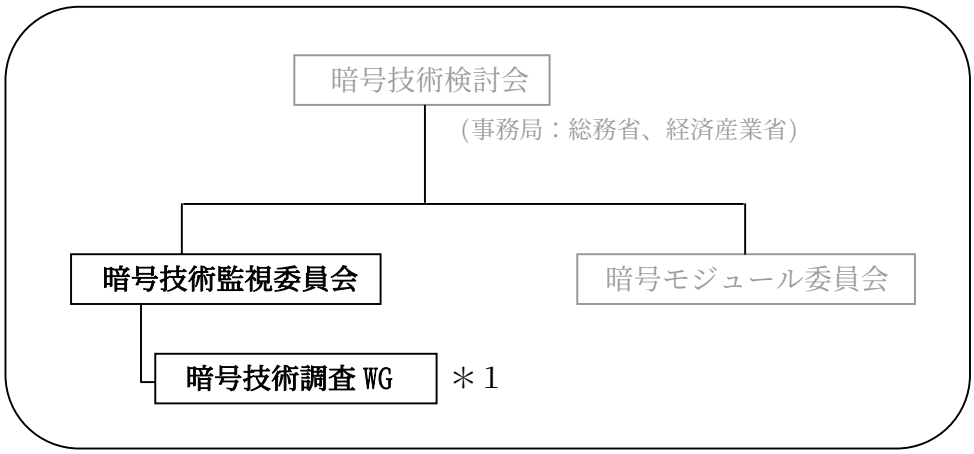
【問合せ先】　cryptrec@ml.nict.go.jp　または　cryptrec@ipa.go.jp

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、独立行政法人情報通信研究機構（NICT）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 NICT 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、NICT 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、NICT 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：廣瀬勝一、川村信一、古屋聡一、盛合志帆

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、廣瀬勝一、栃窪孝也

図１　CRYPTREC 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	情報セキュリティ大学院大学　学長
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	独立行政法人情報通信研究機構 研究員
委員	山村 明弘	独立行政法人情報通信研究機構 グループリーダ
委員	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	情報セキュリティ大学院大学 教授
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 主席研究員
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 主幹技師
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 室長
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	大森 基司	松下電器産業株式会社 チームリーダ
委員	角尾 幸保	日本電気株式会社 主席研究員
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

委員　　廣瀬 勝一　　京都大学 大学院 講師
委員　　盛合 志帆　　株式会社ｿﾆｰ･ｺﾝﾋﾟｭｰﾀｴﾝﾀﾃｲﾝﾒﾝﾄ ﾘｻｰﾁｻｲｴﾝﾃｨｽﾄ

オブザーバー

奥　隆行　　警察庁 情報通信局(2004 年 5 月まで)
森實 克　　警察庁 情報通信局
富田 哲　　防衛庁 長官官房(2004 年 4 月まで)
山城 瑞樹　　防衛庁 長官官房
一條 靖彦　　防衛庁 陸上幕僚監部(2004 年 7 月まで)
加納 信生　　防衛庁 陸上幕僚監部
竹之内 修　　総務省 行政管理局
山本 寛繁　　総務省 行政管理局
野崎 雅稔　　総務省 情報通信政策局
榎本 淳一　　総務省 情報通信政策局
黒田 崇　　総務省 情報通信政策局
石川 雅一　　外務省 大臣官房
小谷 光弘　　経済産業省 産業技術環境局
北浦 康弘　　経済産業省 商務情報政策局(2004 年 7 月まで)
南 英生　　経済産業省 商務情報政策局(2004 年 7 月まで)
松井 洋二　　経済産業省 商務情報政策局
柳原 聡子　　経済産業省 商務情報政策局
滝澤 修　　独立行政法人情報通信研究機構
大蒔 和仁　　独立行政法人産業技術総合研究所

事務局

独立行政法人情報通信研究機構

大久保明、鳥居秀行（2004 年 7 月まで)、曽根裕、天野滋、高橋靖典、
半澤則之（2004 年 10 月まで)、太田将史

・監視要員

山村明弘、田中秀磨

独立行政法人情報処理推進機構

早貸淳子、西原正人、網島和博、山岸篤弘、大熊建司

・監視要員

大塚玲、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。また、2003年8月には、e-Japan重点計画-2003、2004年6月には、e-Japan重点計画-2004と計画の進展にともなってより具体的な施策が示されている。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可能な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推奨暗号の安全性を把握し、もし電子政府推奨暗号の安全性に問題点を有する疑いが

生じた場合には緊急性に応じて必要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推奨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、将来の電子政府推奨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 電子政府推奨暗号リスト

2000年度から2002年度の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（案）」は、2002年に暗号技術検討会に提出され、同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）」において、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとされた。電子政府推奨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、次のＵＲＬから入手できる。

http://cryptrec.nict.go.jp/PDF/c02_report.pdf

1.4 活動の方針

電子政府推奨暗号リスト掲載の暗号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電子政府推奨暗号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、将来の電子政府推奨暗号リストの改正を考慮して、電子政府推奨暗号に関する調査・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NICT及びIPAに監視要員を配置している。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、電子政府推奨暗号の安全性に問題を有する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る。監視要員は情報を参考にして分析を行い、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

NICT および IPA に配置した監視要員を中心に、国内外の研究論文誌、インターネット上に公開されている論文情報や研究集会における情報、電子出版物等を収集したほか、主要な学術国際会議等にも参加し、電子政府推奨暗号リストに掲載されている暗号の安全性に影響を与える研究動向について網羅的に情報収集を実施した。

その結果、2004 年度は特にハッシュ関数について重要な進展が確認され、追加的な情報分析を必要としたが、特に電子政府推奨暗号リストに掲載されている暗号について「審議及び決定」を必要とするような状況には至らなかった。

また、2004年度は2003年度に引き続き擬似乱数生成系調査ワーキンググループと暗号利用モード調査ワーキンググループの2つ調査ワーキンググループを設置した。特に暗号利用モード調査ワーキンググループにおいては、テーマの関連性が高いことなどを考慮し、緊急性の高いハッシュ関数に関する暗号解析技術の動向調査を優先的に実施した。各ワーキンググループの活動概要についてはそれぞれの節で述べる。

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。

・擬似乱数生成系の検定法
・ハッシュ関数
・代数的攻撃法

擬似乱数生成系の検定法、ハッシュ関数の詳細については、それぞれ擬似乱数生成系調査ワーキンググループと暗号利用モード調査ワーキンググループの活動報告を参照して欲しい。代数的攻撃法については、昨年度から特にストリーム暗号や多変数多項式に基づく公開鍵暗号に対する攻撃法として重要な結果が報告されていたため重要な検討課題として来たが、今年度になって代数的攻撃法の限界に関する論文がいくつか出てきており、代数的攻撃に対して我々がこれまで抱いていた危惧のいくつかは既に払拭されたと考えている。

2.1.3 国際学会等参加記録

2004 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
ISO/IEC	ISO/IEC JTC 1/SC 27/WG 2	Singapore	2004/4/19 ～ 2004/4/27
EUROCRYPT 2004	Eurocrypt	Interlaken, Switzerland	2004/5/2 ～ 2004/5/6
AES 4[*1]	Advanced Encryption Standard (AES – State of the Crypto Analysis)	Bonn, Germany	2004/5/9 ～ 2004/5/12
YACC 2004[*2]	Yet Another Conference on Cryptography	Porquerolles Island, France	2004/6/1 ～ 2004/6/5
SAC 2004	Selected Areas in Cryptography	Waterloo, Ontario Canada	2004/8/9 ～ 2004/8/10
CHES 2004	Workshop on Cryptographic Hardware and Embedded Systems	Boston USA	2004/8/11 ～ 2004/8/13
CRYPTO 2004	Crypto	Santa Barbara United States	2004/8/16 ～ 2004/8/19
SASC	The State of Art Stream Ciphers*3	Brugge Belgium	2004/10/14～ 2004/10/15
ISO/IEC	ISO/IEC JTC 1/SC 27/WG 2	Fortaleza Brazil	2004/10/18 ～ 2004/10/22
ASIACRYPT 2004	Asiacrypt	Jeju Island Korea	2004/12/5 ～ 2004/12/9
PKC 2005	International Workshop on Theory and Practice in Public Key Cryptography	Les Diablerets Switzerland	2005/1/23 ～ 2005/1/26
TCC 2005	Theory of Cryptography Conference	Cambridge, MA USA	2005/2/10 ～ 2005/2/12
FSE 2005	Fast Software Encryption	Paris France	2005/2/21 ～ 2005/2/23
SHARCS[*4]	Special-purpose Hardware for Attacking Cryptographic Systems	Paris France	2005/2/24 ～ 2005/2/25

*1 **AES4:** 共通鍵暗号の安全性評価に関連する国際会議である。1998 年から 2000 年にかけて AES1、AES2、AES3 が開催されたが、2001 年に AES が FIPS197 として選定された後はしばらく開催されていなかった。今回は 4 年ぶりの開催になる。

*2 **YACC 2004:** フランスの研究者中心の国際会議である。Meier の EUROCRYPT 2004 での代数的攻撃法の改良法についての詳細な発表や、Courtois による AES を対象にした代数的攻撃法に関する報告があった。

*3 **SASC** - The State of the Art of Stream Ciphers は、EU のセキュリティについてのプロジェクトである ECYRYPT が主催するストリーム暗号の安全性評価と設計法に関する会議である。

*4 **SHARCS:** EU のセキュリティについてのプロジェクトである ECYRYPT が主催する暗号解読専用ハードウェアに関する会議である。

2.1.3.1 公開鍵暗号

１)守秘目的の公開鍵暗号アルゴリズムに関連する報告

公開鍵暗号の解読技術については、今回の範囲では**電子政府推奨暗号の安全性に影響を与える報告はない**が、実装に対する解読技術については Eurocrypt 2004 において報告が 2 件あった。一つは Naccache らによる楕円曲線に基づく署名方式において、楕円曲線上の点の表現方法によっては秘密鍵に関する情報が漏れることがあるという報告である。もう一つは、GNU Privacy Guard（GPG）と呼ばれるオープンソースプログラムの実装レベルでの脆弱性に関する報告である。

また、CRYPTO 2004 において、ドイツの Alexander May が RSA 秘密鍵を求める問題と素因数分解問題が決定的多項式時間で相互に帰着可能であることを示した他、NTT の青木らが数体ふるい法を Pentium 等の汎用 CPU に実装する際にキャッシュミスを減らすことで計算効率を高める手法を提案している。

さらに、PKC 2005 においてオーストラリアの Steinfeld-Contini-Wang-Pieprzyk らは RSA 暗号に対する Wiener 攻撃法の限界について報告した。RSA に対する Wiener 攻撃法は、公開鍵(e,N)が与えられた時に、$d < N^{1/4}$であれば効率的にdを求めることができるというものである。Steinfeld らは$d = N^{1/4+\rho}$かつ$\rho > 0$ の場合には、Wiener 攻撃法の成功確率が無視できるほど小さくなり、Wiener Search Variant 法(Verheul-Van Tilborg1997、Dujella04)でも圧倒的確率で指数時間アルゴリズムになることが示されている。（準指数時間の数体ふるい法がより効率的）Boneh-Durfee00 の Lattice を用いた手法の発見的な方法のバウンド$d < N^{0.292}$についての安全性は未解決問題としている。今回の報告は RSA 暗号において秘密鍵dを$d > N^{1/4}$のようにとった時の安全性を肯定する結果である。従って、$d < N^{1/4}$であれば効率的にdを求めることができるので、CRYPTREC Report 2002 で指摘した通り、今回の結果を加味しても、計算の高速化を理由に秘密鍵dを小さな値に制限することはすべきでない。

また、国際会議 SHARCS において、素因数分解を解く専用ハードウェアがいくつか報告された。1024bit の RSA 鍵を解読するために必要なコストの見積もりは 2003 年度報告書で述べた内容と変化していない。新しく SHARK と呼ばれる素因数分解に特化したハードウェアが提案されたが、SHARK は現実的な ASIC 技術を前提にし、1024bit の RSA 鍵の解読に必要なコストは多く見ても$200M との見積もりを報告している。WSI 技術を前提とする TWIRL の$1.1M よりは大きいが、現実的な見積もりとして注目する必要がある。

２)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。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。**

また、DSA 署名のスマートカード実装に対して、フランスの Naccache-Nguyen-Tunstall-Whelan らは電気的刺激を加えることにより、署名鍵を実際に求める(公開されているものとしては最初の)実験を PKC 2005 において報告した。DSA 署名アルゴリズムで使用する乱数 k の値を電気的刺激で制御することによって、k の最上位バイトを実際に 0 に制御し、署名を計算させることによって、出力された署名に対して Howgrave-Graham Smart の Lattice を用いた攻撃法を適用して署名鍵を求めている。この結果はスマートカード上に実装された DSA に対する攻撃であり、DSA アルゴリズムそのものの安全性に影響はない。

2.1.3.2 共通鍵暗号

１)ブロック暗号に関連する報告

電子政府推奨暗号リストに掲載されているブロック暗号の安全性に影響を与える報告はなかった。

今年度に報告された比較的重要度の高い研究成果には以下のようなものがある。まず、ブロック暗号に対する攻撃法として、CRYPTO 2004 において Biryukov らによる線形解読法の拡張として複数の線形近似をセットとして考えるマルティプルリニアー解読法と Courtois による Bilinear 解読法が提案された。

マルチプルリニアー解読法は従来から提案されていたが、Biryukov らはこの解読法を DES に適用し、線形解読法に比べて解読効率が有意の差で向上したと主張している。

Courtois の提案する Bilinear 解読法は、従来の線形解読法では 1 次式で近似していたものを、Bilinear 関数と呼ばれる特殊な形をした 2 次式による近似に拡張して解読するというもので、特殊な例では解読効率が飛躍的に向上すると主張している。

また、代数的攻撃(algebraic attack)を中心に重要な報告がいくつかなされており、以下に状況を整理する。

現在までのところ下記の４つの algebraic attack が提案されている。

a) XL attack：

[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。

b) XSL attack：
c) F4, F5 を用いた algebraic cryptanalysis：
d) ストリーム暗号に対する algebraic attack：

a) **XL attack** は c)に帰着され、かつ漸近的にも c)よりも強いアタックではありえないことが杉田らの ASIACRYPT 2004、 AES4 の Faugere、YACC2004 の Ars により示されている。
b) **XSL attack** についてはその核心部分である T’method が、実はグレブナー基底アルゴリズムの一部であり、この方法によって解読可能性が飛躍的に高まることはあり得ないことが杉田らの eprint により示されている。また YACC2004 で Courtois 氏がこの事実を認める発言をしていることから、現段階で XSL attack が AES の解読につながることは無いと考えられる。
c) **F4, F5 を用いた algebraic cryptanalysis** では HFE が解読可能であることは実証されており、現段階では最強の algebraic attack であると言える。しかし、AES4 での Faugere 氏による漸近的な解析によって overdefinedness、sparcity の両面から見てもこの方法では AES の解読には至らないことが報告されている。
d) **ストリーム暗号に対する algebraic attack** については理論的には問題は無く、c)の方法を用いることによってさらに改良できる可能性があるものの、適用対象が filtering generator 等の限られたクラスのストリーム暗号であることから電子政府推奨暗号への影響は現段階では無いと考えられる。

2)ストリーム暗号に関連する報告

ストリーム暗号に対する代数的攻撃(Algebraic attack)はフランスの Courtois らにより提案され、解読に必要な計算量の見積もりが与えられていた。

CRYPTO 2004 において Hawks と Rose は、Courtois らの見積もりでは代入計算の部分の計算量を過小評価しており、正しい評価でははるか大きい演算量が必要であることを示した。さらに、離散フーリエ変換を利用することによりこの演算量を大幅に減らすことが可能であり、依然として強力な解読法であるとも主張している。

ASIACRYPT 2004 において、ドイツエッセン大の Diem が、Shamir らが提案する代数的攻撃の一種（XL 攻撃）の漸近的な挙動を理論的に解析した。また、東大の今井、IPA の杉田、フランスの Faugere らは、XL 攻撃が実はグレブナー基底アルゴリズムに他ならないことを示し、Faugere 氏によって提案されていた従来最速とされるグレブナー基底アルゴリズム F4、F5 よりも速度が大幅に劣ることを示すなど、代数的攻撃の限界についての報告があった。

ストリーム暗号に対するその他の結果として、Vaudenay らのグループが CRYPTO 2004 および ASIACRYPT 2004 において、Bluetooth で使用されているストリーム暗号 E0 に対して Fast Correlation Attack を適用し、Courtois らの評価よりも高速な解読が可能であることを示している。

ただし、現在までに示されている代数的攻撃法は LFSR に基づく filtering generator 等のストリーム暗号に対する攻撃法であり、**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これらとは構造的に異なる方式のため、安全性に関して直接的な影響はない**と考えられる。

また、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 MUGI について、いくつかの研究報告があった。Biryukov と Shamir は FSE 2005 において、非線形部分を変形した MUGI の変形版についての解析結果を示した。彼らの解析では、オリジナルの MUGI の安全性上の問題は見つかっていない。関根・金子ら[2]は、Truncate 線形確率評価で最大線形特性確率の上界が 2^{-138} 以下となり、Coppersmith の乱数識別攻撃に対し MUGI が安全であることを示した。さらに、野坂・金子ら[3]は Truncate 線形解析で、再同期攻撃に対する耐性評価を試みている。結果として、最大線形特性確率の上界として 2^{-96} を得たと報告している。この値は、安全性基準 2^{-128} は満足していないが、truncate 評価であることから MUGI の安全性を直ちに脅かすものではないが、さらなる検討が必要である。

2.1.3.3 その他（ハッシュ関数）

CRYPTO 2004 において、フランスの Joux がハッシュ関数 SHA-0 の衝突を発見したほか、中国の Wang がハッシュ関数 MD4,MD5, HAVAL-128, RIPEMD の衝突をそれぞれ発見したと報告した。電子政府推奨暗号リストに掲載されている SHA-1 についても、イスラエル工科大学の Biham が SHA-1 の 80 段の圧縮関数を 36 段に減らした版についての近衝突を発見したことを SAC2004 および CRYPTO 2004 で報告したほか、2005 年 2 月には Wang が、インターネットに論文(Collision search attacks on SHA1[4])を公開し、2^{69} 回程度の SHA-1 の計算で衝突が見つかるという見積もりを示した。また、ASIACRYPT 2004 において、フランス DCSSI の Muller より、ハッシュ関数 MD2 の一方向性を否定する理論的結果が出された。Muller の今回の結果は 2^{104} の複雑度で MD2 の逆像を求められることを示すものである。ただし、MD2 は RSA 社が提案する民間標準 PKCS#1 v2.1 において旧システムとの整合

[2] H.Sekine,T.Nosaka,Y.Hatano,M.Takeda and T.Kaneko:" A Strength Evaluation of a Pseudorandom Number Generator MUGI against Linear Cryptanalysis", IEICE Trans. Vol.E88-A, No.1, pp.16-24 Jan.2005

[3] 野坂哲朗、渡辺大、金子敏信："MUGI の再同期攻撃に対する耐性評価"、SCIS2005、pp.1933-1936、Jan.2005

[4] http://theory.csail.mit.edu/~yiqun/shanote.pdf から入手可能

性が求められる場合にのみ使用が認められており、電子政府推奨暗号や ISO 標準等には含まれていない。その他、電子政府推奨暗号リストに掲載されている SHA-384/SHA-512 についても、これらのハッシュ関数の別原像探索攻撃に対する安全性について疑問を提示する論文がインターネット上で公開されている。ただし、現段階では学術的に信頼できる内容か否かの確認が取れていない。

ハッシュ関数は衝突を発見できないことが重要な安全性の条件であり、ハッシュ関数 SHA-0, MD4, MD5, HAVAL-128, RIPEMD はこの条件を満たしていない。また、Wang らは SHA-1 の衝突困難性について述べた論文を発表しているが、速報であり、詳細な情報が入手できていないため、監視委員会としての判断を得るには至っていない。今後の SHA-1 の解読技術の進展には特に注意する必要がある。また、NIST は SHA-1 の利用を 2010 年までに止め、より安全なハッシュ関数（SHA-224, SHA-256, SHA-384, SHA-512）への移行を推奨する旨のコメントを発表している。

2004 年 8 月にハッシュ関数 SHA-0, MD4, MD5, HAVAL-128, RIPEMD の衝突が相次いで発見されたことを受けて、これらの報告を精査し、2004 年 9 月 8 日付で総務省、経済産業省、NICT、IPA の Web サイトにハッシュ関数の安全性に関するアナウンス（CRYPTREC 見解[5]）を掲載した。また、ハッシュ関数の安全性に関しては調査ワーキンググループで継続調査を実施している。以下に、SAC2004 および CRYPTO 2004 での報告から、アナウンス迄の経過とアナウンスした CRYPTREC 見解を示す。

［検討の経過］

ａ）H16 年 8 月 9 日　SAC2004 の招待講演 1 で Biham がハッシュ関数（SHA-0）の近衝突を発見したと報告した。（New Results on *SHA-0* and *SHA-1*）なお SHA-1 に関しては 80 段のフルスペック版に対する衝突ではなく、36 段に処理段数を減らした縮小版に対する衝突が報告された。

H16 年 8 月 17 日　CRYPTO 2004 のランプセッションで Joux がハッシュ関数（SHA-0）の衝突を発見したと報告し、Wang が複数のハッシュ関数（MD4, MD5, HAVAL-128, RIPEMD）の衝突を発見したと報告した。

ｂ）H16 年 8 月 27 日　事務局会議開催（総務省、経済産業省、ＮＩＣＴ、ＩＰＡ）

・電子政府推奨暗号に安全性の問題が発生していない事が確認された。

・暗号技術検討会、暗号技術監視委員会の招集は見送ることとした。

[5] SHA-1 については 2.1.3.3 節で述べたように、2005 年 2 月になって Wang らにより少ない計算量（2^{69}）で衝突を発見できるとの速報が公開されている。本報告書を作成した 2005 年 3 月時点では詳細が入手できていないため、監視委員会としての判断を得るには至っていない。

・専門外の人々に誤った情報を与えることを防ぐためにCRYPTRECとしての見解をＷｅｂで示す事にした。

ｃ）H16年8月31日　CRYPTREC見解（案）の作成

ｄ）H16年9月6日　暗号技術監視委員会メーリングリスト審議

ｅ）H16年9月8日　ＷｅｂサイトにCRYPTREC見解を掲載

［CRYPTREC見解］

ハッシュ関数SHA-1及びRIPEMD-160の安全性について

平成16年9月8日

CRYPTREC暗号技術監視委員会

ハッシュ関数SHA-0、RIPEMD、MD4、MD5及びHAVAL-128の衝突が発見されたことが学会（CRYPTO 2004）で報告され、一部報道等で大きく取り上げられました。電子政府推奨暗号リストにはハッシュ関数SHA-1およびRIPEMD-160が掲載されていますが、今回衝突が発見されたハッシュ関数とは構造が異なっており、現時点までに公表されている解析技術を適用して衝突を発見するには極めて大きな技術的ギャップが存在すると考えられます。従って、冒頭に述べた学会での報告によって、電子政府推奨暗号リストに掲載されているハッシュ関数の安全性に特段の変化は生じていないと考えています。

また、電子政府推奨暗号リストの注釈にあるように、CRYPTRECとしてはハッシュ値が256ビット以上とより長い方式の利用を薦めており、この方針を維持・強化することが望ましいと考えています。

いずれにせよ、研究の進展は予断を許さないため、引き続き注意深く監視活動を続けていきます。

ご意見・コメントなどの問い合わせがございましたら、下記までお願いいたします。

CRYPTREC暗号技術監視委員会事務局

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	平成１６年6月２４日	活動方針案の説明・審議、監視状況報告
第２回	平成１７年2月１５日	監視状況報告、WG活動報告、報告書案の説明・審議

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	平成１６年8月2日	第１回擬似乱数生成系調査WG
第２回	平成１６年8月5日	第１回暗号利用モード調査WG
第３回	平成１６年１０月7日	第２回暗号利用モード調査WG
第４回	平成１６年１２月２４日	第２回擬似乱数生成系調査WG
第５回	平成１７年1月１３日	第３回暗号利用モード調査WG
第６回	平成１７年2月8日	第４回暗号利用モード調査WG

2.2 暗号技術調査ワーキンググループ

2.2.1 擬似乱数生成系の調査

2.2.1.1 調査背景

電子政府推奨暗号リストにおける擬似乱数系では、SHA-1 を使った擬似乱数生成器が例示されている。しかし、用途によっては、例示された擬似乱数生成器以外でも、暗号学的に安全性が確認できれば、用途によっては利用できる場合もある。そこで電子政府で使用される擬似乱数生成器が、少なくとも高い乱数性を持つことを検証するためのツールが必要と考えられている。

また、乱数の検定法には様々な観点からの検定法が存在しており，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。しかし、これらの検定ツールを比較検討すると、

1) 検定ツールごと採用されている検定法が異なり、検定法の選択基準が明確になっていない
2) 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

など問題点が存在する。特に、NIST FIPS PUB 140-2 と NIST SP800-22 には、いくつかの検定法に不具合があることを指摘した学術論文があり、さらに、2002 年度版暗号技術評価報告書においても同様の指摘がなされている。

他方、暗号モジュール委員会で検討中の暗号モジュール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、擬似乱数生成系調査ワーキンググループで、CRYPTREC としての乱数検定ミニマムセットの策定を目標に、擬似乱数生成系の調査および検定法の調査を行っている。

2003 年度の調査の結果、CRYPTREC の乱数検定ミニマムセット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、計算機実験が行なえる程度の実際的な追試を行い、閾値等の設定値が適切かどうかの確認が必要であるとの判断となった。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、2004 年度以降は調査の範囲を絞ることも課題となった。その結果、2004 年度以降の活動方針を以下のように定めた。

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

2.2.1.2　2004 年度活動内容

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：森井　昌克　徳島大学工学部　教授
委員：廣瀬　勝一　京都大学大学院情報学研究科通信情報システム専攻　講師
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

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。

第１回　　平成１６年８月２日
第２回　　平成１６年１２月２４日

技術的な議論は主にメーリングリストを通じて行った。

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

2004 年度としては、以下の活動を行なった。

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

特に，1)の検定方法に関しては、離散フーリエ変換検定するための数学理論を構築するた

めの予備調査と 2003 年度未解決であった分散値の理論的確認と、擬似乱数生成系に対する各種検定方式の理論的根拠の確認及び計算機実験による検証を実施した。

4)調査概要

調査課題Ⅰ:「離散フーリエ変換検定について」

2003 年度の調査に依れば、以下の問題点が指摘された。

問題点（1）:閾値 T の値は概算である。

問題点（2）:分散値の設定に問題がある。

この問題点を解決する目的で、以下の調査を行った。

1） 擬似乱数列を離散フーリエ変換(DFT)検定するための数学理論を構築するための予備調査。

2） 予備調査の結果に基づき、離散フーリエ変換(DFT)検定における、分散σに関する理論的な検討。

調査課題Ⅱ:「擬似乱数生成系の各検定方式の理論的根拠の確認及び計算機実験による検証について」

（1） CRYPTREC の公開している「擬似乱数生成系の検定方法に関する調査報告書」[6]の「NIST SP800-22 の検定法」に示されている検定法を中心に、「DIEHARD の検定法」に示されている検定法も含めて、わが国における「擬似乱数検定法」として必要最低限の検定方法を定める。また、独立行政法人情報処理推進機構が 2002 年度に作成した「擬似乱数検証ツール」[7]の検定方法の妥当性の検証を含める。

（2） 必要最小限の検定方法のうち、理論的根拠を確認する。なお、理論的な根拠が明白でないものがあれば、理論的な根拠の研究動向を調査する。また、理論的解析へのアプローチの方法について検討する。

（3） CRYPTREC 乱数生成ミニマムセットの案を検討する。

上記の 2 件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することとした。

2.2.1.3 まとめ

現段階での調査結果は、以下のとおりである。

調査 1)「離散フーリエ変換(DFT)検定について」

---

6 http://cryptrec.nict.go.jp/PDF/wat-rep2003/rep_ID0207.pdf

7 http://www.ipa.go.jp/security/fy14/crypto/pseudo_rundum/test-tool.html

NIST の SP 800-22[8]における離散フーリエ変換(DFT)検定における乱数性の検定は、次の手順で行われる。

1．長さｎの２値乱数列を$\{-1,1\}$系列$X=(X_0,X_1,...,X_{n-1})$とし、離散フーリエ変換（DFT）を行い周波数スペクトル$(S_0,S_1,...,S_{n-1})$を求める

2．周波数スペクトルの絶対値の２乗$|S_j|^2$ $(j=0,1,\cdots m)$ $m=\left\lfloor\frac{n}{2}\right\rfloor-1$を、その 95%点で２値化し$Z_j$とする。

3．Z_j $(j=0,1,\cdots,m)$が確率$p=0.95$の二項分布に従っているか否か検定する。

離散フーリエ変換(DFT)検定は、周波数スペクトルで見ても、各係数が一様乱数で有ることを確認するものである。NIST の理論説明文書では、理想乱数であれば、次が成り立つと仮定している。

仮定１．$|S_j|^2$はχ^2分布をし、その 95%点の閾値は$T=\sqrt{3n}$である。

仮定２．Z_j $(j=0,1,\cdots,m)$は、独立な変数であり、確率$p=0.95$の二項分布であり、平均$E\{Z\}=mp$、分散$V(Z)=mp(1-p)$となる。

本ＷＧにおける、理論考察及び学会等発表文献調査により、以下が明らかとなった。

1．$|S_j|^2$の分布はχ^2分布で近似でき、その９５%点を、正確に計算するならば閾値は$T=\sqrt{-(\ln 0.05)n}\approx 1.73082\sqrt{n}$である[9]。

2．{-1,1}に制限された波形の為、周波数スペクトルの実部（cos 成分）と虚部（sin 成分）が独立では無く、系列長 n が小さいと$|S_j|^2$の分布をχ^2分布で近似する根拠が失

[8] http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf

[9] K. Hamano, The distribution of the spectrum for the discrete Fourier transform test included in SP800-22, IEICE Trans. Fundamentals, vol. E88-A, no. 1, pp. 67–73, 2005.

われる。nが大きいときは、χ^2分布と見なして良い。[10]

3．95%閾値$T=\sqrt{-(\ln 0.05)n}$の場合、実験値では、Z_jの分散は、$\sigma^2{}_{\exp}\approx\frac{mp(1-p)}{2}$となり、$Z_j$の独立性に、疑問がある。理由として、乱数波形が{-1,1}に制限されている為、パーセバルの定理より$\sum_{j=0}^{n-1}|S_j|^2=n^2$のエネルギー制限が課せられ$Z_j\ (j=0,1,\cdots,m)$の独立性が失われることも挙げられる。閾値を 0%～100%に変えて、同様の実験を行うと、分散の実験値は、理論値に近づく。これは、エネルギー制限で定性的に説明が可能である。[11]

4．エネルギー制限の影響を回避する為、Z_jの一部$(j=0,1,\cdots,M)$、$M<m$を使用し同様の検定を行うと分散の実験値が理論値に近づく事が観測される。[6]

5．素数のnに対し、$Z_j\ (j=0,1,\cdots,m)$の従属性の定量的評価もある。[4]

以上の様な事実は明らかとなったが、NISTの仮定2に代わる理論分散を解析するには至っていない。理論で明確に示された乱数検定法のみが適切と判断するならば、NISTの離散フーリエ変換(DFT)検定は不適切である。

調査 2) 「擬似乱数生成系の各検定方式の理論的根拠の確認及び計算機実験による検証について」

SP 800-22 の 16 種類の検定法に対し、その背景の理論的分布と、実際の試験値の分布を実験的に比較し、検定法の理論的根拠の妥当性を調査した。調査方法としては、理想的乱数源として Generator-Using SHA-1 を仮定し、理論的に想定される統計量の分布と、計算機実験によって得られた結果の分布を比較し、その検定法の妥当性を調査した[12]。パラメータの設定範囲は、SP800-22 で推奨されている値である。実験地が理論分布に合致しているかの判断は、分布曲線を比較し定性的におこなった。定性的な比較とした理由は以下である。

- 仮想的な理想乱数源として Generator-Using SHA-1 を仮定していること。

---

10 広瀬勝一：“擬似乱数生成系の検定方法に関する調査報告書”
http://cryptrec.nict.go.jp/PDF/wat_rep2004/rep_ID0202.pdf

11 山本尚史, 金子敏信, NIST SP800-22 の DFT 検定に関する一考察, 信学技法, ISEC2004-50,pp. 61–64, 2004.

12 金子敏信：“擬似乱数生成系の検定方法に関する調査報告書”
http://cryptrec.nict.go.jp/PDF/wat_rep2004/rep_ID0201.pdf

- 実験分布と理論分布の一致性を合否検定すると、合格閾値の設定により細部の不一致が見過ごされる危険があること

今回行った実験結果として、離散フーリエ変換(DFT)検定、Lempel-Ziv 圧縮検定では、理論分布と試験値の分布に大きな違いあること。近似エントロピー検定において、推奨パラメータの一部においては、理論分布からの乖離がみられることがわかった。

現在までに、離散フーリエ変換(DFT)検定、Lempel-Ziv 圧縮検定に関しは、疑問点の指摘が学会で行われている。そこで、これらの問題点が指摘されている検定法と同程度の理論－実験分布曲線の乖離が見られた場合、合致していないと判断するならば、各種検定法の評価は以下である。

なお(3)の CRYPTREC 乱数生成ミニマムセット案については､今年度の調査結果に未だ不十分な点が残されているため、結論を得るに至っていない。

1. 頻度検定	○
2. ブロック単位の頻度検定	○
3. 連検定	○
4. ブロック単位の最長連検定	○
5. 2 値行列ランク検定	○
6. 離散フーリエ変換(DFT)検定	× ※1
7. 重なりの無いテンプレート適合検定	○
8. 重なりのあるテンプレート適合検定	○
9. Maurer の「ユニバーサル統計量」	○
10. Lempel-Ziv 圧縮検定	× ※2
11. 線形複雑度検定	○
12. 系列頻度検定	○
13. 近似エントロピー検定	△ ※3
14. 累積和検定	○
15. ランダム回遊検定	○
16. 変形ランダム回遊検定	○

※1 長い系列長に対し理論分布の補正が必要

※2 有限長系列の分布に関する新たな理論解析

※3 推奨パラメータの設定条件を狭めた方が妥当

2.2.2 ハッシュ関数の安全性調査

2.2.2.1 調査背景

昨年度、暗号利用モード調査ワーキンググループでは、米国を中心とする暗号利用モード標準の見直しの流れのもと、ブロック暗号を用いた暗号利用モードの調査研究に注力した。本年度は、暗号利用モード標準化の動きが一段落したこと、ハッシュ関数の衝突解析に進展があり、現在利用されているハッシュ関数に対して脅威が生じる可能性が出てきたことから、電子政府推奨暗号の監視という観点より、ハッシュ関数の安全性に関する調査を行うこととした。

昨年度の調査においても、メッセージ認証のための利用モード(MAC)に関連して、ハッシュ関数、特に鍵付きハッシュ関数の調査についても議論に上がったが、昨年の段階では技術的に比較的新しく、未成熟な部分が多いため、調査範囲が狭いということで積極的には調査を行わなかった。本年度の調査は、これを補完するという意味づけもある。

ハッシュ関数の構成法として、ブロック暗号に基づくもの(ISO/IEC 10118-2)、専用ハッシュ関数と呼ばれるもの(ISO/IEC 10118-3, FIPS180-2)、剰余演算を用いるもの(ISO/IEC 10118-4)などがあるが、電子政府推奨暗号にも含まれ、解析方法の進展が著しい、専用ハッシュ関数に注力して調査を行った。

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：廣瀬勝一　京都大学大学院情報学研究科通信情報システム専攻　講師
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　室長
委員：古屋聡一　株式会社日立製作所 システム開発研究所　研究員
委員：盛合志帆　株式会社ソニー・コンピュータエンタテインメント
　　開発研究本部　リサーチサイエンティスト

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。

第１回　　平成１６年８月５日
第２回　　平成１６年１０月７日
第３回　　平成１７年１月１３日
第４回　　平成１７年２月８日

2)ワーキンググループの活動目標

暗号利用モード及びハッシュ関数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及びハッシュ関数の選定における判断材料となる資料を提供することを最終的な目標とする。特に今年度は、ハッシュ関数の衝突解析に進展があり、電子政府システム及び世の中で広く利用されているハッシュ関数に対して脅威が生じる可能性が出てきたことから、緊急にハッシュ関数の安全性に関する調査を行い、暗号技術監視委員会に報告することを目標とした。

3)今年度の活動内容

電子政府システム及び世の中で広く利用されている代表的なハッシュ関数について、その技術的特徴と最新の採用・標準化状況を整理し、最新の解析結果を調査してまとめる。

4)調査概要

調査 1)「ハッシュ関数の安全性について」

電子政府推奨暗号及び IETF, ISO/IEC, FIPS 標準として広く利用されている MD4, MD5, RIPEMD-160, SHA-1, SHA-256, SHA-512 などの代表的な専用ハッシュ関数を対象とし、技術的特徴と採用・標準化動向をまとめ、最新の解析結果を踏まえた安全性評価を行った。

この調査結果とワーキンググループ内での議論をもとに、報告書を作成した。

2.2.2.3 まとめ

表 2.2 に示すものを中心に調査を行い、本ワーキンググループの報告書としてまとめた。

表 2.2 調査したハッシュ関数

ハッシュ関数名	メッセージ長 (bit)	ハッシュ長 (bit)	採用されている標準規格等
MD4	上限なし	128	RFC 1320
MD5	上限なし	128	RFC 1321
RIPEMD	上限なし	128	
RIPEMD-128	$< 2^{64}$	128	ISO/IEC 10118-3
RIPEMD-160	$< 2^{64}$	160	電子政府推奨暗号[注)] ISO/IEC 10118-3
SHA(SHA-0)	$< 2^{64}$	160	

SHA-1	＜ 2^{64}	160	電子政府推奨暗号[注)] FIPS 180-2 ISO/IEC 10118-3
SHA-224	＜ 2^{64}	224	FIPS 180-2 (Change Notice 1)
SHA-256	＜ 2^{64}	256	電子政府推奨暗号 NESSIE Portfolio FIPS 180-2 ISO/IEC 10118-3
SHA-384	＜ 2^{128}	384	電子政府推奨暗号 NESSIE Portfolio FIPS 180-2 ISO/IEC 10118-3
SHA-512	＜ 2^{128}	512	電子政府推奨暗号 NESSIE Portfolio FIPS 180-2 ISO/IEC 10118-3
Whirlpool	＜ 2^{256}	512	NESSIE Portfolio ISO/IEC 10118-3

注）電子政府推奨暗号リストにおいて、RIPEMD-160, SHA-1 については「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。」という注釈がついている。

MD4

従来より、約 2^{20} 回の MD4 圧縮関数の計算量で MD4 の衝突が見つけられることが知られていたが[2]、2004 年に Wang ら[7]により、さらに少ない計算量で衝突が見つけられることが発表された。MD4 の安全性は十分でなく、衝突困難性が求められる電子署名などのアプリケーションでの利用は避けるべきと思われる。

MD5

2004 年に Wang ら[7]により、IBM P690 を用いて約 1 時間で衝突が見つけられることが報告された。衝突困難性が求められる電子署名などのアプリケーションでの利用は控えるべきと思われる。

RIPEMD

2004 年に Wang ら[7]により、衝突が見つけられることが発表された。衝突困難性が求められる電子署名などでの利用は控えるべきと思われる。

RIPEMD-128

現在のところ、問題点は見つかっていない。但し、ハッシュ長が 128 ビットであるため、衝突攻撃による攻撃計算量は高々2^{64}であり、長い将来に渡って利用されるアプリケーションには適さない。

RIPEMD-160

現在のところ、問題点は見つかっておらず、安全性上、問題はないと思われる。但し、ハッシュ長が 160 ビットであるため、衝突攻撃による攻撃計算量は高々2^{80}であり、将来に渡って安全であるとは保証できない。

SHA (SHA-0)

2004 年に Joux らにより、SHA-0 の衝突が発見された[5]ほか、Wang らにより、SHA-0 の衝突が約2^{40}回の圧縮関数の計算量で見つけられるとの報告があった[7]。これらにより、衝突困難性が求められる電子署名などのアプリケーションでの利用は控えるべきと思われる。

SHA-1

2004 年に Biham らにより、36 段に短縮した SHA-1 の衝突が発見された他、Rijmen により、53 段に短縮した SHA-1 の衝突が発見された。また、2005 年 2 月中旬になって、Wang らによって2^{69}の計算量によって衝突が発見できるという報告があった。詳細なアルゴリズムがまだ公開されておらず計算量の見積もりが適切か不明であるため、2005 年 3 月現在では判断できない状況である。本攻撃結果のみによって SHA-1 を利用したシステム全てが直ちに危険にさらされるとは考えにくいが、今後の動向に厳重に注意する必要がある。2005 年度は引き続き調査を継続する予定である。

SHA-224/256

Gilbertらによる評価[3]で、SHA-256 を含む全てのSHA-2 ファミリーの衝突を見つけるための、最も確率の高い ”differential collision pattern ”の攻撃計算量が2^{66}であり、SHA-256の攻撃計算量は2^{132}となることから、SHA-256は衝突攻撃に対して耐性をもつという結論が導かれている。Hawkesら[4]により、このdifferential collision pattern ”の確率は、算術加算をオペレータとする差分定義のもとでは、より大きな値となると主張されているが、この解析ではメッセージスケジュール関数の解析は不十分であり、単

純な解析による楽観的な攻撃計算量が導かれているにすぎない。SHA-224及びSHA-256の衝突攻撃に対する安全性を評価するにはより詳細なメッセージスケジュール関数の解析が必要である。現時点では致命的な問題点は見つかっていないが、今後の動向に注意していく必要がある。

SHA-384/512

SHA-256/224と同様の解析がGilbertら[3]及びHawkesら[4]によって報告されているが、現時点では安全性を脅かす問題は見つかっていない。今後の動向に注意していく必要がある。

Whirlpool

現在のところ、問題点は見つかっていないが、2000年に提案されて以来、提案者以外からの安全性評価がされていないため、今後の解析に注意していく必要がある。

参考文献

[1] E. Biham, R. Chen, “New results on SHA-0 and SHA-1”, Short talk presented at CRYPTO’04 Rump Session, 2004.

[2] H. Dobbertin, “Cryptanalysis of MD4” Fast Software Encryption – FSE’96, Lecture Notes in Computer Science Vol.1039, Springer-Verlag, 1996, pp.53-69.

[3] H. Handschuh and H. Gilbert, “Security Analysis of SHA-256 and sisters”, Selected Areas in Cryptography・SAC 2003, Lecture Notes in Computer Science Vol. 3006, Springer-Verlag, pp. 175-193, 2004.

[4] P. Hawkes, M. Paddon, G. G. Rose, “On Corrective Patterns for the SHA-2 Family”, Cryptology ePrint Archive, Report 2004/207.

[5] A. Joux, P. Carribault, C. Lemuet, W. Jalby, “Collision in SHA-0”, sci.crypt, August 12, 2004.

[6] V. Rijmen, E. Oswald, “Update on SHA-1”, Topics in Cryptology – CT-RSA 2005, Lecture Notes in Computer Science, Vol.3376, Springer-Verlag, 2005, pp.58-71.

[7] X. Wang, D. Feng, X. Lai, H. Yu, “Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD”, Cryptology ePrint Archive, Report 2004/199.

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 主任研究員 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 ﾄﾘﾄﾝｽｸｴｱｵﾌｨｽﾀﾜｰ 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 主任研究員 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 ネットワークソフトウェア本部　担当本部長　松永和男 TEL： 045-862-8498, FAX： 045-865-9055 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ネットワークソフトウェア本部　担当本部長　松永和男 TEL：045-862-8498, FAX： 045-865-9055 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>