CRYPTREC Report 2013

平成 26 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

「暗号技術評価委員会報告」

目次

はじめに

本報告書は、総務省及び経済産業省が主催する暗号技術検討会の下に設置された暗号技術評価委員会の 2013 年度活動報告である。

2013 年度の CRYPTREC 活動において、特筆すべきは、暗号技術評価委員会及び暗号技術活用委員会の新体制に移行し活動を開始したことである。CRYPTREC の体制は、2012 年度の「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」の改定に鑑み、我が国の暗号政策に係る中長期的視野に立って、「暗号技術の安全性及び実装評価を中心とした技術的な検討課題」と「セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討課題」に対応するために、2012 年度までの、暗号方式委員会、暗号実装委員会、暗号運用委員会の三委員会体制から、上述の二委員会体制に改組された。

暗号技術評価委員会は、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、2012 年度までの暗号方式委員会の全部及び暗号実装委員会の一部からの課題を引き継いで、暗号技術における技術的信頼に関する検討を実施している。2013 年度は、暗号技術の安全性及び実装に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査を行った。また、本委員会の下に暗号解析評価ワーキンググループと軽量暗号ワーキンググループを設置し，暗号解析評価ワーキンググループでは離散対数問題及び格子問題等の困難性に関する調査を行い、軽量暗号ワーキンググループでは、軽量暗号の安全性および実装性能、既存技術との比較に関する調査を行うとともに、今後の軽量暗号に関する CRYPTREC での活動方針に関する議論を開始した。

2013 年 3 月に公表された CRYPTREC 暗号リストの改定版は、暗号技術に対する解析・攻撃技術の高度化や、新たな暗号技術の研究開発が進展している状況を踏まえ、安全性だけではなく、調達容易性、国産暗号の普及促進といった様々な視点で検討されたリストであり、「電子政府推奨暗号リスト」、「推奨候補暗号リスト」、「運用監視暗号リスト」から構成され、暗号技術の広範な利用に対応した使い易いものとなっている。しかし、これらのリストの暗号の安全性は、永遠に保証されるものではない。CRYPTREC 暗号リストの監視は、暗号が使われ続ける限り、電子政府の安全性確保のためにも、またネットワークセキュリティ全般の維持のためにも、継続していかねばならない活動である。暗号技術評価委員会は、今後もこの監視活動を担っていくことになる。さらに、暗号技術活用委員会との連携を保ちつつ、暗号技術の適切な利用の普及にも貢献していくことが求められる。このような CRYPTREC の活動は、これまでも、そしてこれからも、暗号技術やその実装及び運用に係る研究者及び技術者等の多くの関係者の協力を得て成り立つ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深甚な謝意を表する次第である。

暗号技術評価委員会　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章は暗号技術評価委員会の活動概要について説明してある。第2章は暗号技術評価委員会における監視活動に関する報告である。第3章は暗号技術評価委員会の下で活動している暗号技術調査ワーキンググループの活動報告である。

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「暗号技術評価委員会」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証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。

本報告書ならびにこれまでに発行されたCRYPTREC報告書、技術報告書、CRYPTREC暗号リスト記載の暗号技術の仕様書は、CRYPTRECの事務局（総務省、経済産業省、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）が共同で運営する下記のWebサイトで参照することができる。

http://www.cryptrec.go.jp/

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の事務局までご連絡いただけると幸いである。

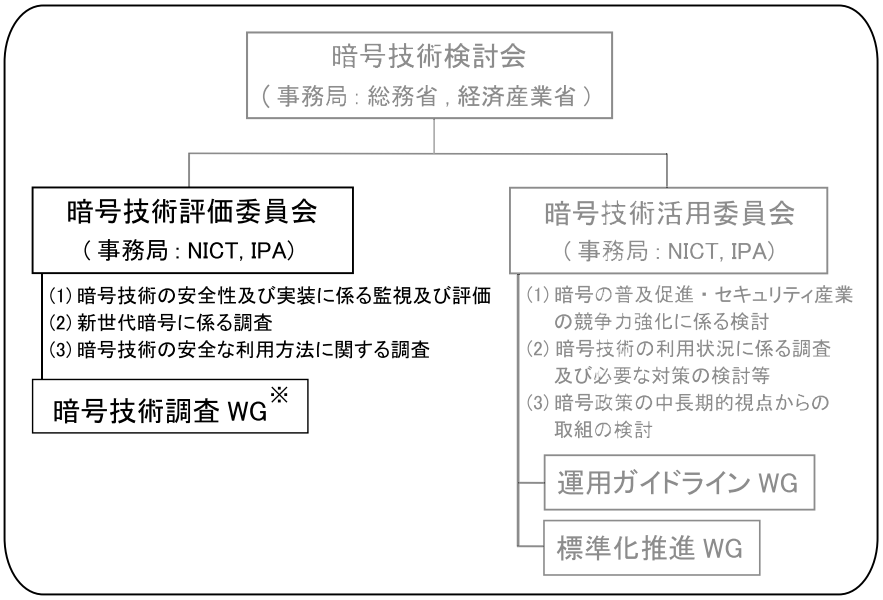
【問合せ先】　info@cryptrec.go.jp

委員会構成

暗号技術評価委員会(以下、「評価委員会」という。)は、総務省と経済産業省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(以下、「NICT」という。)と独立行政法人情報処理推進機構(以下、「IPA」という。)が共同で運営する。評価委員会は、CRYPTREC 暗号リスト(付録 1)に掲載されている暗号技術や電子政府システム等で利用される暗号技術の安全性維持及び信頼性確保の観点から、それらの安全性及び実装に係る監視及び評価を行う等、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、暗号技術の安全な利用方法に関する調査や新世代の暗号に関する調査も行う。

暗号技術調査ワーキンググループ(以下、「調査 WG」という。)は、評価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、評価委員会の指示のもと、評価委員会活動に必要な項目について調査・検討活動を担当する作業グループである。評価委員会の委員長は、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・検討結果を評価委員会に報告する。平成 25 年度、評価委員会の指示に基づき実施される調査項目は、「暗号解析 WG」及び「軽量暗号 WG」である。

評価委員会と連携して活動する「暗号技術活用委員会」も、評価委員会と同様、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。



※ 今年度実施されている調査項目：

- 離散対数問題の困難性や格子問題等の困難性に関する調査
- リソースの制限が厳しいデバイスにも実装可能な軽量暗号に関する調査

図 1：CRYPTREC 体制図

委員名簿

暗号技術評価委員会

委員長	今井 秀樹	中央大学 教授
委員	上原 哲太郎	立命館大学 教授
委員	太田 和夫	国立大学法人電気通信大学 大学院 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	高木 剛	国立大学法人九州大学 教授
委員	手塚 悟	東京工科大学 教授
委員	本間 尚文	国立大学法人東北大学 大学院 准教授
委員	松本 勉	国立大学法人横浜国立大学 大学院 教授
委員	松本 泰	セコム株式会社　マネージャー
委員	盛合 志帆	独立行政法人情報通信研究機構 研究室長
委員	山村 明弘	国立大学法人秋田大学 大学院 教授
委員	渡辺 創	独立行政法人産業技術総合研究所 研究グループ長

暗号技術調査ワーキンググループ(暗号解析評価)

主査	高木 剛	国立大学法人九州大学 教授
委員	青木 和麻呂	日本電信電話株式会社 主任研究員
委員	石黒 司	株式会社 KDDI 研究所 研究員
委員	太田 和夫	国立大学法人電気通信大学 大学院 教授
委員	草川 恵太	日本電信電話株式会社 研究員
委員	國廣 昇	国立大学法人東京大学　大学院　准教授
委員	下山 武司	株式会社富士通研究所 主任研究員
委員	安田 雅哉	株式会社富士通研究所

暗号技術調査ワーキンググループ(軽量暗号)

主査	本間 尚文	国立大学法人東北大学 大学院 准教授
委員	青木 和麻呂	日本電信電話株式会社 主任研究員
委員	岩田 哲	国立大学法人名古屋大学　大学院　准教授
委員	小川 一人	日本放送協会 放送技術研究所 主任研究員
委員	崎山 一男	国立大学法人電気通信大学　大学院　教授
委員	渋谷 香士	ソニー株式会社
委員	鈴木 大輔	三菱電機株式会社 主席研究員
委員	成吉 雄一郎	ルネサスエレクトロニクス株式会社 主任技師
委員	峯松 一彦	日本電気株式会社 主任研究員

委員	三宅 秀享	株式会社東芝 研究主務
委員	渡辺 大	株式会社日立製作所 主任研究員

オブザーバー

福永 利徳	内閣官房情報セキュリティセンター[2013 年 6 月まで]
今福 健太郎	内閣官房情報セキュリティセンター[2013 年 6 月まで]
中山 慎一	内閣官房情報セキュリティセンター[2013 年 8 月まで]
杉浦 幹人	内閣官房情報セキュリティセンター[2013 年 10 月まで]
石原 潤二	内閣官房情報セキュリティセンター[2013 年 6 月から]
高木 浩光	内閣官房情報セキュリティセンター[2013 年 7 月から]
大川 伸也	内閣官房情報セキュリティセンター[2013 年 8 月から]
森安 隆	内閣官房情報セキュリティセンター[2013 年 10 月から]
根木 まろか	警察庁 情報通信局[2013 年 8 月まで]
根本 農史	警察庁 情報通信局[2013 年 8 月から]
大平 利幸	総務省 行政管理局[2013 年 7 月まで]
佐藤 健太	総務省 行政管理局[2013 年 7 月から]
野村 知宏	総務省 自治行政局 住民制度課
飯田 恭弘	総務省 情報流通行政局
河合 直樹	総務省 情報流通行政局
中村 一成	総務省 情報流通行政局
佐久間 明彦	外務省 大臣官房
岩永 敏明	経済産業省 産業技術環境局
中谷 順一	経済産業省 商務情報政策局
室井 佳子	経済産業省 商務情報政策局
谷口 晋一	防衛省 運用企画局
多賀 文吾	警察大学校
滝澤 修	独立行政法人情報通信研究機構
花岡 悟一郎	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 （平和昌、沼田文彦、盛合志帆、野島良、大久保美也子、黒川貴司、金森祥子、側高幸治、笠井祥、大川晋司）

独立行政法人 情報処理推進機構（笹岡賢二郎[2013 年 6 月まで]、伊藤毅志[2013 年 7 月から]、近澤武、小暮淳、大熊建司、神田雅透、菅野哲[2013 年 10 月から]、稲垣詔喬、吉川法子）

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、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。

高度情報通信ネットワーク社会形成基本法（IT 基本法）[1]が策定された 2000 年以降、行政の情報化及び公共分野における情報通信技術の活用に関する様々な取り組みが実施されてくるにつれて、情報セキュリティ問題への取組みを抜本的に強化する必要性がますます認識されるようになってきた。2005 年 4 月に内閣官房に情報セキュリティセンター(NISC)が、同年 5 月に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)に情報セキュリティ政策会議がそれぞれ設置され、同会議により決定された「第 1 次情報セキュリティ基本計画」、「第 2 次情報セキュリティ基本計画」及び「国民を守る情報セキュリティ戦略」により情報セキュリティ水準の向上が図られてきた。

CRYPTREC では、2005 年度にハッシュ関数の安全性評価を実施し、2006 年 6 月に SHA-1 の安全性に関する見解を公表した。これに基づき、上述の第 1 次基本計画の年度計画である「セキュア・ジャパン 2007」では、「電子政府推奨暗号について、その危殆化が発生した際の取扱い手順及び実施体制の検討を進める」こととされ、NISC をはじめとする政府機関において、暗号の危殆化に備えた対応体制等を整備することが喫緊の課題であることが認識された。そして、2006 年度には素因数分解問題の困難性に関する評価を実施し、RSA1024 の安全性の評価を公表した。これらの SHA-1 及び RSA1024 に関する安全性に関する CRYPTREC からの見解に基づき、NISC の情報セキュリティ政策会議において「政府機関の情報システムにおいて使用される暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」[2]が 2008 年度に決定されるに至った。

2010年度から2013年度の4年間を対象とした施策である「国民を守る情報セキュリティ戦略」[3]においては、「政府機関における安全な暗号利用の推進」として「政府機関で使われて

[1] http://www.kantei.go.jp/jp/singi/it2/hourei/honbun.html
[2] http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf （2008 年 4 月 22 日決定情報セキュリティ政策会議決定）
[3] http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf （2010 年 5 月 11 日情報セキュリティ政策会議決定）

いる電子政府推奨暗号について、移行指針に従って暗号の着実な移行を進める。また、電子政府推奨暗号の安全性を継続的に監視・調査し、安全性が低下した暗号については速やかに代替となる暗号への移行を進めるための計画を策定するとともに、急激な安全性の低下に備え、あらかじめ緊急避難的な対応(コンティンジェンシープラン)を検討する。」という施策が取りまとめられた。また、2013年度から2014年度の2年間を対象とした施策である「サイバーセキュリティ戦略」においては、「情報及び情報システムに係る情報セキュリティ水準の一層の向上」として「暗号技術については、安全評価がなされたもの[4]の利用を推進する。」と「国際展開」として「電子政府等における安全性及び信頼性の確保として取り組んでいる暗号評価プロジェクト[5]について、その成果を国内外に発信し、暗号技術の利用促進を図る。」という施策が取りまとめられてきている。

このように、CRYPTREC 暗号リストに記載されている暗号技術の安全性及び信頼性確保のための活動等の機能は非常に重要であり、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・分析することが必要であることはもちろんのこと、今後も、CRYPTRECが発信する情報を踏まえ、各政府機関が連係して情報通信システムをより安全なものに移行するための取り組みを実施していくことが必要不可欠である。

1.2 暗号技術評価委員会

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[6]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、2007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。設置の目的は、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、また、電子政府推奨暗号の監視活動のほかに、暗号理論の最新の研究動向を把握し、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である。

2008 年度において、暗号技術監視委員会では、「電子政府推奨暗号リストの改訂に関する骨子(案)」及び「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)」

[4] 「電子政府における調達のために参照すべき暗号のリスト」(CRYPTREC(Cryptography Research and Evaluation Committees)暗号リスト)を指す。
[5] CRYPTREC の活動を指す。
[6] http://www.cryptrec.go.jp/list_2003.html

を策定したが、2009 年度からは次期リスト策定のために新しい体制に移行し、名称を「暗号方式委員会」と変更した。電子政府推奨暗号リスト改訂のための暗号技術公募(2009 年度)を受けて、2010 年度からは応募された暗号技術などの安全性評価を開始し、2012 年に「電子政府における調達のために参照すべき暗号のリスト(ＣＲＹＰＴＲＥＣ暗号リスト)」[7](付録１)を策定した。その概要については、CRYPTREC Report 2012 を参照のこと。

2013 年度からは、名称を「暗号方式委員会」から「暗号技術評価委員会」と変更し、暗号技術の安全性に係る監視・評価及び実装に係る技術(暗号モジュールに対する攻撃とその対策も含む)の監視・評価を実施することになった。暗号技術評価委員会の活動内容については、第 2 章を参照のこと。引き続き、暗号技術評価委員会では、その下に暗号技術調査ワーキンググループを設置し、暗号技術に関する具体的な検討を行っている。2013 年度については、暗号技術調査ワーキンググループ（暗号解析評価）及び暗号技術調査ワーキンググループ（軽量暗号）の 2 つのワーキンググループが設置されている。詳細については、第 3 章を参照こと。

1.3 CRYPTREC 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」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、CRYPTREC Report 2002 暗号技術評価報告書（平成１４年度版）に詳しく記載されている。CRYPTREC Report 2002 暗号技術評価報告書（平成１４年度版）は、次のURLから入手できる。

http://www.cryptrec.go.jp/report.html

なお、2009 年度は、2008 年度に検討した「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)」に基づき、電子政府推奨暗号リスト改訂のための暗号技術公募が行われた。2010 年度から 2012 年度にかけて、暗号方式委員会、暗号実装委員会及び暗号運用委員会にて評価が行われ、2012 年度に暗号技術検討会にて電子政府推奨暗号リストの改定が行われた。最終的に、総務省及び経済産業省がパブリックコメント[8]を行い、「電子政府における調達のために参照すべき暗号のリスト（ＣＲＹＰＴＲＥＣ暗号リスト)」が決定された。

[7] http://www.cryptrec.go.jp/list.html
[8] http://www.cryptrec.go.jp/topics/cryptrec_201212_listpc.html

1.4 活動の方針

暗号技術評価委員会では、主に、暗号技術の安全性評価を中心とした技術的な検討、すなわち、

(a) 新世代暗号に係る調査(軽量暗号、セキュリティパラメータ、ペアリング、耐量子計算機暗号等)

(b) 暗号技術の安全性に係る監視及び評価(SHA-3 の評価を含む)

(c) 暗号技術の安全な利用方法に関する調査(技術ガイドラインの整備、学術的な安全性の調査・公表等)

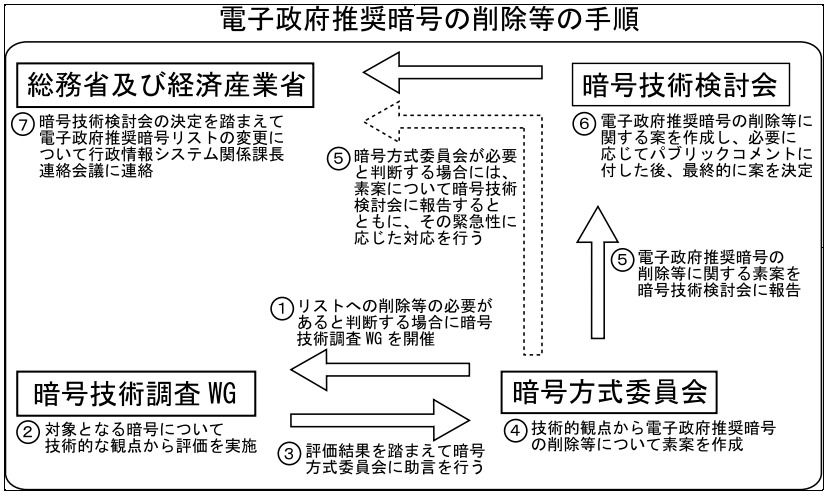
を実施する。

監視に関する基本的考え方は、CRYPTREC Report 2012 までに記載されていた電子政府推奨暗号リスト[9]掲載の暗号技術に対する考え方[10]と基本的に同じであり、仕様変更を認める際にも用いているため、ここに転載する。

(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。



[9] 2003 年 2 月 20 日に策定されたものを指す。

[10] たとえば、暗号技術検討会 2008 年度報告書を参照のこと。

第２章 監視活動

2.1.監視活動報告

電子政府推奨暗号の安全性評価について2013年度の報告時点では収集した全ての情報が引き続き「情報収集」、「情報分析」フェーズに留まり、「審議及び決定」には至らず、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生じていないと判断した。以降、収集、分析した主たる情報について報告する。

2.1.1.共通鍵暗号に関する安全性評価について

AESの安全性に関しては、Eurocrypt 2013とFSE 2014において単一鍵攻撃の進展が発表された。128 ビット鍵(AES-128)の 7 段縮小版に対する解読効率が改良し、192 ビット鍵(AES-192)と 256 ビット鍵(AES-256)では、攻撃可能段数がともに9段に拡張された。単一鍵攻撃について、最も成功した攻撃は次の通りである。

・AES-128: 7段(10段中)を選択平文2^{97}個、メモリ量 2^{98}、計算量 2^{99}で攻撃可能 [1]

・AES-192: 9段(12段中)を選択平文2^{107}個、メモリ量 2^{129}、 計算量 2^{172}で攻撃可能 [2]

・AES-256: 9段(14段中)を選択平文2^{120}個、 メモリ量 2^{203}、 計算量 2^{203}で攻撃可能[1]

一方、関連鍵攻撃の最良攻撃に関する進展はなく、次のとおりである。

・AES-128: 選択平文2^{88}個、計算量 $2^{126.2}$で攻撃可能 [3]

・AES-192: 選択平文2^{116}個、計算量2^{169} で攻撃可能 [3]

・AES-256: 選択平文2^{140}個、計算量$2^{254.4}$で攻撃可能[3]

2.1.2.公開鍵暗号に関する安全性評価について

昨年のCrypto 2012でA.K. Lenstraらは、実社会に公開されているRSA公開鍵証明書(X.509)に、異なる署名に同じmodulusが使われていたり、modulusが素因数分解できたりといった問題を指摘した。これに続き、Asiacrypt 2013においてN. Heningerらは、台湾市民向けのスマートカードで利用される公開鍵証明書約 300 万件について、同じ問題点があることと、Coppersmith 攻撃によって新たな素因数分解が可能となったことを示した[4]。

---

[1] Patrick Derbez, Pierre-Alain Fouque and Jeremy Jean, *Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting*, EUROCRYPT 2013, LNCS 7881, pp. 371-387. Springer 2013

[2] Leibo Li, Keting Jia and Xiaoyun Wang, *Improved Single-Key Attacks on 9-Round AES-192/256*, FSE 2014, LNCS. Springer, 2014

[3] A. Bogdanov, D. Khovratovich, and C. Rechberger, *Biclique Cryptanalysis of the Full AES*, ASIACRYPT 2011, LNCS 7073, pp. 344-371. Springer, 2011.

[4] Daniel J. Bernstein and Yun-An Chang and Chen-Mou Cheng and Li-Ping Chou and Nadia Heninger and

台湾政府はこの発表に対応し、対策を施したスマートカードへの置き換えを実施中である。

楕円曲線暗号に関しては、Asiacrypt 2013 のランプセッションにおいて J.W. Bos らが、実際に暗号通信(TLS/SSH)で利用されている証明書を調べ、TLS 公開鍵の 4%(20 万個)、SSH 公開鍵の 30%(40 万個)に同じものが使用されている問題点を確認した。また、Bitcoin において、同じ nonce の存在が利用されており、59 BTC が盗難されたとしている[5]。

離散対数問題(DLP: Discrete Logarithm Problem)に関しては、A.Joux が Eurocrypt 2013 において、1175 ビット及び 1425 ビットの解読実験、さらに、R.Granger らが Crypto 2013 において 1971 ビット及び 3164 ビットの解読実験に成功したことを発表した。Joux の発表は有限体として中程度のサイズの素体上の Kummer 拡大という特殊なものを対象としていたが、Granger らはこれを標数 2 の基礎体に拡張しており、より重要性が高い。さらに Crypto 2013 のランプセッションで発表した Francisco らも同様の研究を進めている。これら 3 つのグループが各々扱っている問題の対象、条件等が若干異なっており、これらの攻撃が有効となる条件および計算量の整理・明確化する必要がある。

2.1.3. ハッシュ関数に関する安全性評価について

Eurocrypt 2013 において、M.Stevens は、ハッシュ関数 SHA-1 に対し、与えられたローカル衝突の集合に対して理論的な最大成功確率及びその確率を達成する最小のメッセージ条件を与える新しい手法を導入した。この手法を利用して、計算量 2^{61} の同一接頭辞攻撃及び計算量 $2^{77.1}$ の選択接頭辞攻撃を示した。

同じく Eurocrypt 2013 において F.Mendel らは、SHA-256 に対する攻撃可能な段数(仕様では 64 段)を従来の 27 段から 31 段に拡張した。必要な計算量は圧縮関数計算 $2^{65.5}$ 回分である。

NIST は 2012 年 10 月に公募選考で選んだ Keccak を記載したハッシュ関数 SHA-3 の連邦標準規格 FIPS 202 のドラフトを発行する予定である[6]。

2.2. 仕様書の参照先の変更

2013 年 3 月に公表された「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」に掲載されている暗号技術の仕様書の参照先を調査した結果、外

Tanja Lange and Nicko van Someren, Factoring RSA keys from certified smart cards: Coppersmith in the wild, ASIACRYPT 2013, Part II, LNCS 8270, pp. 341-360. Springer 2013.

[5] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow, Elliptic Curve Cryptography in Practice,
http://asiacrypt.2013.rump.cr.yp.to/bb8efcc1194e0ee605e12babd0ca294d.pdf

[6] NIST は 2012 年 10 月に公募選考で選んだ Keccak を記載したハッシュ関数 SHA-3 の連邦標準規格 FIPS 202 のドラフトを 2014 年 5 月 28 日付けで公開した。

部機関の仕様書を参照しているもののうち、更新されたものがあったため、参照先の変更の検討を行った。

DSA(NIST FIPS 186-2(+Change Notice)[7]から NIST FIPS 186-4[8]へ)に関しては、有限体及びハッシュ関数のサイズの拡張は、パラメータ修正等の簡易な修正であると判断し、下記通り仕様書の参照先の変更について了承された。

ECDSA 及び ECDH(SEC 1 v2.0)については、DSA の事例と同様と考えられるが、新たに追加された機能の取り扱いについて検討が必要である。

アルゴリズム	判定結果	理由
DSA (NIST FIPS 186-2(+Change Notice) から NIST FIPS 186-4 へ)	仕様書の参照先の変更を認める。	補助関数(ハッシュ関数、KDF、及び、擬似乱数生成系、素数生成や楕円曲線生成等の基本的なアルゴリズム)を除いた、当該アルゴリズムを実装するための必要最小限の範囲において、パラメータ修正等の簡易な修正である。

2.3.暗号技術活用委員会からの質問に対する回答の検討について

暗号技術活用委員会から、Perfect forward secrecy と forward secrecy に関する技術的見解を求められたため、回答について検討を行った（質問及びその回答内容は、付録４を参照のこと)。

2.3.1.Perfect forward secrecy と forward secrecy 標準化機関での見解について

Perfect forward secrecy と forward secrecy を事務局で調査した結果、Perfect forward secrecy と forward secrecy に関して一致した見解を見つけることができなかった。

(1) IETF における見解

(a) RFC 4949 からの抜粋

[7] http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf

[8] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

> Ordinary forward secrecy vs. "perfect" forward secret: Experts disagree about the difference between these two. Some say there is no difference, and some say that the initial naming was unfortunate and suggest dropping the word "perfect". Some suggest using "forward secrecy" for the case where one long-term private key is compromised, and adding "perfect" for when both private keys (or, when the protocol is multi-party, all private keys) are compromised.

とあり、統一的見解がないとしている。

(b) RFC3268からの抜粋

> At the same time the DHE ciphersuites are the only ones to offer forward secrecy.

とあり、DHE には forward secrecy があるとしている。

(2) NIST SP800-52 revision 1 (Draft)における見解

NIST SP800-52 revision 1 (Draft)からの抜粋

> Cipher suites using ephemeral DH and ephemeral ECDH (i.e., those with DHE or ECDHE in the second mnemonic) provide perfect forward secrecy, ensuring long-term confidentiality of the session. While support of these cipher suites is not required by these guidelines, it is strongly recommended.

とあり、ephemeral DH(DHE)とephemeral ECDH(ECDHE)にはPerfect forward secrecyがあるとしている。

2.3.2.DHE, DH, RSAES-PKCS1-v1_5 の安全性について

SSL/TLS における DHE、DH、RSA の安全性評価は、[1,2]で与えられている。[1,2]では、Perfect forward secrecy の定義はされているが、forward secrecy の定義はされていない。[1,2]で定義されている Perfect forward secrecy は数学的に記述されているものの、NIST の解釈に近い。

NIST SP800-52 revision 1 (Draft)からの抜粋：

> Perfect forward secrecy is the condition in which the compromise of a long-term private key used in deriving a session key subsequent to the derivation does not cause the compromise of the session key.

[1,2]においては、下記が証明されている。

- DHE：安全な認証機能付き鍵交換であることが証明されている。それに加えて、Perfect forward secrecy を満たしていることも証明されている。
- DH：安全な認証機能付き鍵交換であることが証明されている。
- RSA: RSAES-PKCS1-v1_5 ではなく、RSA-OAEP を使った場合には、安全な認証機能付き鍵交換であることが証明されている。

以上をまとめると、
(1) SSL/TLS における、Perfect forward secrecy と forward secrecy には複数の見解があるが、概ね「長期的に使われる秘密鍵が漏洩しても、漏洩前のセッションで交換された鍵の秘密が漏れない」という意味で使われている。
(2) DHE が Perfect forward secrecy [1,2]を満たすこと、及び、RSAES-PKCS1-v1_5 が運用監視暗号であることを考慮に入れると、安全性の観点からは、DHE、DH、RSAES-PKCS1-v1_5 の順に優先順位が高いものと考えられる。

（参考文献）

[1] Tibor Jager, Florian Kohlar, Sven Schäge, Jörg Schwenk: On the Security of TLS-DHE in the Standard Model. CRYPTO 2012: 273-293
[2] Florian Kohlar, Sven Schäge, Jörg Schwenk: On the Security of TLS-DH and TLS-RSA in the Standard Model. IACR Cryptology ePrint Archive 2013: 367 (2013)

2.4.暗号技術の安全な利用方法に関する調査

2.4.1.128-bit key RC4 の注釈の変更について

128-bit key RC4（以下、RC4 という。）は、現在、運用監視暗号リストに掲載され、「128-bit RC4 は、SSL(TLS1.0 以上)に限定して利用すること」という注釈が付与されている。近年、報告されている脆弱性に鑑み、注釈の修正について検討を行ったが、継続審議となった。

2.4.2.CRYPTREC 暗号技術ガイドライン

CRYPTREC 暗号技術ガイドライン（SSL/TLS における近年の攻撃）

2013 年度は、SSL/TLS における近年の攻撃に関して、その攻撃手法の概要、システムに対する影響を分析するとともに、暗号スイートにおける安全性の観点での影響について、SSL/TLS に対する近年の攻撃に関するガイドラインを作成した。

SSL/TLS について、近年、プロトコルの仕組みの脆弱性やソフトウェアの脆弱性を複合的に利用する攻撃がいくつか公開されている。また、プロトコル内で用いる暗号として RC4 を選択することができるが、RC4 は運用監視暗号リストに位置づけられており、安全性に係る問題のある暗号技術として、互換性維持以外の目的での利用が推奨されていない。さらに、RC4 に対する攻撃が適用できる環境下では SSL/TLS の安全性が保てなくなることが示されている。このような状況を踏まえ、近年示されている攻撃の解説を行うとともに、SSL/TLS を安全に利用するため近年注目されている攻撃に対して推奨される対応を示すことを目的とした。

本ガイドラインでは、プロトコルの仕組みを利用した攻撃に起因する脆弱性について、解説するとともに推奨される対応策を示している。また、プロトコル内で用いる暗号として RC4 を用いた場合に、RC4 のアルゴリズムの弱さに起因する脆弱性を利用した攻撃方法、事例を示している。この場合は攻撃を回避する効果的な対応策がないため、RC4 を選択しない利用方法の推奨などを述べている。

プロトコルの仕組みを利用した攻撃に起因する脆弱性については、BEAST、CRIME、TIME、BREACH、Lucky Thirteen、Renegotiation を利用した攻撃などについて攻撃の仕組みを解説するとともにその回避策などについても言及している。それぞれの攻撃に対して、回避策や防止方法も明らかになっており、これらの攻撃があることを理由にプロトコル内で用いる暗号としてブロック暗号を利用しないという結論には至らない。

プロトコル内で用いる暗号として RC4 を用いた場合の RC4 のアルゴリズムの弱さに起因する脆弱性を利用した攻撃については、SSL/TLS の実際の利用環境を踏まえると、現実的な脅威として配慮すべき攻撃であるといえる。この場合、攻撃を回避する効果的な対応策がないため、RC4 を選択しない利用方法の推奨などを述べている。SSL/TLS にはいくつかのバージョンが存在するため、バージョン毎に具体的な対応策について言及している。

推奨される設定として、TLS 1.0 より古いバージョンについては、新しいバージョンへアップデートすることが推奨される。TLS 1.0 については、CBC モードを用いた場合の脆弱性に対してパッチが提供されているため、Java 等のソフトウェアを最新版に更新した上で、CBC モードを選択することが推奨される。TLS 1.1 については、CBC モードを用いた場合の脆弱性が解消されていることから、CBC モードを選択することが推奨される。TLS1.2 については、CBC モード、CCM モード、GCM モードが選択できるため、それらを使うことが推奨される。

CRYPTREC 暗号技術ガイドライン(SHA-1)

電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、CRYPTREC 暗号リストの運用監視暗号リストに記載されているハッシュ関数 SHA-1 を利用する際に必要となる情報、すなわち、SHA-1 に関する非推奨及び許容事項や参考情報について記載した。

推奨されない利用範囲として、電子署名における署名生成の１つ、許容される利用範囲として、電子署名における署名検証、HMAC、KDF、擬似乱数生成系、パスワード・ハッシングやチェックサムの計算としての利用の５つを定めた。

2.4.3.擬似乱数生成アルゴリズム Dual_EC_DRBG について

NIST Special Publication 800-90A 及び ANS X9.82 に記載されている擬似乱数生成アルゴリズム Dual_EC_DRBG(Dual Elliptic Curve Deterministic Random Bit Generation)にセキュリティ上の懸念が示されていることを受け、同アルゴリズムを含む暗号ライブラリ等を利用しているユーザー向けへの注意喚起の目的として、2013 年 9 月に米国 NIST が出した声明[9]の概要を CRYPTREC の Web ページ[10]において紹介した。

同 Web ページの抜粋：

・SP 800-90A Dual_EC_DRBG を使用しないよう推奨

NIST は SP 800-90A (January 2012)で規定されている Dual_EC_DRBG を使用しないことを強く推奨する。なお、Dual_EC_DRBGに関するセキュリティ上の懸念の解決とSP 800-90Aの再発行については現時点では未決定である。

・SP 800-90A をドラフトとして再発行し、パブリックコメントを受付

NIST SP 800-90A をドラフトとして再発行し、2013年11月6日までパブリックコメントを受け付ける。NISTは受領した全てのコメントについて精査し、60日以内に回答する。

・SP 800-90B および SP 800-90C に対するパブリックコメント期間の再開

NIST は SP 800-90B（乱数生成に利用されるエントロピー源）および SP 800-90C（乱数生成の構成法に関する勧告）のドラフトを追加レビューするため、2013年11月6日までパブリックコメントを受け付ける。

なお、Dual_EC_DRBG は、平成 15 年に発表した電子政府推奨暗号リストにも、平成 25 年に発表した CRYPTREC 暗号リストのいずれにも掲載されていませんが、本件については、今後も引続き状況を監視し、お知らせしてまいります。

2.5.学会等参加状況

国内外の学術会議に参加し、暗号解読技術に関する情報収集を実施した。参加した国際会議は、表2.1に示す通りである。

[9] http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf
[10] http://www.cryptrec.go.jp/topics/cryptrec_20131106_dual_ec_drbg.html

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 2013	International Conference on the Theory and Applications of Cryptographic Techniques	ギリシャ・アテネ	2013 年 5 月 26 日～2013 年 5 月 30 日
Crypto 2013	International Cryptology Conference	米国・サンタバーバラ	2013 年 8 月 18 日～2013 年 8 月 22 日
FDTC 2013	Workshop on Fault Diagnosis and Tolerance in Cryptography	米国・サンタバーバラ	2013 年 8 月 20 日
CHES 2013	Workshop on Cryptographic Hardware and Embedded Systems	米国・サンタバーバラ	2013 年 8 月 20 日～2013 年 8 月 23 日
Asiacrypt 2013	International Conference on the Theory and Application of Cryptology and Information Security	インド・バンガロール	2013 年 12 月 3 日～12 月 6 日
TCC 2014	Theory of Cryptography Conference	米国・サンディエゴ	2014 年 3 月 3 日～3 月 6 日
FSE 2014	International Workshop on Fast Software Encryption	英国・ロンドン	2014 年 3 月 11 日～3 月 13 日
PKC 2014	International Conference on Practice and Theory in Public-Key Cryptography	アルゼンチン・ブエノスアイレス	2014 年 2 月 27 日～3 月 1 日

以下に、国際学会等に発表された論文を中心に、暗号解読技術の最新動向を示す。詳しくは、付録 3 を参照のこと。

2.5.1.ブロック暗号の解読技術

・Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting [Eurocrypt 2013]

単一鍵モデルにおける AES(Advanced Encryption Standard、米国標準暗号)に対する中間者攻撃が発表された。ASIACRYPT 2010 における Dunkelman らの攻撃を改良したものであり、7 段の AES-128 に対し、データ計算量が 2^{97}、時間計算量が 2^{99}、空間計算量が 2^{98} となる最良の攻撃が示された。更に、8 段の AES-192/256 に対し、データ計算量が 2^{107} の選択平文、時間計算量が $2^{172}/2^{196}$、空間計算量が 2^{96} となる攻撃が、また 9 段の AES-256 に対して、データ計算量が 2^{120} の選択平文、時間・空間計算量が 2^{203} となる攻撃が示された。

・Improved Single-Key Attacks on 9-Round AES-192/256 [FSE 2014]

単一鍵モデルにおけるAESに対し、鍵依存篩による鍵候補の絞り込みによって、AES-192の解読可能段数を9段に伸ばした。データ計算量は2^{121}の選択平文、時間計算量が$2^{177.5}$、空間計算量は$2^{186.5}$。

2.5.2.ハッシュ関数の解読技術

・New collision attacks on SHA-1 based on optimal joint local-collision analysis [Eurocrypt 2013]

ハッシュ関数 SHA-1 に対する暗号解析の新しい方向性を与える。即ち、与えられたローカル衝突の集合に対し、理論的な最大成功確率及びその確率を達成する最小のメッセージ条件を与える新しい手法を導入する。これによる近接衝突攻撃の計算量は、関数$2^{57.5}$のSHA-1圧縮となる。また、計算量2^{61}の同一接頭辞攻撃及び計算量$2^{77.1}$の選択接頭辞攻撃も示す。

2.5.3.公開鍵暗号の解読技術

・On the Function Field Sieve and the Impact of Higher Splitting Probabilities [Crypto 2013, BEST PAPER]

電子政府推奨暗号のうち、DSA署名、DH鍵交換プロトコル等の安全性の根拠となるDLP解読の進展が5月のEurocryptでも報告されたが、今回も更なる進展が報告された。Joux-Lercierらの中程度サイズの基礎体に対する関数体篩法を標数2の基礎体に拡張したものであり、任意の元に対する離散対数を求める計算量は、$L_{q^n}(1/3,(4/9)^{1/3})$となる。更に、体が適切なサイズの中間体を持つ場合には、degreeが1および2の元に対する離散対数を求める計算量はヒューリスティックに多項式時間となるアルゴリズムが与えられた。この方法を用いて位数2^{1971}および2^{3164}の有限体の離散対数問題解読に成功し、記録が更新された。現在、3つのグループでそれぞれ研究が進んでいる。今回本セッションで発表を行ったGrangerらのアイルランドチーム、ランプセッションで発表を行ったFranciscoらのメキシコチーム、Eurocryptで発表を行ったJouxらのフランスチームである。

各々扱っている問題の対象、条件等が若干異なっており、これらの攻撃が有効となる条件および計算量の整理・明確化が課題である。

・Factoring RSA keys from certified smart cards: Coppersmith in the wild [Asiacrypt 2013]

N. Heninger らが、台湾市民向けのスマートカードで利用される公開鍵証明書約 300 万件を国民ディレクトリより収集し、秘密鍵解読実験を行った結果を発表した。Crypto 2012 で発表された最大公約数を求める攻撃法を適用した結果、103 個の秘密鍵を求めることに成功した。また、特殊な形をした素数が多数見つかったので、新たな試みとして、試し割りや Coppersmith 攻撃等を行った結果、81 個の秘密鍵を求めることに成功した。このような事態が生じた原因は、秘密鍵生成時の擬似乱数生成の使い方が安易であったり、後処理をしていない場合に、秘密鍵の形を推定されてしまうことにある。台湾政府はこの発表に対応し、対策を施したスマートカードを作成しており、順次置き換えを開始している。

・Elliptic Curve Cryptography in Practice [Asiacrypt 2013, Rump session]

マイクロソフト・ミシガン大学・ペンシルベニア大学の共同チームが、楕円曲線暗号を使った暗号通信(TLS/SSH)の公開鍵を調べたところ、楕円曲線暗号を利用した暗号通信(SSH/TLS)の公開鍵のうち、TLS 公開鍵の 4%(20 万個)、SSH 公開鍵の 30%(40 万個)、に同じものの使用が確認された。これはデフォルトの設定を安易に利用したことが原因と考えられ、実際、最近急速に注目を集めつつあるクラウドサービス Digital Ocean の SSH セットアップガイドに従った公開鍵設定をしているホストが 5614 件もあった。また、bitcoin のアドレスのうち 158 個が同じ nonce を使っており、アドレス 1HKywxiL4JziqXrzLKhmB6a74ma6kxbSDj は 59 BTC を盗んでおり、このうち 3 BTC は Android Java の乱数生成器の脆弱性が原因となっている。(http://eprint.iacr.org/2013/734)。

・Faster index calculus for the medium prime case. Application to 1175-bit and 1425-bit finite fields [Eurocrypt 2013]

フランスの A.Joux が、離散対数問題(DLP: Discrete Logarithm Problem)の解読実験を行い、1175 ビットおよび 1425 ビットの解読に成功したことを発表した。解読実験では暗号パラメーターが特殊な場合の性質(中程度のサイズの素体上の Kummer 拡大)を用いており、電子政府推奨暗号に影響しない。ただし、DLP の困難性に基づいた暗号技術を使用する場合には、これらの特殊なパラメーターを避けるよう注意しなければならない。

本論文の内容には含まれていないが、標数 2 の 2168=257×24 次拡大における DLP 解読に成功したというアナウンスが数論 ML において発表された。これも“twisted Kummer 拡大”の場合であるが、適用条件および効率を精査する必要がある。

2.5.4.その他の解読技術

・New Generic Attacks Against Hash-based MACs [Asiacrypt 2013]

具体的なハッシュ関数を使った HMAC とハッシュ関数に PRF を使った HMAC を識別する攻撃を Distinguishing-H 攻撃と定義する。このとき、1 ビットの単一鍵 HMAC では、Distinguishing-H 攻撃は $2^{1/2}$ 回の計算で攻撃可能であることを示した。この攻撃法を利用すると、HMAC-GOST に対し 2^{192} 回の計算で鍵が導出できることを示した。ここではチェックサムが攻撃を容易にしている。

2.6.暗号調査ワーキンググループ開催状況

2013 年度は、各ワーキンググループ（WG）が活動した主要活動項目は、表 2.2 の通りである。

表 2.2　2013 年度の主要活動項目

ワーキンググループ名	主査	主要活動項目
暗号解析評価 WG	高木 剛	近年、研究の進展している有限体上あるいは楕円曲線上の離散対数問題の困難性に関する調査を行う。2013 年度は、有限体上の離散対数問題の解読記録において、以前より長い鍵長のものが出現しているので、それらについて調査を行う。また、格子問題のほか、NP 困難に係る問題、多変数多項式に係る問題、符号理論に係る問題等、の数学的問題の困難性に関する調査を行う。
軽量暗号 WG	本間 尚文	これまでに提案されている軽量暗号の調査（安全性および実装性能、既存技術との比較）を行う。次に、今後活用される軽量暗号技術に求められる要求条件を明らかにし、評価方法等を検討する。これらの検討結果をふまえ、軽量暗号について CRYPTREC でどのような活動を進めるのが望ましいかを検討する。

2.7.委員会開催記録

2013 年度、暗号技術評価委員会は、表 2.3 の通り 2 回開催された。暗号技術調査ワーキンググループは、表 2.4 及び表 2.5 の通り計 5 回開催された。各会合の開催日及び主な議題は以下の通りである。

(1) 暗号技術評価委員会

表 2.3 暗号技術評価委員会の開催

回	年月日	議題
第1回	2013年7月29日	暗号技術評価委員会活動方針の検討、暗号技術調査ワーキンググループ活動方針の検討、暗号技術評価方法の検討、監視状況報告。
第2回	2013年12月13日	ワーキンググループ活動の中間報告 外部評価(ハッシュ関数)、仕様変更、RC4の取り扱い、技術ガイドラインについての審議 監視状況報告 擬似乱数生成アルゴリズムDual_EC_DRBGについての報告
第3回	2014年3月6日	ワーキンググループ活動の年度報告 ハッシュ関数の実装評価、技術ガイドライン、RC4の取り扱い、CRYPTREC Report 2013、2014年度活動計画案についての審議 暗号技術活用委員会からの質問について

(2) 暗号技術調査ワーキンググループ

表 2.4 暗号技術調査ワーキンググループ(暗号解析評価)の開催

回	年月日	議題
第1回	2013年9月3日	活動計画案についての審議と了承 作業内容及び作業分担についての審議
第2回	2014年2月20日	調査内容についての審議と了承

表 2.5 暗号技術調査ワーキンググループ(軽量暗号)の開催

回	年月日	議題
第1回	2013年9月17日	現状調査(サーベイ)について作業方針・分担の審議 アプリケーションに関する議論
第2回	2013年12月26日	現状調査(サーベイ)に関する中間報告 エンドユーザーからのヒアリング(自動車、制御システム) 今後の活動方針に関する議論
第3回	2014年2月20日	今年度実施した調査内容のとりまとめ 実装評価報告 2014年度の検討項目の抽出

第3章 暗号技術調査ワーキンググループ

3.1.暗号解析評価ガイドワーキンググループ

3.1.1.活動目的

公開鍵暗号の安全性は、素因数分解の困難性や離散対数問題の困難性などさまざまな数学的問題に依存している。本 WG ではこれまで、素因数分解の困難性及び離散対数問題等の困難性に関する調査を行ってきた。2013 年度も下記(1)及び(2)の調査等を継続して行う。

(1) 離散対数問題の困難性に関する調査

近年、研究の進展している有限体上あるいは楕円曲線上の離散対数問題の困難性に関する調査を行う。2013 年度は、有限体上の離散対数問題の解読記録において、以前より長い鍵長のものが出現しているので、それらについて調査を行う。

(2) 格子問題等の困難性に関する調査

格子問題のほか、NP 困難に係る問題、多変数多項式に係る問題、符号理論に係る問題等、量子計算機が実現しても安全性が保たれると期待されている「耐量子計算機暗号」を支える数学的問題の困難性に関する調査を行う。2013 年度は、昨年度リストアップした論文の中から注目すべき数学的問題をいくつか取り上げて、安全性について検討を行う。

3.1.2.委員構成(敬称略，五十音順)

主査：	高木 剛	九州大学
委員：	青木 和麻呂	NTT
委員：	石黒 司	KDDI研究所
委員：	太田 和夫	電気通信大学
委員：	草川 恵太	NTT
委員：	國廣 昇	東京大学
委員：	下山 武司	富士通研究所
委員：	安田 雅哉	富士通研究所

3.1.3.活動概要

2013 年度は、下記(1)～(3)の調査を実施した。なお、ワーキンググループの開催スケジュールは下記の通りであった。

第1回　　2013年9月3日　　活動計画案や作業内容についての審議と了承
第2回　　2014年2月20日　　調査内容についての審議と了承

(1) 離散対数問題の困難性について

標数が小さい有限体上の離散対数問題を解くことに適したアルゴリズムとして、関数体篩法が知られている。近年、関数体篩法の計算量を改善する方法として、Joux らにより Pinpointing(及びその改良)という手法の概要ついて報告があった。また、この手法の CRYPTREC 暗号リストに掲載の暗号技術への影響についても検討した。

(2) 格子問題等の困難性について

今年度は、昨年度検討予定としていた数学的問題の中から、研究が進んできている下記の数学的問題、

① Shortest Vector Problem (SVP)
② Learning with error (LWE)
③ Learning parity with noise (LPN)
④ Approximate Common Disivor (ACD)

を選び、その定義や解読アルゴリズム及び計算量について調査を行った。内容及び担当は下表の通りとなった。

表 3.1 ：調査内容と執筆担当

章	執筆担当	内容
1 章	事務局	調査の目的、まとめ (非専門家向け)
2 章 総論	石黒 司委員	総論 (General な攻撃に関する総論) : SVP、LLL、BKZ
3 章 LWE	下山 武司委員、 安田 雅哉委員	各問題について以下の項目を記述 (1) 公開鍵方式からの帰着、証明の有無、追加の問題・制約など (2) 攻撃や量子アルゴリズム - General な攻撃との関係 - 固有の攻撃 - 量子アルゴリズムとの関係
4 章 LPN	草川 恵太委員	
5 章 ACD	國廣 昇委員	

(3) 予測図の更新

スーパーコンピュータのベンチマーク結果の 1 位から 500 位を 1993 年から半年毎に集計している Web サイト TOP500.Org[1]において、2013 年 6 月・11 月のベンチマーク結果が追加されたので、素因数分解問題及び楕円曲線上の離散対数に関する 2 つの予測図を更新した。

[1] http://www.top500.org/

3.1.4.成果概要

数学的問題の困難性に関する調査報告書の概要は下記(1)及び(2)の通りである。詳細については、付録5を参照のこと。また、予測図の更新版を(3)に掲載する。

(1) 離散対数問題の困難性について

Pinpointing という近年提案された手法により、関数体篩法における篩(sieving)において、一つの relation を得るために必要な候補となる多項式の個数を従来の方法に比べて少なくすることが可能となった。この手法の適用範囲は、有限体の大きさそのものではなく、その中間体及び拡大次数の「バランス」に依存する。

そのため、素体(GF(p),p 素数)上構成されている DSA 及び DH への安全性に影響はない。

(2) 格子問題等の困難性について

① 格子の SVP(近似版を含む)のうち、近似因子が次元の多項式で表される場合に適用される、4つの解読アルゴリズム(LLL、BKZ、篩、ボロノイセル)の計算量等に関する概説、及び、最新の計算機実験(SVP Challenge, Lattice Challenge, Ideal Lattice Challenge)についての報告があった。

② LWE問題は、GapSVP及びSIVPの困難性に関する仮定のもとで解くことが困難であることが知られており、効率的に解くことが困難であると予想されている。完全準同型暗号スキームをはじめ、LWE問題ベースの暗号スキームが提案されてきている。実際の構成の際には、BKZアルゴリズム等の格子縮約アルゴリズムに対し耐性を持つようにパラメータ設定を行う必要があり、安全なLWEパラメータを選択することは今後の課題である。

③ 総当たり法で解く他に、LPN 問題を解くアルゴリズムを大別すると、3つの解読アルゴリズム(BKW、Arora-Ge による再線形化、シンドローム復号(SD)問題を経由するもの)が知られている。McEliece 暗号や Niederreiter 暗号をはじめ、90 年代から様々な暗号スキームが提案されてきている。BKW アルゴリズムの改良版である LF アルゴリズムの計算機実験例や SD 問題の高速化によるパラメータの評価例がある。

④ ACD 問題を、素因数分解を直接的に経由しないで解くアルゴリズムは、大別すると、組み合わせ論に基づく方法と格子理論に基づく方法がある。前者については、最近提案された Chen-Nguyen のアルゴリズムを使って、実際に提案論文で書かれた推奨パラメータのいくつかが解読されているため、今後の研究の動向に注視する必要がある。

(3) 予測図の更新

「1 年間でふるい処理を完了するのに要求される処理能力の予測」の更新後の図は、図3.1の通りとなる。

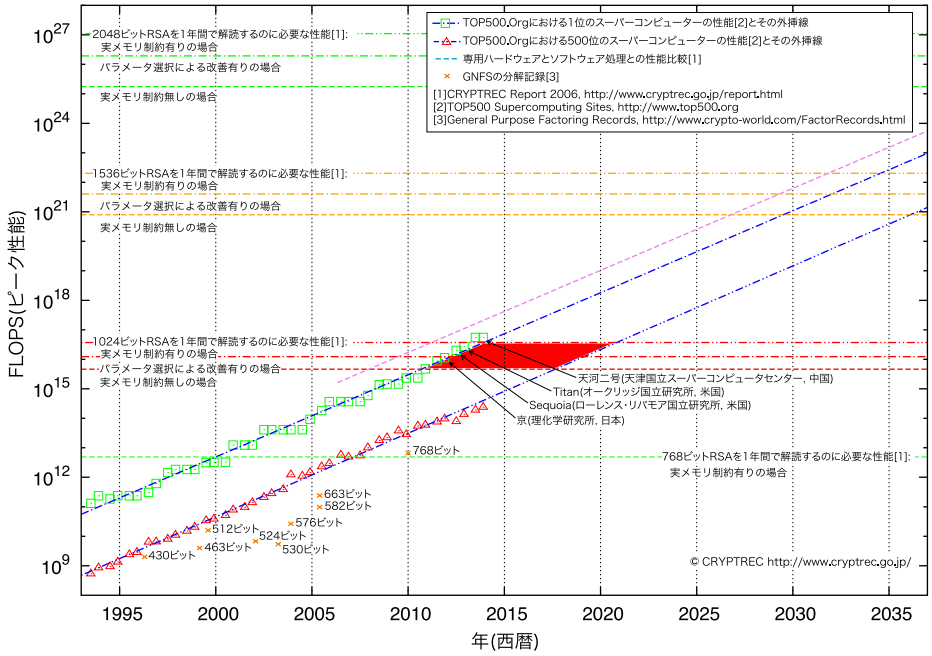


図 3.1：1 年間でふるい処理を完了するのに要求される処理能力の予測(2014 年 2 月更新)

また、「ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測」の更新後の図は、図 3.2 の通りとなる。

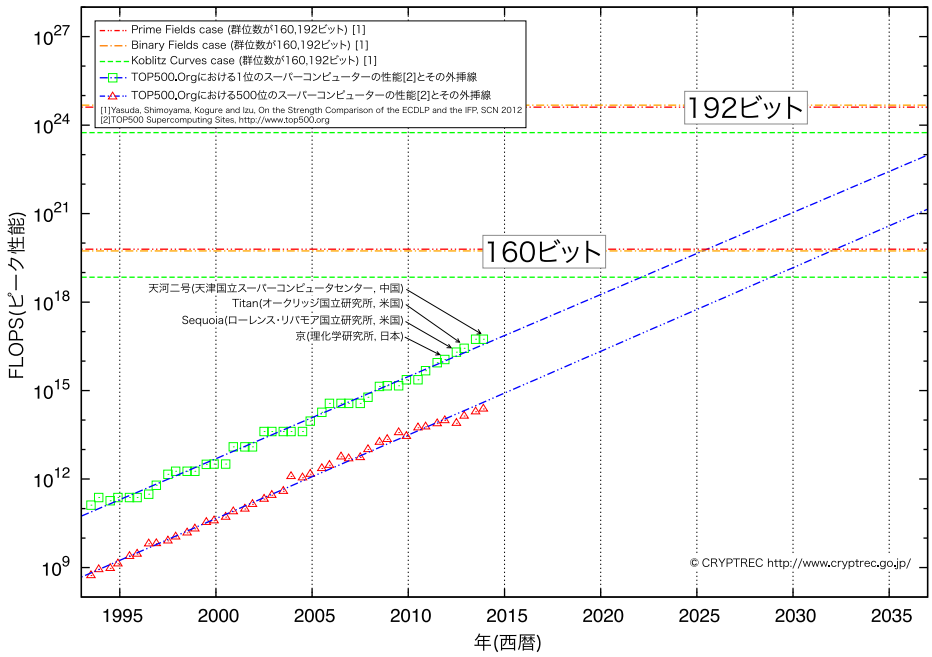


図 3.2： ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測(2014 年 2 月)

3.2.軽量暗号ワーキンググループ

3.2.1.活動目的

軽量暗号 WG は、軽量暗号技術が求められるサービスにおいて、電子政府のみならず利用者が最適な暗号方式を選択でき、容易に調達できることをめざして設置された。

本 WG では、これまでに提案されている軽量暗号の調査（安全性および実装性能、既存技術との比較）を行う。次に今後活用される軽量暗号技術に求められる要求条件を明らかにし、評価方法等を検討する。これらの検討結果をふまえ、軽量暗号について CRYPTREC でどのような活動を進めるのが望ましいかを検討する。

3.2.2.委員構成

主査：	本間　尚文	東北大学
委員：	青木　和麻呂	NTT
委員：	岩田　哲	名古屋大学
委員：	小川　一人	NHK
委員：	﨑山　一男	電気通信大学
委員：	渋谷　香士	ソニー
委員：	鈴木　大輔	三菱電機
委員：	成吉　雄一郎	ルネサスエレクトロニクス
委員：	峯松　一彦	NEC
委員：	三宅　秀享	東芝
委員：	渡辺　大	日立製作所

3.2.3.活動概要

2013 年度は、下記の活動を実施した。

（1）　軽量暗号技術に関する現状調査(サーベイ)

・軽量暗号アルゴリズム調査（安全性・実装性能)、軽量暗号に関わる新しい技術動向、外部動向（CAESAR プロジェクト)、軽量暗号の活用事例および標準化動向

（2）　軽量暗号のアプリケーションに関する調査

・ 軽量暗号の活用が期待される分野

・ エンドユーザーからのヒアリング(自動車、制御システム)

（3）　軽量暗号の実装評価

軽量ブロック暗号のハードウェア実装評価及びソフトウェア実装評価

（4）　今後の活動方針に関する議論

・ 暗号技術ガイドラインの発行、暗号技術の公募など、どのようなアプローチが望ま

しいのかの検討

・ 2014 年度の検討項目の抽出

なお、ワーキンググループの開催スケジュールは下記の通りであった。

第１回　2013年9月17日

- 現状調査(サーベイ)について作業方針・分担の審議
- アプリケーションに関する議論

第２回 2013年12月26日

- 現状調査(サーベイ)に関する中間報告
- エンドユーザーからのヒアリング(自動車、制御システム)
- 今後の活動方針に関する議論

第３回　2014年2月20日

- 今年度実施した調査内容のとりまとめ
- 実装評価報告
- 2014 年度の検討項目の抽出

3.2.4. 成果概要

(1) 軽量暗号技術に関する現状調査(サーベイ)

2013 年度は、軽量暗号技術に関する現状調査(サーベイ)として、表 3.2 に示した項目の調査を行った。

表 3.2: 軽量暗号技術に関する現状調査(サーベイ)

軽量暗号アルゴリズム調査		
	安全性	**実装性能**
ブロック暗号	青木 和麻呂 委員	渋谷 香士 委員
認証暗号(モード)	峯松 一彦 委員	鈴木 大輔 委員
ストリーム暗号	渡辺 大 委員	
ハッシュ関数	三宅 秀享 委員	
軽量暗号に関わる新しい技術動向		
Low-latency	﨑山 一男 委員	
サイドチャネル耐性	成吉 雄一郎 委員	
外部動向		
CAESAR	岩田 哲 委員	
軽量暗号の活用事例および標準化動向		
	小川 一人 委員	

(a) 軽量暗号アルゴリズム調査（安全性・実装性能）

軽量暗号アルゴリズム調査では、表 3.3 に示したブロック暗号、認証暗号、ストリーム暗号、ハッシュ関数を中心に、安全性および実装性能について学会等で発表されている文献調査を行い、その結果を各委員が報告書としてまとめた。

表 3.3: 調査対象の技術分類とアルゴリズム

技術分類	CRYPTREC （電子政府推奨暗号）	ISO/IEC 29192	その他
ブロック暗号	AES, TDES, Camellia	PRESENT, CLEFIA	LED, Piccolo, TWINE, PRINCE
認証暗号 （モード）	CCM, GCM （CTR, CMAC）		ALE, OCB
ストリーム暗号	KCipher-2	Trivium, Enocoro	Grain, MICKEY
ハッシュ関数	SHA-2	（PHOTON, SPONGENT）	SHA-3 (Keccak), Quark

※下線を引いたアルゴリズムは日本からの提案

(b) 軽量暗号に関わる新しい技術動向（低レイテンシ暗号（low-latency cryptography）及びサイドチャネル耐性）

暗号処理における低レイテンシ性は、データ通信における暗号処理時の応答速度を重視するアプリケーション、例えば、車の安全運転支援システム（Car2X communication）、セキュア・ストレージ、CPU-外部ストレージ間のバス暗号化等で求められている。現在、CMOS テクノロジの微細化による集積回路の信号遅延時間短縮はあまり期待できないため、低レイテンシ暗号を実現するためには、暗号処理に要する計算量を大幅に削減する必要があり、軽量暗号が新たに求められる理由のひとつとなっている。例えば，AES では回路規模，レイテンシともに上述のアプリケーションが求める要求は満たせず、数 10kGE の回路規模で，数 ns のレイテンシでハードウェア実装することは，現在の実装技術では達成できていない。

サイドチャネル耐性については、軽量暗号アルゴリズムにおけるリーク解析、電流解析、電磁波解析も含めたサイドチャネル攻撃および故障利用攻撃に関する文献調査を行った。

(c) 外部動向 (CAESAR プロジェクト)

2013年1月から開始された「認証暗号」(データの暗号化と認証を同時に行うための共通鍵暗号技術) の選定プロジェクト CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) について調査を行った。本プロジェクトでは「軽量」性についても評価要素に入ることが予想される。AES コンペティション, eSTREAM プロジェクト, SHA-3プロジェクトに続く国際的なコンペティションであり, 本WGで継続的に注視していく。

(d) 軽量暗号の活用事例および標準化動向

今後の暗号の開発において、活用事例・標準化動向から軽量暗号に関する要求条件を導き出し、研究開発、標準化の指針を得ることを目的として調査を行った。活用事例調査としては、軽量暗号が活用されると期待されている分野 (RFID、センサーネットワーク (環境測定等)、医療センサー、ＩＴＳ、記録メディア (HDD、SSD 等)、携帯端末 (携帯電話、タブレット端末、ポータブルゲーム機等) について公開されている情報を調査するほか、メーカー数社にヒアリングを行った。調査の結果、軽量暗号に対する要求はあるものの、具体的なスペックまで落とし込んだ要求条件は出ていないことが分かった。しかしながら医療センサーの事例で、標準化されれば使用する業者があるということも分かった。CRYPTREC などの機関で評価・選定を行うことで、軽量暗号の利用促進につながると考えられる。

標準化動向調査では、ISO/IEC JTC 1/SC 27/WG 2 で進められてきた標準化状況及び IETF Light-Weight Implementation Guidance (lwig)で開始された軽量暗号の実装に関する活動状況調査を行った。

(2) アプリケーションに関する調査

下記に挙げられるような軽量暗号の特徴から、軽量暗号の活用が期待されるアプリケーションのリストアップを行った。

<u>軽量暗号の特徴</u>

- ハードウェア規模が小さい, 低消費電力で動作, 消費電力が少ない, 低コスト
- コードサイズが小さい, RAM が少ない
- 低レイテンシ性, リアルタイム性

<u>軽量暗号の活用が期待されるアプリケーション</u>

- RFID タグ, センサー, ワイヤレスセンサー
- IC カード
- 医療機器(体内埋め込みや携帯型など), ヘルスケア製品
- スマートメータ
- モバイル製品

- バッテリ
- 車, ITS システム

また、エンドユーザーからのヒアリングとして、下記の２名の方から自動車および社会インフラへの軽量暗号技術の応用について意見を伺った。

「自動車におけるITセキュリティ」（トヨタIT 開発センター 小熊 寿氏）

「制御システム向け暗号の要件の考察」（日立製作所 大和田 徹氏）

小熊氏からは、自動車における IT セキュリティでは、例えば、車載ネットワーク CAN のデータ長が８バイトであることから、軽量暗号は、MAC を生成するアルゴリズムとして処理性能や MAC サイズの点で AES よりも有利と思われるとのコメントがあった。

また、大和田氏からは、課題からみた制御システム向け暗号の要件が抽出され、高速処理、低処理負荷、柔軟な暗号化対象長、低リソースでの鍵管理・更新機能等の要件で軽量暗号が役立つ可能性があるとコメントがあった。

(3) 軽量暗号の実装評価

(1)で行った現状調査にも軽量暗号の実装評価は含まれるが、既存文献の調査であることから、文献により評価環境や実装者が異なるため、暗号アルゴリズム間の比較が困難であった。そこで、NICT にて表 3.3 に示す軽量ブロック暗号について、同一プラットフォーム上で、同一の実装者または統一的な実装ポリシーによりハードウェア実装およびソフトウェア実装の評価を行い、統一的な評価環境で比較を行った結果が第 3 回軽量暗号 WG にて報告された。実装環境および測定指標は下記の通りである。

・ ハードウェア実装評価

- 標準的な CMOS セルライブラリ：NANGATE Open Cell Library (45nm CMOS)
- unrolled 実装, round 実装, serial 実装の 3 通りのアーキテクチャ
- 測定指標：最大動作周波数、処理速度、ゲートカウント、サイクルカウント、消費電力、ピーク電流

・ ソフトウェア実装評価

- プロセッサ：ルネサスエレクトロニクス RL78 (16bit 組み込みマイコン)
- 測定指標：処理速度, RAM サイズ, ROM サイズ

ROM, RAM サイズに関して下記4通りの組み合わせで、それぞれの範囲内で処理速度を最大化する実装を行った。

ROM	512B	1024B
RAM	64B	128B

このハードウェア実装評価では､軽量暗号は AES と比較して 1-2Kgate 回路規模が小さく、この違いはマチュアなプロセス(180nm-350nm)において実装の可否に影響する場合があり、アドバンテージとなること、リアルタイムのメモリ暗号化やμ秒クラスのリアルタイム通信などのアプリケーションにおいて優位となる可能性があることが報告された。また、小さい、速いという一つの指標だけだと AES との差分が少ないが、小さく、速く、サイドチャネル対策が容易という複数の軸で比較したときに AES に対する優位性がより明確になると報告された。

ソフトウェア（組み込みマイコン）実装においては、コードサイズの小さい暗号への要求が高い。メモリが十分あれば（例えば、アルゴリズム単体で暗号復号込みで ROM 1KB あれば） AES で十分である。よって組み込みマイコンにおいて AES より価値ある軽量ブロック暗号は、暗号・復号込みで ROM 200B 以下、RAM 32B 以下でそれなりの速度が達成できるアルゴリズムと考えられるという報告があった。

(4) 今後の活動方針に関する議論

当初は、今年度中に CRYPTREC における軽量暗号に関する今後の活動方針について WG として結論を出し、暗号技術評価委員会に報告する予定であったが、もう少しじっくり時間をかけて調査、議論を行い、結論を出すべきだという意見が出たことから、2014 年度末に方針を提言することで合意された。CRYPTREC における軽量暗号に関する今後の活動方針とその意義・目的としては、以下のような案が考えられうる（図 3.3 参照)。

A) 「暗号技術ガイドライン（軽量暗号の最新動向)」の発行

- 軽量暗号の最新技術動向をまとめた技術レポートであり、暗号技術者や専門家等が軽量暗号に関する専門的知識を得るのに活用される。

B) 「暗号技術ガイドライン（軽量暗号の詳細評価)」の発行

- 代表的な軽量暗号の安全性・実装性能を統一的に評価した技術レポートであり、ユーザが軽量暗号アルゴリズムを選択・利用する際の技術的判断材料として活用される。これにより、軽量暗号の利用促進、軽量暗号アルゴリズムの第三者評価レポートとして ISO/IEC 等国際標準化への貢献が期待される。

C) 軽量暗号に関する技術公募の実施

- CRYPTREC 暗号リストへの掲載を視野に、軽量暗号の公募・詳細評価を行い、選定を行う。これにより、軽量暗号が CRYPTREC 暗号リストへ新技術として追加され、電子政府システム等で最適な方式を選択でき、容易に調達できるようになることが期待される。

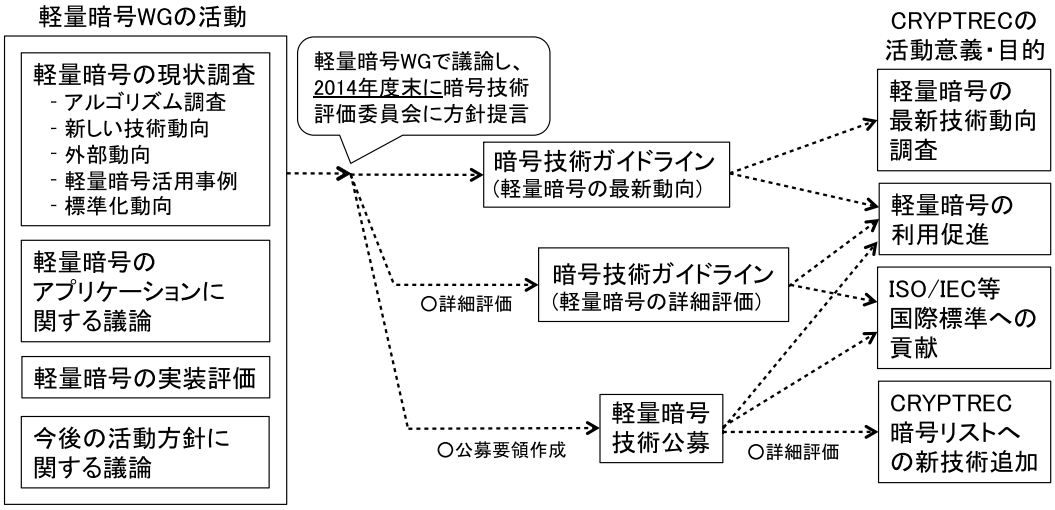


図 3.3: 今後の活動方針案

2014 年度に検討すべき課題

① 軽量暗号に関する検討
- 軽量暗号が既存暗号に対してアドバンテージをもつエリア
- 軽量暗号で達成すべき安全性

② 軽量暗号技術に関する現状調査（サーベイ）
- 認証暗号:CAESAR プロジェクト提案アルゴリズム等から軽量性に優れた方式を調査
- ハッシュ関数: SHA-3 の調査

③ 今後の活動方針に関する検討
- CRYPTREC における軽量暗号技術の位置づけと意義
- A)暗号技術ガイドライン（軽量暗号の最新動向）の発行、B)暗号技術ガイドライン（軽量暗号の詳細評価）の発行、C)軽量暗号に関する技術公募の実施のいずれがよいか検討を行い、暗号技術評価委員会に提言を行う。

付録 1

電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）

平成２５年３月１日
総　　務　　省
経　済　産　業　省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト。

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64 ビットブロック暗号(注2)	3-key Triple DES(注3)
	128 ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報通信担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

（注1） 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注2） より長いブロック長の暗号が利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3） 3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。
1） NIST SP 800-67 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4） 初期化ベクトル長は 96 ビットを推奨する。

推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術[3]のリスト。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64 ビットブロック暗号(注6)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128 ビットブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01(注7)
ハッシュ関数		該当なし
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES
エンティティ認証		ISO/IEC 9798-4

（注5） KEM（Key Encapsulating Mechanism）- DEM（Data Encapsulating Mechanism）構成における利用を前提とする。

（注6） より長いブロック長の暗号が利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7） 平文サイズは 64 ビットの倍数に限る。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

運用監視暗号リスト

実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術[4]のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない。

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64 ビットブロック暗号	該当なし
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPEMD-160
		SHA-1(注8)
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		CBC-MAC(注11)
エンティティ認証		該当なし

（注8） 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成20年4月 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成 25 年 3 月 1 日現在）

（注9） SSL 3.0 / TLS 1.0, 1.1, 1.2 で利用実績があることから当面の利用を認める。

（注10） 128-bit RC4 は、SSL （TLS 1.0 以上）に限定して利用すること。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合 CRYPTREC 暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

付録 2

CRYPTREC 暗号リスト掲載暗号の問い合わせ先一覧

電子政府推奨暗号リスト

1. 公開鍵暗号

暗号名	DSA
関連情報	仕様 ・NIST Federal Information Processing Standards Publication 186-2 (+ Change Notice) (January 2000, Change Notice 1 は October 2001), Digital Signature Standard (DSS) で規定されたもの。 ・ 参照 URL <http://csrc.nist.gov/publications/PubsFIPS.html>

暗号名	ECDSA (Elliptic Curve Digital Signature Algorithm)
関連情報 1	公開ホームページ 和文：http://jp.fujitsu.com/group/labs/techinfo/technote/crypto/ecc.html 英文：http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/ecc.html
問い合わせ先 1	富士通株式会社 電子政府推奨暗号 問い合わせ窓口 E-MAIL：soft-crypto-ml@ml.css.fujitsu.com
関連情報 2	仕様 ・ANS X9.62-2005, Public Key Cryptography for The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) 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	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.rsa.com/rsalabs/node.asp?id=2124> 和文： なし 英文： http://www.rsa.com/rsalabs/node.asp?id=2005
問い合わせ先	〒151-0053 東京都渋谷区代々木 2 丁目 1 番 1 号 新宿マインズタワー EMC ジャパン株式会社 RSA 事業本部 第二営業部 三田 晃 TEL：03-6830-3341, FAX：03-5308-8979, E-MAIL：akira.mita@rsa.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.rsa.com/rsalabs/node.asp?id=2124〉 和文：　なし 英文：　http://www.rsa.com/rsalabs/node.asp?id=2125
問い合わせ先	〒151-0053 東京都渋谷区代々木２丁目１番１号　新宿マインズタワー EMC ジャパン株式会社　RSA 事業本部　第二営業部　三田 晃 TEL：03-6830-3341, FAX：03-5308-8979, E-MAIL：akira.mita@rsa.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.rsa.com/rsalabs/node.asp?id=2124〉 和文：　なし 英文：　http://www.rsa.com/rsalabs/node.asp?id=2146
問い合わせ先	〒151-0053 東京都渋谷区代々木２丁目１番１号　新宿マインズタワー EMC ジャパン株式会社　RSA 事業本部　第二営業部　三田 晃 TEL：03-6830-3341, FAX：03-5308-8979, E-MAIL：akira.mita@rsa.com

暗号名	DH
関連情報 1	仕様 ・ANSI X9.42-2003, 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。
関連情報 2	仕様 ・NIST Special Publication 800-56A (March 2007), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revides) において、FCC DH プリミティブとして規定されたもの。 ・参照 URL〈http://csrc.nist.gov/publications/PubsSPs.html〉

暗号名	ECDH (Elliptic Curve Diffie-Hellman Scheme)
関連情報 1	公開ホームページ 和文:http://jp.fujitsu.com/group/labs/techinfo/technote/crypto/ecc.html 英文:http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/ecc.html
問い合わせ先 1	富士通株式会社 電子政府推奨暗号 問い合わせ窓口 E-MAIL：soft-crypto-ml@ml.css.fujitsu.com
関連情報 2	仕様 ・NIST Special Publication SP 800-56A (March 2007), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revides) において、C(2,0,ECC CDH)として規定されたもの。 ・参照 URL <http://csrc.nist.gov/publications/PubsSPs.html>

2. 共通鍵暗号

暗号名	Triple DES
関連情報	仕様 ・NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004. ・参照 URL <http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf>

暗号名	AES
関連情報	仕様 ・ NIST FIPS PUB 197, Specification for the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001. ・ 参照 URL <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

暗号名	Camellia
関連情報	公開ホームページ 和文：http://info.isl.ntt.co.jp/crypt/camellia/index.html 英文：http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11 日本電信電話株式会社　NTT セキュアプラットフォーム研究所 Camellia 問い合わせ窓口　担当 TEL:0422-59-3461, FAX:0422-59-3885 E-MAIL:camellia@lab.ntt.co.jp

暗号名	KCipher-2
関連情報	公開ホームページ 和文:http://www.kddilabs.jp/products/security/kcipher2/product.html 英文:http://www.kddilabs.jp/english/Products/Security/kcipher2/product.html
問い合わせ先	〒356-8502 埼玉県ふじみ野市大原 2-1-15 株式会社 KDDI 研究所　情報セキュリティグループ 研究マネージャー　清本 晋作 TEL:049-278-7885, FAX:049-278-7510 E-MAIL:kiyomoto@kddilabs.jp

3. ハッシュ関数

暗号名	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>

4. 暗号利用モード(秘匿モード)

暗号名	CBC, CFB, CTR, OFB
関連情報 1	仕様 ・NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation Methods and Techniques ・ 参照 URL <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>

5. 暗号利用モード(認証付き秘匿モード)

暗号名	CCM
関連情報 1	仕様 ・ NIST SP 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004. ・ 参照 URL <http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf>

暗号名	GCM
関連情報	仕様 ・NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007. ・ 参照 URL 〈http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf〉

6. メッセージ認証コード

暗号名	CMAC
関連情報 1	仕様 ・NIST FIPS SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005. ・ 参照 URL 〈http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf〉

暗号名	HMAC
関連情報 1	仕様 ・NIST FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008. ・ 参照 URL 〈http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf〉

7. エンティティ認証

暗号名	ISO/IEC 9798-2
関連情報	仕様 ・ISO/IEC 9798-2:2008, Information technology - Security techniques - Entity Authentication - Part 2: Mechanisms using symmetric encipherment algorithms, 2008. 及び ISO/IEC 9798-2:2008/Cor.1:2010, Information technology - Security techniques - Entity Authentication - Part 2: Mechanisms using symmetric encipherment algorithms. Technical Corrigendum 1, 2010. で規定されたもの。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	ISO/IEC 9798-3
関連情報	仕様 ・ISO/IEC 9798-3:1998, Information technology - Security techniques - Entity Authentication - Part 3: Mechanisms using digital signature techniques, 1998. 及び ISO/IEC 9798-3:1998/Amd.1:2010, Information technology - Security techniques - Entity Authentication - Part 3: Mechanisms using digital signa- ture techniques. Amendment 1, 2010. で規定されたもの。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。

推奨候補暗号リスト

1．公開鍵暗号

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/crypt/psec/index.html 英文　http://info.isl.ntt.co.jp/crypt/eng/psec/index.html
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11 日本電信電話株式会社　NTT セキュアプラットフォーム研究所 PSEC-KEM 問い合わせ窓口　担当 TEL: 0422-59-3462　　FAX: 0422-59-4015 E-MAIL: publickey@lab.ntt.co.jp

2．共通鍵暗号

暗号名	CIPHERUNICORN-E
関連情報	公開ホームページ 和文：http://www.nec.co.jp/cced/SecureWare/advancedpack/
問い合わせ先	〒211-8666 神奈川県川崎市中原区下沼部 1753 日本電気株式会社　システムソフトウェア事業部 セキュリティ G E-MAIL：info@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/index.htm
問い合わせ先	〒212-8582 神奈川県川崎市幸区小向東芝町 1 株式会社東芝 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 研究主幹 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 http://www.mitsubishielectric.co.jp/corporate/randd/information_technology/security/code/misty01_b.html
問い合わせ先	〒100-8310 東京都千代田区丸の内 2-7-3（東京ビル） 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 インフォメーションシステム統括事業部　社会インフラシステム部　坂上 勉 TEL：03-3218-3221　　FAX：03-3218-3638 E-MAIL：Sakagami.Tsutomu@bp.MitsubishiElectric.co.jp

暗号名	CIPHERUNICORN-A
関連情報	公開ホームページ 和文：http://www.nec.co.jp/cced/SecureWare/advancedpack/
問い合わせ先	〒211-8666 神奈川県川崎市中原区下沼部 1753 日本電気株式会社　システムソフトウェア事業部 セキュリティ G E-MAIL：info@security.jp.nec.com

暗号名	CLEFIA
関連情報	公開ホームページ 和文：http://www.sony.co.jp/Products/cryptography/clefia/ 英文：http://www.sony.net/Products/cryptography/clefia/
問い合わせ先	ソニー株式会社 CLEFIA 問い合わせ窓口 E-MAIL：clefia-q@jp.sony.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/index.htm
問い合わせ先	〒212-8582 神奈川県川崎市幸区小向東芝町 1 株式会社東芝 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 研究主幹 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://jp.fujitsu.com/group/labs/techinfo/technote/crypto/sc2000.html 英文： http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/sc2000.html
問い合わせ先	富士通株式会社 電子政府推奨暗号 問い合わせ窓口 E-MAIL：soft-crypto-ml@ml.css.fujitsu.com

暗号名	Enocoro-128v2
関連情報	公開ホームページ 和文:http://www.hitachi.co.jp/rd/yrl/crypto/enocoro/ 英文:http://www.hitachi.com/rd/yrl/crypto/enocoro/index.html
問い合わせ先	〒244-0817 神奈川県横浜市戸塚区吉田町 292 株式会社日立製作所　横浜研究所　エンタープライズシステム研究部 主任研究員　渡辺 大 TEL：050-3135-3440, FAX：050-3135-3387 E-MAIL: dai.watanabe.td@hitachi.com

暗号名	MUGI
関連情報	公開ホームページ 和文：http://www.hitachi.co.jp/rd/yrl/crypto/mugi/ 英文：http://www.hitachi.com/rd/yrl/crypto/mugi/
問い合わせ先	〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地 株式会社　日立製作所　情報・通信システム社 IT プラットフォーム事業本部　開発統括本部 主管技師長　松永 和男 TEL：045-862-8498,　FAX：050-3139-8348 E-MAIL：kazuo.matsunaga.bz@hitachi.com

暗号名	MULTI-S01
関連情報	公開ホームページ 和文：http://www.hitachi.co.jp/rd/yrl/crypto/s01/ 英文：http://www.hitachi.com/rd/yrl/crypto/s01/
問い合わせ先	〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地 株式会社　日立製作所　情報・通信システム社 IT プラットフォーム事業本部　開発統括本部　主管技師長　松永 和男 TEL：045-862-8498,　FAX：050-3139-8348 E-MAIL：kazuo.matsunaga.bz@hitachi.com

3. メッセージ認証コード

暗号名	PC-MAC-AES
関連情報	
参照 URL: http://jpn.nec.com/rd/crl/code/research/pcmacaes.html	
問い合わせ先	〒211-8666 神奈川県川崎市中原区下沼部 1753 日本電気株式会社　クラウドシステム研究所　主任研究員 峯松 一彦 TEL：044-431-7665, FAX：044-431-7707 E-MAIL: k-minematsu@ah.jp.nec.com

4. エンティティ認証

暗号名	ISO/IEC 9798-4
関連情報	仕様 ・ ISO/IEC 9798-4:1999, Information technology - Security techniques - Entity Authentication - Part 3: Mechanisms using a cryptographic check function, 1999.及び ISO/IEC 9798-4:1999/Cor.1:2009, Information technology - Security techniques - Entity Authentication - Part 3: Mechanisms using a cryptographic check function. Technical Corrigendum 1, 2009. で規定されたもの。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。

運用監視暗号リスト

1．公開鍵暗号

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.rsa.com/rsalabs/node.asp?id=2125〉
問い合わせ先	〒151-0053 東京都渋谷区代々木２丁目１番１号　新宿マインズタワー EMC ジャパン株式会社　RSA 事業本部　第二営業部　部長　齊藤 賢一 TEL：03-6830-3341，FAX：03-5308-8979，E-MAIL：kenichi.saito@rsa.com

2．共通鍵暗号

暗号名	RC4
関連情報	仕様 ・問い合わせ先 EMC ジャパン株式会社 RSA 事業本部(http://japan.rsa.com) ・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.rsa.com/rsalabs/node.asp?id=2149〉

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
関連情報	仕様 ・FIPS PUB 186-2，Secure Hash Standard (SHS) ・参照 URL 〈http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf〉

4. メッセージ認証コード

暗号名	CBC-MAC
関連情報	仕様 ・ ISO/IEC 9797-1:1999, Information technology - Security techniques - Message Authentication Codes(MACs) - Part 1: Mechanisms using a block cipher, 1999. で規定されたもの。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。

付録 3　　学会等での主要攻撃論文発表等一覧

目次

1.1. 具体的な暗号の攻撃に関する発表

表 2 に具体的な暗号の攻撃に関する発表のリストをカテゴリー別に示す。★は電子政府推奨暗号の安全性に直接関わる技術動向、☆はその他の注視すべき技術動向である。

表 2 具体的な暗号の攻撃に関する発表

公開鍵暗号		頁
	Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers [Eurocrypt 2013]	54
☆	Candidate Multilinear Maps from Ideal Lattices (BEST PAPER) [Eurocrypt 2013]	54
☆	On the Function Field Sieve and the Impact of Higher Splitting Probabilities [Crypto 2013, BEST PAPER]	57

1.2. Eurocrypt 2013 の発表

1.2.1. Eurocrypt 2013 の発表(1 日目)

Faster index calculus for the medium prime case. Application to 1175-bit and 1425-bit finite fields [Eurocrypt 2013]
Antoine Joux

フランスの A.Joux が、離散対数問題(DLP: Discrete Logarithm Problem)の解読実験を行い、1175 ビットおよび 1425 ビットの解読に成功したことを発表した。電子政府推奨暗号では、電子署名アルゴリズム DSA および鍵共有アルゴリズム DH が関係するが、解読実験では暗号パラメーターが特殊な場合の性質(中程度のサイズの素体上の Kummer 拡大)を用いており、電子政府推奨暗号には影響しない。ただし、DLP の困難性に基づいた暗号技術を使用する場合には、これらの特殊なパラメーターを避けるよう注意しなければならない。
本論文の内容には含まれていないが、標数 2 の 2168=257×24 次拡大における DLP 解読に成功したというアナウンスが数論 ML において発表された。これも“twisted Kummer 拡大”の場合であるが、適用条件および効率を精査する必要がある。

Candidate Multilinear Maps from Ideal Lattices (BEST PAPER) [Eurocrypt 2013]
Sanjam Garg, Craig Gentry, and Shai Halevi

最優秀論文賞は、S. Garg 氏(UCLA、アメリカ)他による多重線型写像の構成に関する論文である。多重線型写像の概念は 10 年ほど前から知られていたが、具体的な実現は知られていなかったため、新な応用が期待される。例えば、鍵交換、属性ベース暗号、Witness 暗号、関数型暗号、アグリゲート署名等への応用が挙げられている。

Cryptanalysis of Full RIPEMD-128 [Eurocrypt 2013]
Franck Landelle and Thomas Peyrin

フルラウンドの RIPEMD-128(圧縮関数に対する衝突攻撃および圧縮関数／ハッシュ関数に対する識別攻撃)が発表された。圧縮関数に対する衝突攻撃の計算量は $2^{61.57}$、圧縮関数に対する識別攻撃の計算量は $2^{59.57}$、ハッシュ関数に対する識別攻撃の計算量は $2^{105.40}$ である。

1.2.2. Eurocrypt 2013 の発表(2 日目)

New collision attacks on SHA-1 based on optimal joint local-collision analysis [Eurocrypt 2013]
Marc Stevens

ハッシュ関数 SHA-1 に対する暗号解析の新しい方向性を与える。即ち、与えられたローカル衝突の集合に対し、理論的な最大成功確率及びその確率を達成する最小のメッセージ条件を与える新しい手法を導入する。これによる近接衝突攻撃の計算量は、関数 $2^{57.5}$ の SHA-1 圧縮となる。また、計算量 2^{61} の同一接頭辞攻撃及び計算量 $2^{77.1}$ の選択接頭辞攻撃も示す。が発表された。

Improving Local Collisions: New Attacks on Reduced SHA-256 [Eurocrypt 2013]
Florian Mendel, Tomislav Nad and Martin Schlaffer

SHA-256 に対する semi-free-start 衝突の構成及び衝突への変換により、27 段から 31 段までの SHA-2 ハッシュ関数への既知結果を凌ぐ衝突攻撃が発表された。31 段 SHA-256 ハッシュ関数の衝突は計算量 $2^{65.5}$ の、38 段の semi-free-start 衝突は計算量 2^{37} となった。

Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting [Eurocrypt 2013]

Patrick Derbez, Pierre-Alain Fouque and Jeremy Jean

単一鍵モデルにおける AES(Advanced Encryption Standard、米国標準暗号)に対する中間者攻撃が発表された。ASIACRYPT 2010 における Dunkelman らの攻撃を改良したものであり、7 段の AES-128 に対し、データ計算量が 2^{97}、時間計算量が 2^{99}、空間計算量が 2^{98} となる最良の攻撃が示された。更に、8 段の AES-192/256 に対し、データ計算量が 2^{107} の選択平文、時間計算量が $2^{172}/2^{196}$、空間計算量が 2^{96} となる攻撃が、また 9 段の AES-256 に対して、データ計算量が 2^{120} の選択平文、時間・空間計算量が 2^{203} となる攻撃が示された。

1.3. Crypto 2013 の発表

1.3.1. Crypto 2013 の発表(1 日目)

Counter-cryptanalysis - reconstructing Flame's new variant collision attack [Crypto 2013, BEST YOUNG-AUTHOR PAPER]

Marc Stevens

暗号解析に対して弱い暗号プリミティブを強くする新しいパラダイムとして「暗号解析対抗」という手法を導入する。暗号解析攻撃による避けられない異常現象を利用することにより、暗号解析を検知しブロックすることができる。これにより互換性を損なうことなく弱い暗号プリミティブを安全に使い続けることができる。例えば、MD5 もしくは SHA-1 の衝突攻撃によって作られたメッセージであるか否かを判定することができる。また、この手法によりマルウェア Flame は、MD5 に対する選択接頭辞衝突攻撃の知られていないバリアントを用いていることを発見することができた。

Real Time Cryptanalysis of Bluetooth Encryption with Condition Masking [Crypto 2013]

Bin Zhang, Chao Xu, and Dengguo Feng

Bluetooth 標準の 2 レベル E0 ストリーム暗号に対する新たな攻撃手法である「条件マスク」を導入し、条件相関攻撃の時間/メモリ/データ計算量を削減した。$2^{22.7}$ フレームの最初の 24 ビットが利用可能であると仮定した場合、2^{27} のオンライン計算と、$2^{21.1}$ のオフライン計算と 4MB メモリにより、秘密鍵を求めることができる。

Structural Evaluation of AES and Chosen-Key Distinguisher of 9-round AES-128 [Crypto 2013]

Pierre-Alain Fouque and Jeremy Jean and Thomas Peyrin

構造解析により、フル AES-128 は、MDS 行列の係数および Sbox の差分特性を考慮に入れない限り、その構造だけで関連鍵差分攻撃に対し安全性を証明することはできないことを示した。また、9 ラウンドの AES-128 に対する選択鍵モデルにおける非自明な識別攻撃を示し、長年の未解決問題を解決した。

Bounds in Shallows and in Miseries [Crypto 2013]

Celine Blondeau and Andrey Bogdanov and Gregor Leander

差分特性の期待差分確率(EDP: Expected Differential Probability)の境界値と、固定した鍵に対する特性を実際に満たす入力ペアの最大値との量的な関係を示した。理論的結果を最近の著名なブロック暗号とハッシュ関数に適用した結果、ほとんどの場合において特性に従うペアの数は少ないという良い結果となった。しかしながら Keccak に関しては、我々のテクニックに対して意味のあるペアの最大値を保証するのは、より多くの段数が必要であるという結果となった。ただしこれは Keccak の脆弱性を示すことにはならない。

Sieve-in-the-Middle - Improved MITM Attacks [Crypto 2013]

Anne Canteaut and Maria Naya-Plasencia and Bastien Vayssiere

中間一致攻撃を改良し、より多くの段数を攻撃可能とする「中間篩攻撃」という新しい一般的な攻撃を示す。中間状態の衝突を探すことで鍵候補を選ぶ代わりに、ある中間 Sbox の有効な変換に対応しない鍵候補を無視する。このテクニックを bicliques テクニックと結びつけることにより、同じ時間計算量により攻撃段数を 1～2 段増やすことが可能となり、更に鍵サイズがブロックサイズより大きいときには追加データを必要としない。これらのテクニックは PRESENT, DES, PRINCE, AES に適ようすることができ、特に PRINCE の場合は 12 段中 8 段(これまでは 6 段)までの攻撃が可能となる。

Construction of Differential Characteristics in ARX Designs -- Application to Skein [Crypto 2013]
Gaetan Leurent

ARX 設計の暗号スキームに対し、差分特性を構成するアルゴリズムを与え、ハッシュ関数 Skein の縮約版に適用した。やや強い仮定の元で計算量を低くした攻撃では、free-start の衝突を 20 段の Skein-256 に対して、また、semi-free-start の衝突を 12 段の Skein-256 に対して構成することができた。フルバージョンの Skein-256 は 72 段であるため、セキュリティマージンはまだ十分である。

1.3.2. Crypto 2013 の発表(3 日目)

On the Function Field Sieve and the Impact of Higher Splitting Probabilities [Crypto 2013, BEST PAPER]
Faruk Gologlu, Robert Granger, Gary McGuire and Jens Zumbragel

電子政府推奨暗号のうち、DSA 署名、DH 鍵交換プロトコル等の安全性の根拠となる DLP 解読の進展が 5 月の Eurocrypt 2013 でも報告されたが、今回も更なる進展が報告された。Joux-Lercier による中程度のサイズの関数体篩法を標数 2 の体の場合に拡張したものであり、任意の元に対する離散対数を求める計算量は、$L_{q^n}(1/3, (4/9)^{1/3})$となる。更に、体が適切なサイズの中間体を持つ場合には、degree が 1 および 2 の元に対する離散対数を求める計算量はヒューリスティックに多項式時間となるアルゴリズムが与えられた。この方法を用いて位数 2^{1971} および 2^{3164} の有限体の離散対数問題解読に成功し、記録が更新された。現在、3 つのグループでそれぞれ研究が進んでいる。今回本セッションで発表を行った Granger らのアイルランドチーム、ランプセッションで発表を行った Francisco らのメキシコチーム、Eurocrypt 2013 で発表を行った Joux らのフランスチームである。
各々扱っている問題の対象、条件等が若干異なっており、これらの攻撃が有効となる条件および計算量の整理・明確化が課題である。

1.3.3. Crypto 2013 の発表(ランプセッション)

Factoring RSA keys from certified smart cards: Coppersmith in the wild [Crypto 2013, Rump session]
Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, Nicko van Someren

台湾市民の公開鍵証明書約 300 万件を国民ディレクトリより収集し、秘密鍵解読実験を行った結果をランプセッションにて発表した。昨年度発表された最大公約数攻撃による解読では、103 個の秘密鍵を求めることに成功した。また、新たな試みとして、特殊な形をした素数による試し割り、Coppersmith 攻撃等を行い、いくつかのケースにおいて秘密鍵を求めることに成功した。
問題は、秘密鍵生成時の疑似乱数生成の使い方が安易であったり、後処理をしていない場合に、秘密鍵の形を推定されてしまうことにある。

1.4. Asiacrypt 2013 の発表

1.4.1. Asiacrypt 2013 の発表(2 日目)

Block ciphers - past and present
Lars R. Knudsen

ブロック暗号の攻撃と証明可能安全性で著名な Knudsen 氏による招待講演。DES, LOKI などに対する攻撃、Feistel 型暗号の証明可能安全性など研究初期の話から、最近の軽量暗号 PRESENT, PRINTcipher, Maya, PRINCE に対する攻撃など過去 25 年に渡るブロック暗号研究を紹介した。最後に、最も遅れているテーマは鍵スケジュールであること、軽量暗号がブロック暗号研究を再活性化していると述べた。

Generic Key Recovery Attack on Feistel Scheme [Asiacrypt 2013]
Takanori Isobe and Kyoji Shibutani

Feistel 暗号に対する汎用の鍵復元攻撃で攻撃可能な段数を解析した。F 関数として、(1)鍵依存のみ仮定、(2)鍵の XOR 後に非線形変換、(3)鍵の XOR 後に S-box 処理と線形拡散 の３種類を対象とし、ブロック長 n ビット、鍵長 k ビットとしたとき、鍵回復攻撃の可能段数は次のようになった。

	(1) 一般	(2) XOR + 非線形	(3) XOR + S + P
k=2n	8	9	11
k=3n/2	6	7	9
k=n	4	5	7

1.4.2. Asiacrypt 2013 の発表(3 日目)

New Generic Attacks Against Hash-based MACs [Asiacrypt 2013]
Gaetan Leurent and Thomas Peyrin and Lei Wang

具体的なハッシュ関数を使った HMAC とハッシュ関数に PRF を使った HMAC を識別する攻撃を Distinguishing-H 攻撃と定義する。このとき、1 ビットの単一鍵 HMAC では、Distinguishing-H 攻撃は $2^{1/2}$ 回の計算で攻撃可能であることを示した。この攻撃法を利用すると、HMAC-GOST に対し 2^{192} 回の計算で鍵が導出できることを示した。ここではチェックサムが攻撃を容易にしている。

Cryptanalysis of HMAC/NMAC-Whirlpool [Asiacrypt 2013]
Jian Guo and Yu Sasaki and Lei Wang and Shuang Wu

Whirlpool に対する Mendel らの解析をベースに、HMAC/NMAC-Whirlpool を攻撃した結果、フルラウンド(10 段)の Distinguish-H 攻撃、6 段縮小版に対する鍵復元攻撃に成功した。

1.4.3. Asiacrypt 2013 の発表(4 日目)

Factoring RSA keys from certified smart cards: Coppersmith in the wild [Asiacrypt

2013]
Daniel J. Bernstein and Yun-An Chang and Chen-Mou Cheng and Li-Ping Chou and Nadia Heninger and Tanja Lange and Nicko van Someren

N.Heningerらが、台湾市民向けのスマートカードで利用される公開鍵証明書約300万件を国民ディレクトリより収集し、秘密鍵解読実験を行った結果を発表した。Crypto 2012 で発表された最大公約数を求める攻撃法を適用した結果、103 個の秘密鍵を求めることに成功した。また、特殊な形をした素数が多数見つかったので、新たな試みとして、試し割りや Coppersmith 攻撃等を行った結果、81 個の秘密鍵を求めることに成功した。このような自体が生じた原因は、秘密鍵生成時の疑似乱数生成の使い方が安易であったり、後処理をしていない場合に、秘密鍵の形を推定されてしまうことにある。台湾政府はこの発表に対応し、対策を施したスマートカードを作成しており、順次置き換えを開始している。

Improved Cryptanalysis of Reduced RIPEMD-160 [Asiacrypt 2013]
Florian Mendel and Thomas Peyrin and Martin Schlaffer and Lei Wang and Shuang Wu

運用監視暗号リストに掲載されている RIPEMD-160 に対して、free-start-collision 攻撃の解析を行い、攻撃可能段数を従来の 36 段(仕様は 80 段)から 42 段に伸ばした。

1.4.4. Asiacrypt 2013 の発表(ランプセッション n)

Equivalent Key Recovery Attacks against HMAC and NMAC with Whirlpool Reduced to 7 Rounds [Asiacrypt 2013, Rump session]
Jian Guo, Yu Sasaki, Lei Wang, Meiqin Wang, Long Wen

Whirlpool をハッシュ関数に利用した HMAC/NMAC に対して、本会議の３日目に同じ著者らが 6 段までの攻撃を発表している。論文投稿後に解析が進み、7 段まで攻撃できたことが報告された。

Security of SIMON against Linear Cryptanalysis [Asiacrypt 2013, Rump session]
Javad Alizadeh, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar, Somitra Sanadhya Kumar

SIMON は米国 NIST がハードウェア実装向けに開発した軽量暗号で、CHES 2013 のランプセッションで発表された。古典的な Feistel 構造で、ブロック長は 32 ビットと 64 ビットの２種類がある。F 関数は不可逆であるが、線形特性にはいくつかの高いものが見つかっている。線形解読で攻撃可能な段数を調べた結果、32 ビット・ブロック版に対しては、鍵長 64 ビットでは 12 段(32 段中)、鍵長 96 ビットでは 15 段(36 段中)まで攻撃可能。64 ビット・ブロック版に対しては、鍵長 128 ビットでは 19 段(44 段中)、鍵長 144 ビットでは 28 段(54 段中)、鍵長 256 ビットでは 35 段(72 段中)まで攻撃可能だった。

Elliptic Curve Cryptography in Practice [Asiacrypt 2013, Rump session]
Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow

マイクロソフト・ミシガン大学・ペンシルベニア大学の共同チームが、楕円曲線暗号を使った暗号通信(TLS/SSH)の公開鍵を調べたところ、楕円曲線暗号を利用した暗号通信(SSH/TLS)の公開鍵のうち、TLS 公開鍵の 4%(20 万個)、SSH 公開鍵の 30%(40 万個)、に同じものの使用が確認された。これはデフォルトの設定を安易に利用したことが原因と考えられ、実際、最近急速に注目を集めつつあるクラウドサー

ビス Digital Ocean の SSH セットアップガイドに従った公開鍵設定をしているホストが 5614 件もあった。また、bitcoin のアドレスのうち 158 個が同じ nonce を使っており、アドレス 1HKywxiL4JziqXrzLKhmB6a74ma6kxbSDj は 59 BTC を盗んでおり、このうち 3 BTC は Android Java の乱数生成器の脆弱性が原因となっている。(http://eprint.iacr.org/2013/734)

Discrete Log Computation in a field of size p^{40}, p is a 19-bits prime (728-bits) [Asiacrypt 2013, Rump session]

Palash Sarkar, Shashank Singh

Joux らは、Eurocrypt 2006 において 556 ビット (GF(p^{30}), p = 370801)、Eurocrypt 2013 において 1425 ビット (GF(p^{57}), p は 25 ビット)の離散対数問題を説いているが、今回、この間に位置する 728 ビット (GF(p^{40}), p=297079)と 560 ビット (GF(p^{35}), p=65407) の離散対数問題を解くことに成功した。

1.5. FSE 2014 の発表

1.5.1. FSE 2014 の発表(1 日目)

Match Box Meet-in-the-Middle Attack against KATAN [FSE 2014]

Thomas Fuhr and Brice Minaud

KATAN は De Canniere らが CHES 2009 で発表した軽量ブロック暗号で、KATAN32, KATAN48, KATAN64 の 3 種類がある。数値はブロック長(単位はビット)を表し、鍵長は 80 ビット、254 段繰り返し構造である。基本的な中間一致攻撃に、biclique 攻撃と match-box 攻撃を適用して攻撃可能段数を伸ばすことにより、K32 の 153 段縮小版、K48 の 129 段縮小版、K64 の 119 段縮小版が理論的に攻撃であることを示した。攻撃では、データ複雑度が 3 種類共通で 2^5 個の選択平文と $2^{78.5}$ の時間複雑度、空間複雑度は各々、2^{76}, 2^{76}, 2^{74} である。

Collision Spectrum, Entropy Loss, T-Sponges, and Cryptanalysis of GLUON-64 [FSE 2014]

Leo Paul Perrin and Dmitry Khovratovich

GLUON は、Africacrypt 2012 で提案された T スポンジ型の軽量ハッシュ関数のファミリであり、GLUON-64 はビットレート r=8、容量 c=128 である。f 関数は置換ではないため、メッセージが長くなるにつれ、エントロピー損失が起こり、衝突の発見が容易となる。本論文では、f 関数の置換からの違いを示す衝突確率スペクトラム(CPS)を導入し、解析した。その結果、最後が 1Mb の 0 で終わるメッセージに対する原像探索に要する計算量が、提案者が示した 2^{128} より小さい $2^{115.3}$ となることを理論的に示した。

Improved All-Subkeys Recovery Attacks on FOX, KATAN and SHACAL-2 Block cipher [FSE 2014]

Takanori Isobe and Kyoji Shibutani

Asiacrypt 2013 で提案された Function Reduction 法を Lai-Massey 型と LFSR 型に適用可能になるよう拡張し、繰り返し型にした ASR(All-Subkeys Recovery)攻撃に適用して必要データ量を削減す方法を提案し、FOX64/128, KATAN32/48/64, SHACAL-2 に適用した。各暗号に対する攻撃結果を表で示す。

暗号名	鍵長	攻撃段数	時間複雑度	メモリ複雑度	データ複雑度
FOX64	128	7/64	2^{124}	2^{124}	$2^{30.9}$
FOX128	256	7/64	2^{124}	2^{124}	$2^{30.9}$
KATAN32	32	119/254	$2^{79.1}$	$2^{79.1}$	144
KATAN48	48	105/254	$2^{79.1}$	$2^{79.1}$	144
KATAN64	64	94/254	$2^{79.1}$	$2^{79.1}$	142
SHACAL-2	256	42/64	2^{508}	2^{508}	2^{25}

Improved Single-Key Attacks on 9-Round AES-192/256 [FSE 2014]

Leibo Li, Keting Jia and Xiaoyun Wang

単一鍵モデルにおける AES に対し、鍵依存篩による鍵候補の絞り込みによって、AES-192 の解読可能段数を 9 段に伸ばした。データ計算量は 2^{121} の選択平文、時間計算量が $2^{177.5}$、空間計算量は $2^{186.5}$。

Cryptanalysis of FIDES [FSE 2014]

Itai Dinur and Jeremy Jean

FIDES は鍵なし AES の段関数を利用した認証付き暗号(Authenticated Encryption)である。パラメータ c を持ち、鍵サイズが 80 ビットの FIDES-80 (c=5)と 96 ビットの FIDES-96 (c=6)の 2 種類がある。設計者は 16c ビットの安全性を主張していたが、本論文では、guess-and-determine アルゴリズムによって、17 個の連続する既知平文に対する leaked nibbles と追加値があれば、2^{15c} 回分の計算量で内部状態を復元できることを示した。

1.5.2. FSE 2014 の発表(2 日目)

Impact of ANSI X9.24-1:2009 Key Check Value on ISO/IEC 9797-1:2011 MACs [FSE 2014]
Tetsu Iwata and Lei Wang

Key check value(KCV)は、ANS X9.24-1:2009 の Annex C に記載された、CBC MAC 属の鍵をチェックするための数値である。本論文では、ISO/IEC 9797-1:2001 に掲載されている CBC MAC 属 10 方式のうち 5 方式(MAC2.1, MAC2.2, MAC3, MAC5(CMAC), MAC6.2)の安全性が、KCV によって低下することを示した。KCV を s ビットとすると安全性の低下は s/2 ビット分である。

Plaintext Recovery Attacks Against WPA/TKIP [FSE 2014]
Kenneth G. Paterson, Jacob C. N. Schuldt and Bertram Poettering

WPA/TKIP は無線 LAN の暗号化プロトコルの一つであり、安全性に問題が指摘されている RC4 を使用しているが、現実には今だに広く使われている。TKIP(Temporal Key Integrity Protocol)では、TKIP sequence Counter (TSC)という 48 ビットのカウンターが利用されており、本論文ではこれに着目し、同じ平文を多数の異なる鍵で通信する設定での攻撃が提案された。攻撃は攻撃に使用するデータ量に関し、minimum と ideally の 2 種類を示し、実際の攻撃に掛かる計算時間を下表のように示した。

	鍵ストリーム長 (TSC 組ごと)	TSC 組数	データ量	計算時間 (コア*日数)
minimum	2^{32}	2^{16}	2^{48}	2^{14}
ideal	2^{40}	2^{16}	2^{56}	2^{22}

Dependence in IV-related bytes of RC4 key enhances vulnerabilities in WPA [FSE 2014]
Sourav Sen Gupta, Subhamoy Maitra, Willi Meier, Goutam Paul and Santanu Sarkar

RC4 を使用する WPA に対する既存の攻撃では、鍵ストリーム自体の偏りに注目しているが、本論文では鍵ストリーム間の相関に注目し、観測されている偏りの理論的証明や平文回復攻撃の効率を改善した。

Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64 [FSE 2014]
Itai Dinur, Orr Dunkelman, Nathan Keller and Adi Shamir

ブロック暗号に対する中間一致攻撃において、新規開発の線形鍵篩法と既知平文攻撃に利用可能な splice-and-cut 法を利用する方法提案した。提案法を軽量暗号 LED-64 に適用し、攻撃可能段数は増えないものの攻撃の効率を改良した。攻撃の複雑度は下表の通り。

攻撃タイプ	ステップ数	時間複雑度	データ複雑度	メモリ複雑度
単一鍵	2	2^{48}	2^{16} CP	2^{16}
単一鍵	2	2^{48}	2^{48} KP	2^{48}
関連鍵	3	2^{49}	2^{49} CP	2^{49}

Improved Slender-set Linear Cryptanalysis [FSE 2014]
Guo-Qiang Liu, Chen-Hui Jin and Chuan-Da Qi

ブロック暗号の Maya は PRESENT にした構造で、秘密の 4 ビット S-box が利用されている。本論文では、フーリエ変換を利用して S-box を絞り込む方法を利用した攻撃法を提案した。16 段縮小版に対する攻撃では、データ複雑度 2^{36}、時間複雑度 $2^{18.9}$、成功率 87.5%である。

Cryptanalysis of KLEIN [FSE 2014]
Virginie Lallemand and Maria Naya-Plasencia

KLEIN は RFIDSec 2011 で提案された軽量暗号で、KLEIN-64/80/96 の 3 種類がある。従来の攻撃では、高位ニブルと低ニブルの間の拡散が遅いことを利用した。本論文では、ニブル混合(MixNibbles)に注目して鍵候補を絞り込む改良を行った。攻撃は truncated 差分攻撃であるが、差分経路の取り方によってトレードオフがあるので、それらを下表に示す。

暗号名	攻撃段数/仕様	データ複雑度	時間複雑度	メモリ複雑度
KLEIN-64	12/12	$2^{54.5}$	2^{57}	2^{16}
KLEIN-64	12/12	2^{35}	$2^{63.8}$	2^{32}
KLEIN-80	13/16	$2^{60.49}$	$2^{71.1}$	2^{16}
KLEIN-80	13/16	2^{41}	2^{78}	2^{32}
KLEIN-96	14/20	2^{47}	2^{92}	2^{32}
KLEIN-96	14/20	2^{58}	$2^{89.2}$	2^{16}

Branching Heuristics in Differential Collision Search with Applications to SHA-512 [FSE 2014]
Maria Eichlseder, Florian Mendel and Martin Schlaffer

SHA-512 に対する semi-free-start での攻撃可能段数を従来 24 段(仕様では 80 段)から 38 段に拡張した。本論文では、自動化した差分の衝突探索が利用されている。

Collision Attack on 5 Rounds of Grøstl [FSE 2014]
Florian Mendel, Vincent Rijmen and Martin Schlaffer

GrøstlはKnudsenらによって設計されたSHA-3最終5候補の一つである。本論で取り上げるGrøstl-256とGrøstl-512は各々、10段と14段であり、従来ともに3段縮小版までしか攻撃されていなかった。本論文では、差分が複数のメッセージブロックに広がること許容しつつ、計算量削減のため通過する置換は2個のうち1つに限定した結果、両方とも衝突発見可能段数を5段に伸ばした。攻撃は、Grøstl-256では、時間複雑度が 2^{123}、メモリ複雑度が 2^{64}。Grøstl-512では、時間複雑度が 2^{176}、メモリ複雑度が 2^{64}。

1.5.3. FSE 2014 の発表(3 日目)

Differential Cryptanalysis of round-reduced SIMON and SPECK [FSE 2014]
Farzaneh Abed, Eik List, Jakob Wenzel and Stefan Lucks

SIMON と SPECK は 2013 年 6 月に NSA が公開した軽量ブロック暗号で、ソフト実装・ハード実装の両方で高い実装性能を示すように設計されている。本論文では、各ブロッ長、鍵長の組み合わせに対し、差分攻撃と長方形(Rectangle)攻撃を適用した結果が発表された。結果を下表に示す。

SIMON に対する差分攻撃

暗号	攻撃段数/仕様	時間複雑度	データ複雑度	メモリ複雑度	成功率
SIMON32/64	18/32	$2^{46.0}$	$2^{31.2}$	$2^{15.0}$	0.63
SIMON48/72	19/36	$2^{52.0}$	$2^{46.0}$	$2^{20.0}$	0.98
SIMON64/96	26/42	$2^{63.9}$	$2^{63.0}$	$2^{31.0}$	0.86
SIMON96/96	35/52	$2^{93.3}$	$2^{93.2}$	$2^{37.8}$	0.63
SIMON128/128	46/68	$2^{125.7}$	$2^{125.6}$	$2^{40.6}$	0.63

SPECK に対する差分攻撃

暗号	攻撃段数/仕様	時間複雑度	データ複雑度	メモリ複雑度	成功率
SPECK32/64	10/22	$2^{29.2}$	2^{29}	2^{16}	0.99
SPECK48/72	12/22	$2^{45.3}$	2^{45}	2^{24}	0.99
SPECK64/96	15/26	$2^{61.1}$	2^{61}	2^{32}	0.99
SPECK96/96	15/28	$2^{89.1}$	2^{89}	2^{48}	0.99
SPECK128/128	16/32	$2^{111.1}$	2^{116}	2^{64}	0.99

SPECK に対する長方形攻撃

暗号	攻撃段数/仕様	時間複雑度	データ複雑度	メモリ複雑度	成功率
SPECK32/64	11/22	$2^{46.7}$	$2^{30.1}$	$2^{37.1}$	～1
SPECK48/72	12/22	$2^{58.8}$	$2^{43.2}$	$2^{45.8}$	～1
SPECK64/96	14/26	$2^{89.4}$	$2^{63.6}$	$2^{65.6}$	～1
SPECK96/144	16/29	$2^{135.9}$	$2^{90.9}$	$2^{94.5}$	～1
SPECK128/192	18/33	$2^{182.7}$	$2^{125.9}$	$2^{121.9}$	～1

Differential Analysis of Block Ciphers SIMON and SPECK [FSE 2014]

Alex Biryukov, Arnab Roy and Vesselin Velichkov

ブロック暗号の差分解読において ARX 型一般に適用可能な差分経路探索法を開発した。この探索法では、探索打ち切りの閾値に新規開発の Highway−Country road approach を利用している。NSA が設計したブロック暗号 SIMON と SPECK に適用したところ、新規の差分経路が発見でき、次に示す各ブロッ長、鍵長の組み合わせに対する解読が可能であることを理論的に示した。

暗号	鍵長	攻撃段数/仕様	時間複雑度	データ複雑度
SIMON32	64	19/32	2^{32}	2^{31}
SIMON48	72	20/36	2^{52}	2^{46}
SIMON48	96	20/36	2^{75}	2^{46}
SIMON64	96	26/42	2^{89}	2^{63}
SIMON64	128	26/44	2^{121}	2^{63}
SPECK32	64	11/22	2^{55}	2^{31}
SPECK48	72/96	12/22	2^{43}	2^{43}
SPECK64	96	16/26	2^{63}	2^{63}
SPECK64	128	16/27	2^{63}	2^{63}

Equivalent Key Recovery Attacks against HMAC and NMAC with Whirlpool Reduced to 7 Rounds [FSE 2014]

Jian Guo, Yu Sasaki, Lei Wang, Meiqin Wang and Long Wen

ハッシュ関数に Whirlpool を使用した HMAC に対する鍵回復攻撃において、実際の鍵の代りに HMAC の等価鍵を求めることにより、攻撃可能な縮小版 Whirlpool の段数(仕様では 10 段)を従来の 6 段から 7 段に伸ばした。攻撃は AES ベースのブロック暗号に対して開発された中間攻撃の手法を利用しており、必要な計算コストは、時間複雑度 $2^{482.3}$、メモリ複雑度 2^{481}、データ複雑度 $2^{481.7}$ である。

Multiple Differential Cryptanalysis of Round-Reduced PRINCE [FSE 2014]

Anne Canteaut, Thomas Fuhr, Henri Gilbert, Maria Naya-Plasencia and Jean-Rene Reinhard

PRINCE は Asiacrypt 2012 で Borghoff らが提案したブロック暗号で、ブロック長 64 ビット、鍵長 128 ビット、12 段 SP 構造である。本論文では、複数差分経路の効果を考慮した 6 段 differential を利用して、10 段縮小版に対する攻撃を示した。コストはデータ複雑度 $2^{57.9}$、時間複雑度 $2^{60.7}$、メモリ複雑度 $2^{60.5}$。この結果は 10 段縮小モデルに対する攻撃としては最善のものである。

1.6. PKC 2014 の発表

1.7.1. PKC 2014 の発表(1 日目)

Discrete logarithm in GF(2^{809}) with FFS [PKC 2014]
Razvan Barbulescu, Cyril Bouvier, Jeremie Detrey, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thome, Marion Videau, Paul Zimmermann

関数体篩法において、GPU を使用した高速化を実現するため、主要部分の高速化と篩計算と線形計算の適切なバランスを取った方法が示された。その結果、有限体 GF(2^{809})上の離散対数問題を 7.6 コア年と 0.1GPU 年で計算できるという理論結果を得た。

1.7.2. PKC 2014 の発表(3 日目)

Parallel Gauss Sieve Algorithm: Solving the SVP Challenge over a 128-Dimensional Ideal Lattice [PKC 2014]
Tsukasa Ishiguro, Shinsaku Kiyomoto, Yutaka Miyake, Tsuyoshi Takagi

最短ベクトル問題(SVP)解決のための並列化したガウス篩アルゴリズムを提案した。提案法の一般的な特徴は、サンプリングした短いベクトルと SIMD 命令の活用である。これに有限体ごとの最適化を行う。Ideal Lattice Challenge に適用したところ、世界で初めて 128 ビットの解法に成功するなどの成果が得られた。計算には 29,994CPU 時間を要した。

付録 4
暗号技術活用委員会からの質問及びその回答について

2014.2.27

暗号技術評価委員会
委員長　　今井　秀樹　殿

暗号技術活用委員会
委員長　松本　勉

Perfect Forward Secrecy に関する技術的見解について

現在、暗号技術活用委員会の傘下で活動をしている運用ガイドラインワーキンググループ（主査：菊池浩明）において、SSL/TLS サーバ構築ガイドラインを作成しています。

このたび、同ガイドラインの作成にあたり、Perfect Forward Secrecy についての重要性・有効性を踏まえた判断が必要となることから、以下の点についての技術的見解を示していただきたく、暗号技術評価委員会に回答を依頼するものです。

事情をご高察のうえ、何卒ご理解を賜りますようお願い申し上げます。

【背景】

SSL/TLS サーバ構築ガイドラインにおいて、暗号スイートの優先順位を検討しています。

暗号スイートは「鍵交換＿署名＿暗号化＿ハッシュ関数」の組によって構成されており、サーバとクライアント（主としてブラウザ）間での暗号化通信前の事前通信（ハンドシェイク）時に、両者の合意により一つの暗号スイートが選択されます。その際、暗号スイートの優先順位の上位から順に両者が合意できる暗号スイートを見つけていくのが一般的です。

暗号スイートが選択された後は、選択された暗号スイートに記載の鍵交換、署名、暗号化、ハッシュ関数の方式により SSL/TLS における各種処理が行われます。

運用ガイドラインワーキンググループでは、暗号スイートの優先順位を検討するに当たり、「鍵交換」方式である、(EC)DHE、(EC)DH、RSAES-PKCS#1 v1.5 については、Perfect Forward Secrecy の観点を一つの判断基準にしようと考えています。これは、NIST SP800-52 revision 1 (Draft)[1]において、

> Cipher suites using ephemeral DH and ephemeral ECDH (i.e., those with DHE or ECDHE in the second mnemonic) provide **perfect forward secrecy, ensuring long-term confidentiality of the session**. While support of these cipher suites is not required by these guidelines, it is strongly recommended.

との記述があるためです。なお、同文書内では、

[1] http://csrc.nist.gov/publications/drafts/800-52-rev1/draft_sp800_52_r1.pdf

Perfect forward secrecy is the condition in which the compromise of a long-term private key used in deriving a session key subsequent to the derivation does not cause the compromise of the session key.

と注釈をつけています。

【回答依頼内容】

NIST SP800-52 revision 1 (Draft)記載の内容に関連して、運用ガイドラインワーキンググループとしては以下の技術的な確認をいたしたく、回答を依頼するものです。

1. （SSL/TLS における）Perfect Forward Secrecy と Forward Secrecy の定義（概念）及びその効果についての説明。特に、Perfect Forward Secrecy と Forward Secrecy に違いがあるのであれば、その違いはどのようなものであり、またどの程度の重要性の違いがあるか

2. Perfect Forward Secrecy と Forward Secrecy と ephemeral 特性をもつ DH/ECDH（つまり、DHE, ECDHE）との関係

3. Perfect Forward Secrecy と Forward Secrecy と ephemeral 特性をもたない DH/ECDH（つまり、DH, ECDH）との関係

4. Perfect Forward Secrecy と Forward Secrecy と RSAES PKCS#1 v1.5 との関係

回答希望日：2014 年 3 月 10 日

以上

２０１４年3月１２日

暗号技術活用委員会
委員長　松本 勉　殿

暗号技術評価委員会
委員長　今井 秀樹

Perfect Forward Secrecy に関する技術的見解について（回答）

２０１４年２月２７日付けで照会がありました標記の件について、第３回暗号技術評価委員会（２０１４年３月６日開催）における事務局からの要請に基づき、回答依頼内容の項番１についてのみ、下記の通り回答します。

記

１．（SSL/TLS における）Perfect Forward Secrecy と Forward Secrecy の定義（概念）及びその効果についての説明。特に、Perfect Forward Secrecy と Forward Secrecy に違いがあるのであれば、その違いはどのようなものであり、またどの程度の重要性の違いがあるか

Perfect Forward SecrecyとForward Secrecyについては、概ね、鍵共有プロトコルにおいて、長期的に使う鍵(long-term key)が危殆化(compromise)しても、それ以前に導出される一時的に使う鍵(session key)が危殆化しないという意味で用いられているものの、IETF RFC 4949 [10]に記載の通り、統一的見解はない。

（参考文献）

[1] M. Bellare, D. Pointcheval, P. Rogaway. Authenticated key exchange secure against dictionary attacks. EUROCRYPT ’00.
[2] S. Blake-Wilson, A. Menezes, Authenticated Diffie-Hellman Key agreement protocols, SAC ’98, LNCS 1355.
[3] S. Blake-Wilson, D. Johnson, A. Menezes, Key agreement protocols and their security analysis, Crytography and Coding 1997, LNCS 1355.
[4] R. Canetti, H. Krawczyk, Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels, EUROCRYPT 2001.
[5] Certicom Research, SEC 1: Elliptic Curve Cryptography Version 2.0, May 21, 2009.
[6] W. Diffie, P. van Oorschot, M. Wiener, Authentication and Authenticated Key Exchange, Design, Codes and Cryptography 2, 1992, 107-125.
[7] C. Günther, An identity-based key-exchange protocol, Eurocrypt ’89, LNCS 434, 1990.
[8] T. Jager, F. Kohlar, S. Schäge, J. Schwenk, On the Security of TLS-DHE in the Standard Model. CRYPTO 2012.
[9] T. Polk, S. Chokhani K. McKay, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, NIST Special Publication 800-52 Revision 1 (Draft), Sep.2013.
[10] R. Shirey, Internet Security Glossary, Version 2, Request for Comments: 4949, August 2007.

[11] P. Rogaway, M. Bellare, D. Boneh, Evaluation of Security Level of Cryptography ECDHS (from SEC 1), January 16 2001. (CRYPTREC Technical Report No.1067)

以上

CRYPTREC 暗号技術ガイドライン
(SSL/TLS における近年の攻撃への対応)

平成 26 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

目次

1. 序章

1.1 本ガイドラインの目的

SSL/TLS について、近年、プロトコルの仕組みの脆弱性やソフトウェアの脆弱性を複合的に利用する攻撃がいくつか公開されている。また、プロトコル内で用いる暗号として RC4 を選択することができるが、RC4 は運用監視暗号リストに位置づけられており、安全性に係る問題のある暗号技術として、互換性維持以外の目的での利用が推奨されていない。さらに、RC4 に対する攻撃が適用できる環境下では SSL/TLS の安全性が保てなくなることが示されている。このような状況を踏まえ、本ガイドラインでは、近年示されている攻撃の解説を行うとともに、SSL/TLS を安全に利用するため近年注目されている攻撃に対して推奨される対応を示すことを目的としている。

本文では、プロトコルの仕組みを利用した攻撃として、BEAST、TIME、CRIME、Lucky Thirteen などについて解説するとともに推奨される対応策を示す。また、プロトコル内で用いる暗号として RC4 を用いた場合の実際の攻撃方法、事例を示す。この場合は攻撃を回避する効果的な対応策がないため、RC4 を選択しない利用方法の推奨などを述べている。

1.2 総論

SSL/TLS に関して、 (1) プロトコルの仕組みを利用した攻撃に起因する脆弱性と、 (2) プロトコル内で用いる暗号として RC4 を用いた場合に、RC4 のアルゴリズムの弱さに起因する脆弱性とが指摘されている。

(1) に分類される脆弱性：BEAST は、プロトコルで CBC モードを用いた場合に CBC モードの脆弱性として知られる特性を利用した攻撃である。具体的には、特定のブロックの平文を意図した値に差し替えられる攻撃者が、別のブロックの解読が容易になるという脆弱な性質を利用しており、 SSL/TLS のプロトコルの仕様との複合的事象として、Java アプレット実行環境が脆弱なブラウザにおいて攻撃が発生することが指摘されている。ただし、プロトコルそのものを変更しなくても平文を 1 対 (N-1) の分割を行うことで回避できる可能性が示されている。また、Java アプレットのパッチを当てることでも回避することができるとされている。これらの状況から、この攻撃をもって、 SSL/TLS において、ブロック暗号を利用しないという結論には至らない。 CRIME、TIME、BREACH、Lucky Thirteen は、圧縮データのサイズの差異や、実行時間の差異を利用して暗号解読の攻撃を行う、いわゆる実装攻撃に属する攻撃であるが、これらの攻撃は、一般の実装攻撃への対策と同様の考え方で、圧縮機能の無効化、データや実行時間の平準化やランダム化などの回避策が示されている。その他、圧縮機能を無効化せずに，回避する方法も検討されはじめている。 これらの攻撃を鑑みても SSL/TLS において、ブロック暗号を利用しないという結論には至らない。

(2) に分類される脆弱性： RC4 は、同じデータに対して異なる鍵を用いて生成された暗

号文を複数入手できる Broadcast Setting や同じデータをセッションごとに同じ位置で、異なる鍵で暗号化して送信する Multi-Session Setting の環境が攻撃者に与えられた場合、効率的に攻撃が実現できることが知られている。 SSL/TLS で用いる暗号として RC4 を選択した場合、攻撃者に効率的に RC4 に対する攻撃が適用できる環境を提供してしまうことになる。近年の解析結果では、現実的なコスト、および起こりうる確率で平文が回復できることが示されている。(一例としては、同じメッセージに対して 2^{34} の暗号文が集められた場合、メッセージの先頭から約 1000 T byte を非常に高い確率（0.97）で復元可能であることが示されている［1]）。RC4 の攻撃を適用できる環境として利用されている Broadcast Setting は、BEAST、TIME、CRIME 等の攻撃の中でも利用されており、この攻撃のみで想定している特殊な環境ではない。また、 HTTPS + basic 認証（例：ネットワーク利用者認証、グループ利用の Web ページ）を利用する際に攻撃者に繰り返し re-negotiation をさせられてしまう場合や JavaScript のバグを攻撃者が悪用し、攻撃者のサーバに大量の暗号文を送らされてしまう場合等には、比較的容易に整えられる環境であり、PC 版の Internet Explorer、 Firefox、 Opera、 Safari などのブラウザに対してブロードキャスト状態にするのは十分に実行可能な設定条件であるといえる。ゆえに、RC4 を用いた場合の解析結果は現実的な脅威として配慮すべきである。

SSL/TLS にはいくつかのバージョンが存在する。推奨される設定として、TLS 1.0 より古いバージョンについては、新しいバージョンへアップデートすることが推奨される。TLS 1.0 については、CBC モードを用いた場合の脆弱性に対してパッチが提供されているため、Java 等のソフトウェアを最新版に更新した上で、CBC モードを選択することが推奨される。TLS 1.1 については、CBC モードを用いた場合の脆弱性が解消されていることから、CBC モードを選択することが推奨される。TLS1.2 については、CBC モード、CCM モード、GCM モードが選択できるため、それらを使うことが推奨される。

1.3 本ガイドラインの構成

2 章に、本文中で取り扱っている技術説明/用語説明を記す。3 章に、プロトコルの仕組みを利用した攻撃を記す。4 章に、RC4 の脆弱性に基づく攻撃を記す。

1.4 注意事項

本ガイドラインは状況の変化に伴い、改訂される場合がある。

2. 技術説明 / 用語説明

SSL/TLS

SSL（Secure Socket Layer）、TLS（Transport Layer Security）は、ネットワーク上のアプリケーションに対して通信相手の認証と暗号化された通信を提供するプロトコル。SSL は Netscape Communications 社が開発し、その仕様を引き継ぐ形で IETF において TLS として標準化されている。

https

アプリケーションにおいて、SSL/TLS を用いて通信を行う際に使われる URI のスキームのこと。

Deflate

可逆データ圧縮アルゴリズムである。SSL などのプロトコル内の圧縮で使われるケースでは 16KB ごとの境界が存在するため、攻撃対象の Cookie の値がちょうどこの境界上に来るようにパディングのサイズを調節することによる 1 バイトずつのブルートフォース攻撃などに利用される。

Cookie

HTTP プロトコルで通信する、ウェブブラウザとウェブクライアントの間で、主に状態管理のために情報を保存するために使われるプロトコル、およびこのプロトコルによって保存される情報そのもの。

3. プロトコルの仕組みを利用した攻撃

3.1 CBC モードの構成を利用した攻撃：BEAST

BEAST [2] は 2011 年に開発された攻撃ツールであり、SSL3.0/TLS1.0 の CBC モードの脆弱性を利用して選択平文攻撃を行い、Cookie（平文）を得る。BEAST の概要は公開されているが、ツールは非公開のため、詳細については不明な部分が多く、以降の説明には一部推測が含まれる。

まず、図 1　に、SSL3.0/TLS1.0 における CBC モードの処理概要を示す。

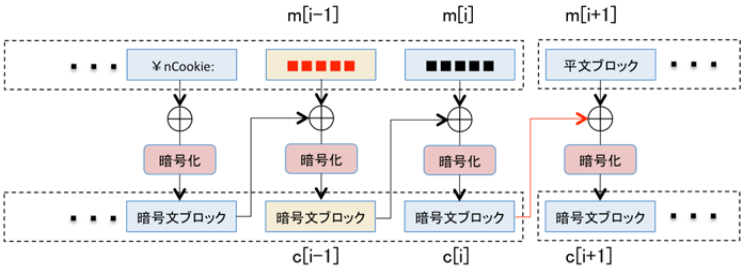


図 1　SSL3.0/TLS1.0 における CBC の概要

ここでのポイントは、初期化ベクトルとして直前の最終暗号文ブロック c[i] を使用している点である。これにより、一つ前の平文ブロック m[i-1]（Cookie に対応）に対して以下の選択平文攻撃が可能となる。

1. 攻撃者は平文 m[i-1] の推測 M[i-1] を生成
2. 次の平文の最初のブロックとして M[i+1]=M[i-1] XOR c[i-1] XOR c[i] を設定
3. 対応する暗号文 C[i+1] と c[i-1] を比較
4. 異なっていれば、1 からやり直し、なお、

C[i+1]=E(M[i+1] XOR c[i])
=E(M[i-1] XOR c[i-1])
=E(m[i-1] XOR c[i-1]), if M[i-1]=m[i-1]
=c[i-1]

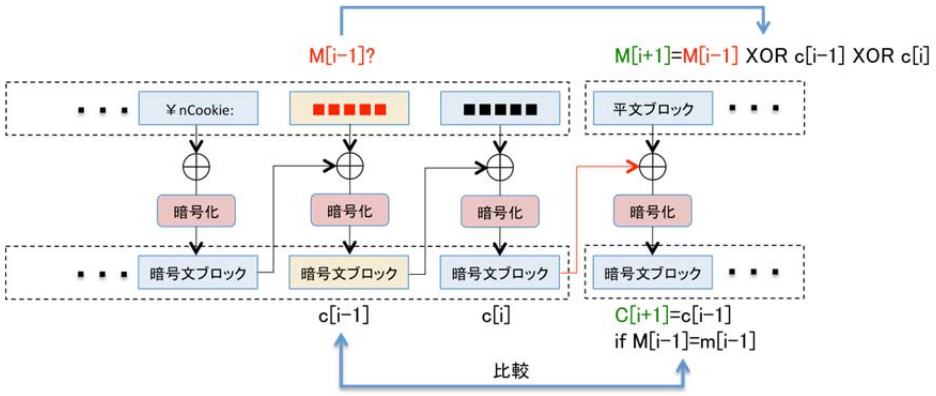


図 2　SSL3.0/TLS1.0 への平文選択攻撃

図 2 の攻撃では、平文ブロックをブロック全体で全数探索しており、特定に（最大）2^{128} 回の平文選択が必要となり脅威は小さい。

それに対して BEAST では攻撃の効率向上のため、ブロック単位ではなくバイト単位で全数探索することで、特定に必要な平文選択を $2^8 \times 16$ と大幅に削減した。具体的には、アクセス先の URL を変更し、図 3 に示すように Cookie の 1 バイト目が平文ブロックの最後となるようにした上で、選択平文攻撃でこの 1 バイトを特定する。そしてさらに、URL を 1 バイト短くすることで、Cookie の 2 バイト目がブロックの最後となるようにし、同様に処理を繰り返し、バイト単位で特定する。これにより、攻撃の効率が飛躍的に向上し、実際に適用可能となった。

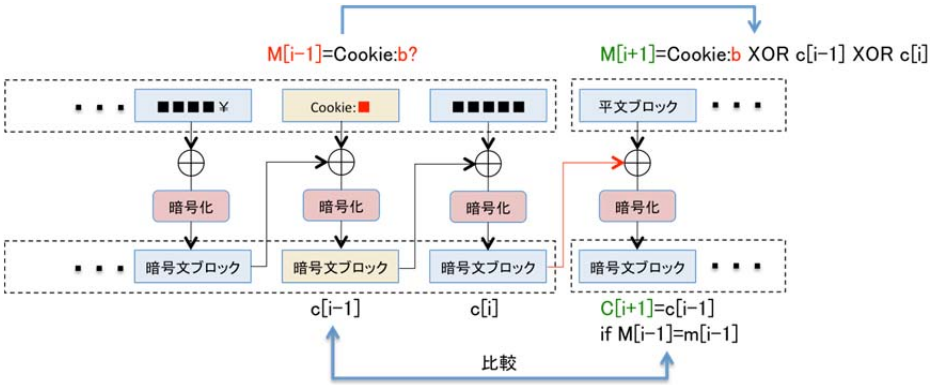


図 3　BEAST におけるバイト単位の平文選択攻撃

BEAST への対策には、TLS1.0 で実施可能な対策と、TLS1.1 以降への移行で実施可能となる対策の 2 種類がある。前者の対策として、セキュリティパッチの適用が挙げられる。現時点のセキュリティパッチ [3]（1/n-1 レコード分割，1/n-1 Record Splitting Patch と呼ばれる）については、その安全性が [4]で評価されており、ある条件下で BEAST 系の平文選択攻撃に対して識別不能性を満たすことが証明されている。ここで条件には、CBC モードでの暗号化の前に平文に付け加えられる MAC（後述の 3.3 節の図 6 参照）の長さがブロ

ック長より短いことが含まれる。よって、ブロック長より長い MAC を生成する Truncated HMAC（RFC6066 [5]）を使う場合には、必ずしも安全性が保証されるわけではないため、注意が必要である。一方、後者の TLS1.1 以降で実施可能な対策として、改良された CBC モード（初期化ベクトルに直前のブロックは使わず、リフレッシュする）の使用が挙げられ、さらに TLS1.2 以降であれば、新たに追加された認証付き秘匿モード(GCM モード、CCM モード)の使用も対策となる。なお、BEAST のデモでは、実装に Java アプレットが使用されているが、その理由は Java アプレットの脆弱性を使用するためと言われている。よって、上述のいずれの対策でも、Java を最新に保つことが不可欠となる。

短期的な対策として共通鍵ブロック暗号の代わりにストリーム暗号 RC4 を使うことが挙げられるが、RC4 の脆弱性が数多く報告されており、長期的な対策としては推奨できない。

3.2 圧縮処理部分の観測に基づく攻撃

3.2.1 CRIME

CRIME（Compression Ratio Info-Leak Mass Exploitation） [6] は、2012 年のセキュリティカンファレンス Ekoparty において、Rizzo と Duong によって発表された攻撃である。SSL/TLS において、入力データに対する圧縮後のパケット長の違いから平文である Cookie を解読する攻撃である。一般的にデータ圧縮の技術では、頻度が高いデータが多いほど圧縮後のデータ長は短くなる。この性質を利用し、圧縮後のメッセージの長さを参照しながら解読を行う。解読の例を図 4 に示す。

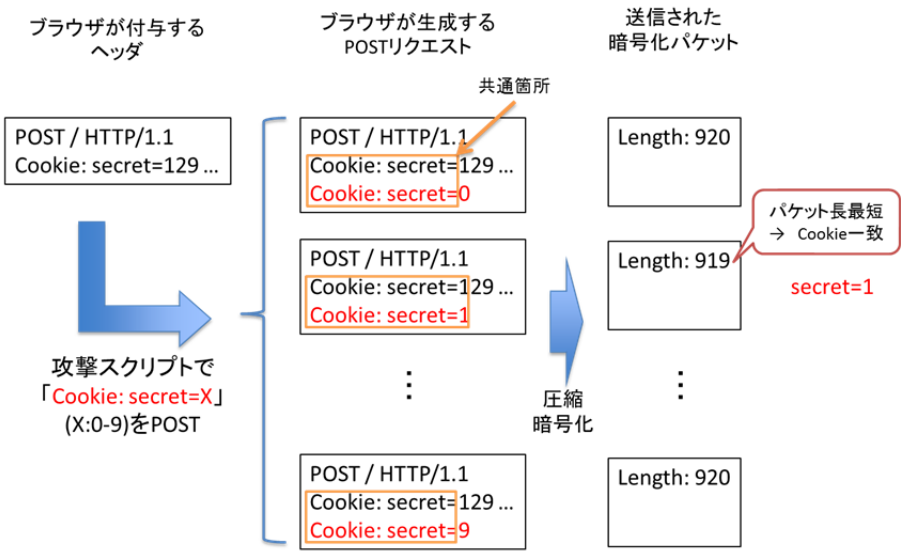


図 4 CRIME の攻撃の流れ

この例では、 Cookie の中に、secret という属性値がセットされているが、攻撃スクリ

プトを利用し、secret=X という形で X を 0 から 9 に変化させたデータを SSL/TLS のデータとして送る。その結果として圧縮されたデータのパケット長から、secret の値を類推することができる。

この攻撃は、SSL/TLS において使われているデータ圧縮の機能に依存するものであり、SSL/TLS の圧縮機能を使わないことで対応できる。Web ブラウザの Internet Explorer ではもともと圧縮機能に対応していなかったため本攻撃は適用が出来なかった。また、Google Chrome ではバージョン 21.0.1180.89、Firefox ではバージョン 15.0.1、Opera では 12.01、Safari ではバージョン 5.1.7（Windows）、5.1.6（MacOS）で圧縮機能が無効化されており、これら以降のバージョンでは本攻撃の影響はない。

また、 Web サーバソフトウエアの Apache2.2 with MOD_SSL ではデフォルトで圧縮機能を利用しており機能の無効化の設定はないが、 Apache2.4 with MOD_SSL ではデフォルトで圧縮機能を利用しているものの無効化も可能となっている。また、Microsoft IIS (Internet Information Services) ではもともとすべてのバージョンで圧縮機能が存在せず、Amazon ELB (Elastic Load Balancing) ではデフォルトで圧縮機能は無効となっている。

3.2.2 TIME

TIME（Time Info-leak Made Easy） [7] は 2013 年に Liu らによって発表された攻撃で、 CRIME と同様に、 SSL/TLS の圧縮機能を用いて Cookie などの値を解読する攻撃である。図 5 に攻撃の流れを示す。 CRIME がデータ長を推定に利用したことに対して、TIME ではブラウザにおいての処理時間の差によって攻撃に必要な情報を収集するため、攻撃者による中間者攻撃が必要であった CRIME に比べて、攻撃の実現性が高いことが特徴である。TIME では、HTTP レスポンスの圧縮結果を用いていることが攻撃の原因となっており、圧縮機能の無効化が攻撃を回避する有効な方法である。しかし、現実のアプリケーションにおいては性能上要件により圧縮機能の無効化が受け入れられない場合があり、このような場合においては HTTP レスポンスの圧縮を無効化という対策を講じることは難しいのが現状である。

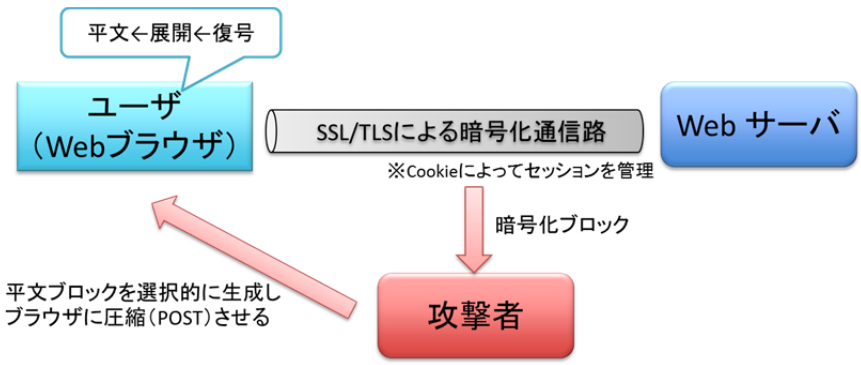


図 5 TIME の攻撃の流れ

3.2.3 BREACH

BREACH [8] は、2013 年に行われた BlackHat において Prado らによって発表された攻撃である。基本的な考え方は、 CRIME と同様に HTTP リクエストメッセージをコントロールして、圧縮データのデータ長の違いにより暗号文を解読する攻撃である。CRIME との違いは、 http レスポンスに含まれる情報を奪うことと、 SSL/TLS のデータ圧縮機能を用いるのではなく、アプリケーション層における圧縮機能、例えば Web アプリケーションによる gzip を用いた圧縮においても攻撃が成功するため、SSL/TLS の設定変更では対策にならないという点である。一方で、攻撃成功の条件は限定的であり、gzip 圧縮の他に、レスポンスの平文にリクエストの情報そのものと、レスポンス自体に CRSF Token などの秘密情報が含まれることが必要である。前述の通り、SSL/TLS の設定変更では対処できないため、 SSL/TLS を用いるアプリケーションでの対応が必要となる。

3.3 MAC-then-Encryption の構成を利用した攻撃：Lucky Thirteen

Lucky Thirteen [9] は 2013 年に発見された TLS が使用する HMAC 付き CBC モード(MAC-then-Encrypt、以下 MEE-CBC-TLS) の脆弱性を利用した中間者攻撃であり、攻撃者は復号処理の処理時間差(ハッシュ関数の計算回数の違い)を特定することで平文を得る。図 6 に、TLS における MEE-CBC-TLS の処理概要を示す。

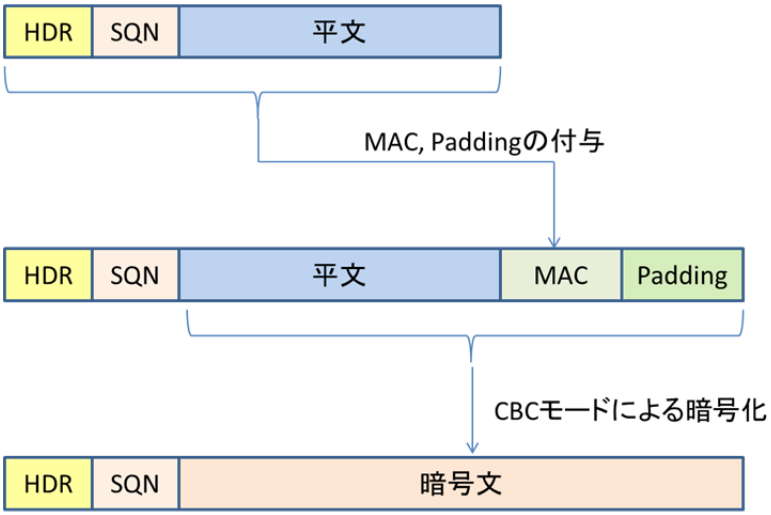


図 6 TLS における MEE-CBC-TLS の概要

ここで MAC の生成に HMAC-SHA1 を用いる場合、ハッシュ対象のデータ長により MAC の生成に用いる SHA-1 の実行回数が異なることが知られている。 SHA-1 の処理回数は[((64+M) +1+8)/64]で表現されるため、具体的には M mod 64 が 55 か 56 になるかで SHA-1 実行回数が変化する。

実際の攻撃は次の通りである。

1. 暗号文を入手する
2. MAC エラーが発生するような攻撃用の暗号文を用意し、サーバに送付する
3. 意図的に MAC エラーを発生させ、エラー発生のタイミング（SHA-1 実行回数の変化）から平文を得る
4. エラー発生箇所を変更し、2、3 を繰り返す

図 6 に示す通り、MAC の対象は平文にヘッダ（HDR）5 byte とシーケンス番号（SQN）8 byte の合計 13 byte を加えたデータとなるため、この 13 byte を加えた平文ブロックのデータ長を変化させる。

また、実際に攻撃を行うためには、攻撃者はネットワーク越しに MEE-CBC-TLS 復号の処理時間差を厳密に測定する必要があるため、実際に攻撃を適用することは難しい。Lucky Thirteen の提案者は、 OpenSSL 及び GnuTLS を使用しているサーバに対して同一セグメント内からの攻撃に成功した実験結果を示している。

Lucky Thirteen に対する対策としては、認証付き暗号利用モード(GCM モード、CCM モード）を利用することである。これは TLS 1.2 以降でサポートされている。

3.4 Renegotiation を利用した攻撃

3.4.1 攻撃方法

Renegotiation を利用した攻撃とは、2009 年に発見された SSL/TLS のハンドシェイクにおいて確立された暗号アルゴリズムと鍵長を更新(Renegotiation)する際の脆弱性を利用した中間者攻撃である [10]。

Renegotiation は、SSL/TLS が確立され暗号通信を行っているセッションを更新して、新たにセッションを確立させる手法である。Renegotiation の概要を図 7 に示す。Renegotiation は最初のハンドシェイクにおいて確立された暗号チャネルを使用して、新規にハンドシェイクを行うことで実施されるため、新たに確立された暗号チャネルが既存の暗号チャネルに置き換わる。なお、---は平文データ、===は暗号化データを示す。

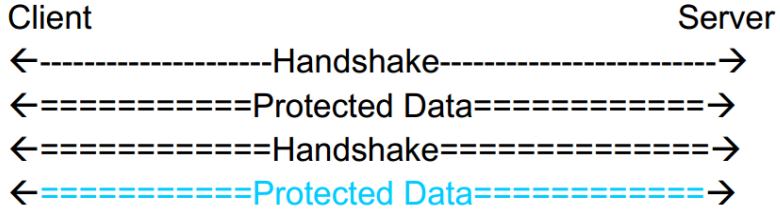


図 7 Renegotiation の概要（[11]より引用）

実際の攻撃は次の通りである。

1. 攻撃者はクライアントのハンドシェイクを受信し、パケットを保持しておく
2. 攻撃者とサーバの間で通常のハンドシェイクを行い、サーバと暗号通信を行う
3. 攻撃者は Renegotiation を要求し、クライアントとサーバの間でのハンドシェイクに対して、1 で保持していたパケットをサーバに送信する

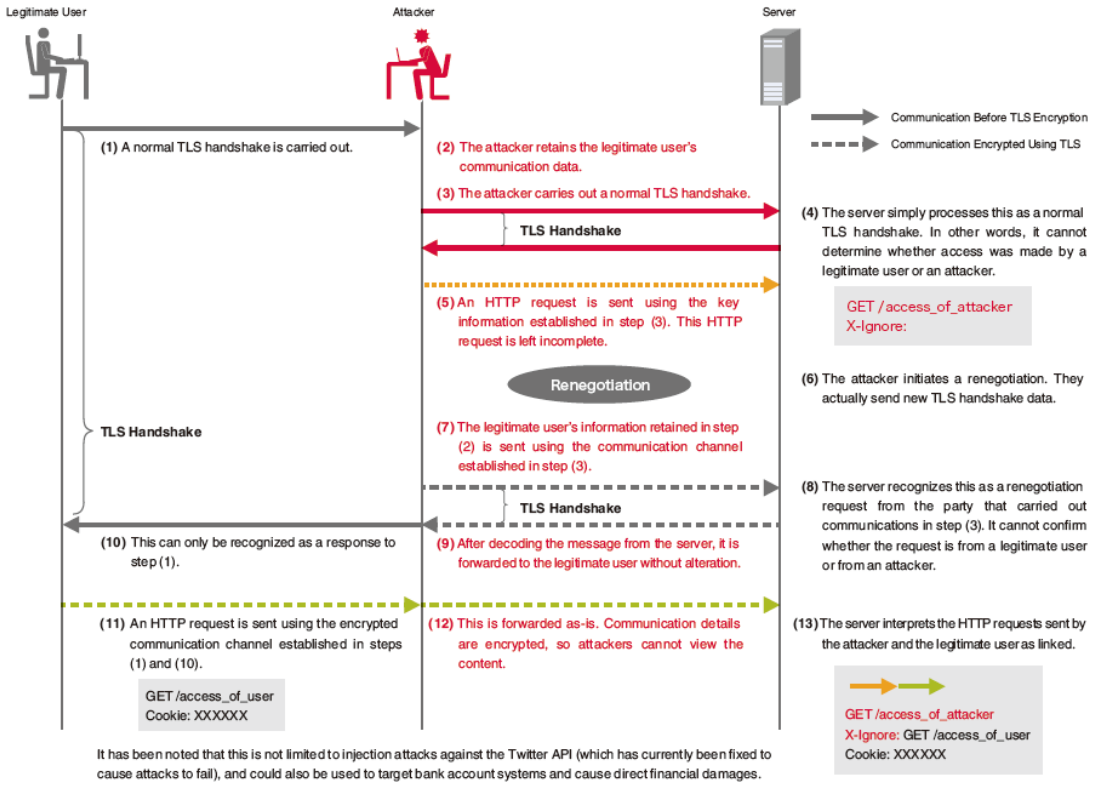


図 8 Renegotiation 攻撃の概要（[12]より引用）

図 8 に示すように、Renegotiation されたデータは暗号化されているため、攻撃者が内容を参照することはできないが、サーバはクライアントからのパケットと攻撃者からのパケットを区別することができない。具体的な攻撃としては、サーバ認証のハンドシェイクをクライアント認証(相互認証)に切り替える例が考えられている。

3.4.2 対策方法：RFC5746

Renegotiation の対策として RFC5746 が提案されている。 RFC5746 では TLS 1.2 で定義されている TLS connection state に対して、secure_renegotiation フラグの追加と、client_verify_data と server_verify_data が追加されている。

追加された内容の詳細は次の通りである。これにより、 Renegotiation を安全に行う実

装がなされていることをサーバとクライアントの間で共有することが可能となる。

① secure_renegotiation フラグ：セキュアな Renegotiation が使用されているかを示す
② client_verify_data：直前のハンドシェイクにおいてクライアントから送信された Finished メッセージ
③ server_verify_data：直前のハンドシェイクにおいてサーバから送信された Finished メッセージ

また、 SSLv3、 TLS 1.0/TLS 1.1 に対して本対策は適用できないため、 RFC5746 では Cipher Suite に TLS_EMPTY_RENEGOTIATION_INFO_SCSV を追加することでハンドシェイクを中断する方法も提案されている。

なお、これらの実装が行われていない Renegotiation が行われた場合に、正しい相手からのリクエストであるかを安全に確認する手段がないため、この実装が行われていない Renegotiation を拒否することが推奨されている。

4. RC4 の脆弱性に基づく攻撃

4.1 RC4 に対する攻撃

本節では、ストリーム暗号 RC4 において現在までに指摘されている脆弱性について示す。

RC4 は、1987 年に Ronald Rivest によって開発されたストリーム暗号である。1 バイトから 256 バイトの鍵から、鍵スケジューリングアルゴリズム（KSA）により 256 バイトの内部状態を作り出し、内部状態からキーストリーム生成アルゴリズムにより 1 バイト単位のキーストリームを出力する。内部の処理はバイト単位であり、鍵は 1 バイトから 256 バイトの可変長（推奨値は 16 バイト）、内部状態は 256 バイトの配列と、2 つのインデックスからなる。

ストリーム暗号の安全性評価としては、以下の 4 つの攻撃を想定する。

1) 鍵回復攻撃:出力されたキーストリームから、ストリーム暗号に対する入力鍵（の一部）を求める攻撃
2) 内部状態復元攻撃：出力されたキーストリームから、内部状態を推定する攻撃
3) 出力予測攻撃：出力されたキーストリームから、将来出力されるキーストリームを予測する攻撃
4) 識別攻撃：出力されたキーストリームと真性乱数を 1/2 以上の無視できない確率で識別する攻撃

これらの攻撃に対し、それぞれ、入力の鍵長を x とした場合、2^x 以下の計算量で推定ができれば攻撃成功となる

鍵回復攻撃においては、入力の鍵長を推奨値である 128 ビットにした場合、FSE2013 において発表された Sepehrdad らの攻撃により無線 LAN の暗号・認証プロトコルである WEP において、19,800 パケットを収集することで鍵回復攻撃が成立することが示されている。また、弱鍵の性質を用いる Weak Key Attack については、長尾らの攻撃 [13] [14] [15] により、$2^{96.36}$ の計算量、$2^{-18.75}$ の確率で鍵回復攻撃が成立することが示されている。

内部状態回復攻撃においては、 CRYPTO2008 における Maximov らの発表により、2^{241} の計算量で内部状態の復元を行うことが示されている。このため、 RC4 においては、鍵長を 241 ビットよりも長くしても安全性は向上しないことが示されている。

出力予測攻撃においては、 EUROCRYPT2005 の Mantin らの攻撃により、2^{45} バイトのキーストリームから、85%の確率で 1 ビットの出力を予測できることが示されている。

識別攻撃においては、同じく EUROCRYPT2005 の Mantin らの攻撃により、$2^{26.5}$ バイトのキーストリームを用いることで、真性乱数との識別ができることが示されている。

また、複数の鍵を用いた場合、 FSE2001 の Mantin らの攻撃により、2^8 バイトのキーストリームを用いることで真性乱数との識別ができることが示されている。このような攻撃は、4.2 に示すように攻撃環境が整った場合には、RC4 に対する攻撃を適用することに

より SSL/TLS のメッセージに対する平文回復攻撃が可能となることが示されている。

4.2 RC4 の攻撃を SSL/TLS に適用した場合の攻撃事例

4.1. に記載のとおり RC4 のアルゴリズム自体の脆弱性は多く示されている。SSL/TLS の中で RC4 を選択した場合、その脆弱性を利用した攻撃が示されている。RC4 の攻撃が適用できる条件として、同じデータに対して異なる鍵を用いて生成された暗号文を複数入手できるような環境下を想定している。そのような環境は比較的容易に得られることが出来る。一例として、図 9 に示すような Broadcast Setting と呼ばれる環境が相当する。Broadcast Setting は、複数のユーザが同じファイルを取得する場合や同じファイル(=平文) を繰り返し送信するような場合に得られる環境である。例えば、ネットワーク利用者の認証やグループ利用の Web ページへのログインなどのように、https の中で basic 認証を行うケースなどで Broadcast Setting の環境は整えることができてしまう。また、OS イメージの配布などの場合でも、Broadcast Setting の環境は準備可能である。その他、図 10 に示す Multi-Session Setting と呼ばれる SSL/TLS で通信を行う際に異なるセッションで同じデータを同じポジションで送信する場合(攻撃対象となるデータ以外の平文は毎回任意のデータで構わない)なども RC4 の攻撃が適用できる条件を満たす。この場合、攻撃対象となるのは、例えば cookie やパスワードといった情報になる。このように RC4 の攻撃が適用できる条件は特殊な利用環境というわけではなく、一般的に存在しうる環境であるといえる。

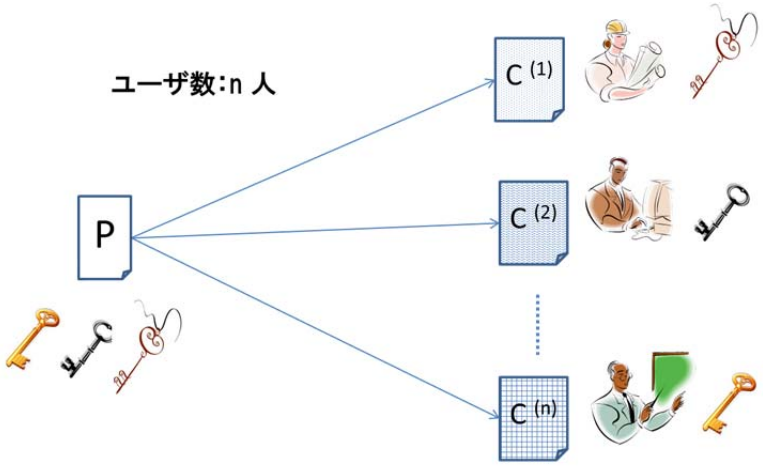


図 9 Broadcast Setting

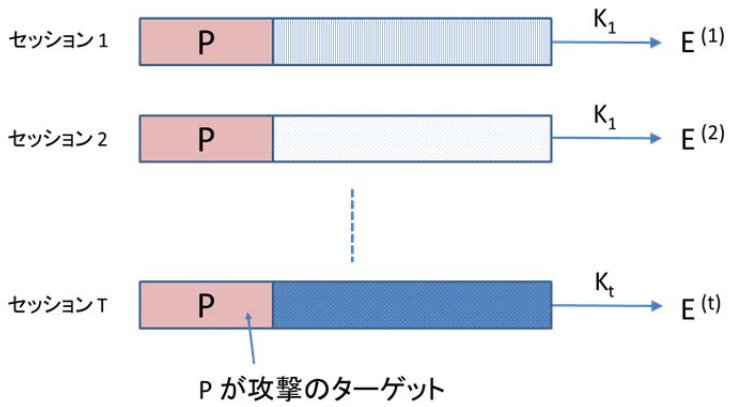


図 10 Multi-Session Setting

近年の結果として [1] [16] では、RC4 の解析を行いキーストリームにおける新しい bias が発見され、それが解析に有効であることを具体的に示されており、RC4 の攻撃が適用できる環境下で、先頭 1000 T バイトの平文を 2^{34} 個の暗号文から 0.97 以上の確率で復元できてしまうことが示されている。さらに [17]では、平文となり得る候補が絞れる場合は、より効率的に解析が行えることが示されている。例えば，平文が PIN code などの場合、入力に使われる文字の種類は 10 種類に限られる。この場合、平文の先頭 257 バイトを 2^{23} の暗号文からランダムに推定する場合よりも高い確率で平文を回復することができる。SSL/TLS の場合、先頭 36 バイトはセッションごとに変化するため、RC4 の解析により、先頭 257 バイトのうち 221 バイトが復元可能となり、入力の種類が限られる場合、より現実的な脅威となることが示されている。

RC4 の攻撃に関しては、 [18] にまとめられている。近年示された強力な攻撃の結果としては、2^{32} の暗号文が集まれば平文の初期 257 byte の任意 byte を確率 0.5 以上で推定

が可能であることが示されている [1] [16]。この結果を鑑みても、SSL/TLS で RC4 を用いる場合のリスクがより高くなっているといえる。

[1] [16] などで示されている解析は、RC4 のキーストリームの先頭の n バイト（推奨 n = 768、理想的には n = 3072）を捨てることにより回避することができる。しかしこのような対応をした場合であっても、回避できない攻撃があることが [19] により示されている。具体的には平文の一部(連続した 6 バイト程度) が知られてしまっている場合、同じ平文に対して 2^{34} の暗号文が集められてしまうと，連続した 1 ペタバイトの平文が 0.6 以上の確率で復元されてしまう．また、平文の情報が一切知られていない場合であっても、同じ平文に対して 2^{35} の暗号文が集められてしまうと，平文のどの位置であっても 1 に近い確率で復元されてしまうことが示されている。

また、 [20] では基本的な攻撃方針としては [1] と同様の手法を用い、成功確率を上げるための最適化を施した解析結果を示している。 具体的には、Broadcast セッティングが実現できるいくつかの具体的な事例を実際に実装し SSL/TLS で RC4 を用いることが現実的な脅威になりうることを示している。事例 1) Java スクリプトの脆弱性を利用し、不正な JavaScript をユーザに使わせることにより、その Java スクリプトを使って大量のターゲットメッセージの Cookie を暗号化して送信させることにより、Broadcast セッティングの環境を実現させる。この不正な Java スクリプトを用いた Broadcast セッティングは、具体的には攻撃者の Web サイトから Java スクリプトマルウェア をダウンロードさせ、その上で https リクエストを大量にリモートサーバに送らせることにより実現できる。事例 2) IMAP(Internet Message Access Protocol；メールサーバ上の電子メールにアクセスし操作するためのプロトコル) で送られるパスワードをターゲットとし、IMAP サーバにアクセスする際に暗号化されたパスワードが送られる仕組みに着目し、暗号化されたパスワードが送られた後に TCP コネクションをリセットし、暗号化されたパスワードを繰り返し送らせることにより Broadcast セッティングを実現させている。具体的に示されている結果として、先頭 256 バイトの bias を実験的に調べ、同じ平文に対して 2^{26} の暗号文を集められると毎回変化する 36 バイトを除いた 40 バイト が 0.5 以上の確率で復元されてしまうことが示されている。 また、同じ平文に対して 2^{32} の暗号文を集められると毎回変化する 36 バイトを除いた 220 バイト が 0.96 以上の確率で復元されてしまうことが示されている。また、ターゲットとなる平文の直前の平文が知られている場合、そのターゲットとなっている平文について、$16 \cdot 2^{30}$ の暗号文を集められるとおおよそ 1 の確率で復元されてしまうことが示されている。

このように、RC4 の攻撃が適用できる条件が整う環境下では、RC4 のアルゴリズムの攻撃は現実的に実現し得るものであり、攻撃者は暗号文を集めれば攻撃を試みることができてしまう。3 章に示された数々の攻撃に対してはそれらを防止する対処策を施すことができる一方、 RC4 の攻撃は対処策がないため、SSL/TLS を運用する選択肢として、RC4 を用いることは、現実的な脅威を招く原因となり得る。

謝辞

本ガイドラインの執筆にあたり、国立大学法人広島大学 大東俊博助教、株式会社富士通研究所 伊豆哲也様、株式会社インターネットイニシアティブ 須賀祐治様、ソニー株式会社 五十部孝典様より、SSL/TLS 及び RC4 に対する攻撃および安全性に関する知見のご提供とご助言をいただきました。ここに深く感謝申し上げます。

引用文献

[1] T. Isobe, T. Ohigashi, Y. Watanabe , M. Morii, “Full Plaintext Recovery Attack on Broadcast RC4,” FSE, 2013.

[2] J. Rizzo and T. Duong, BEAST: Surprising Crypto Attack against HTTPS, http://www.ekoparty.org/eng/2011/thai-duong.php.: ekoparty, 2011.

[3] “Bug 665814,”: https://bugzilla.mozilla.org/show_bug.cgi?id=665814#c59.

[4] 黒川 貴司, 野島 良, 盛合 志帆, “TLS1.0 における CBC モードの安全性について,” 第 31 回暗号と情報セキュリティシンポジウム (SCIS2014), 2014.

[5] “Transport Layer Security (TLS) Extensions: Extension Definitions.,”: http://tools.ietf.org/ html/rfc6066..

[6] J. Rizzo and T. Duong, “The CRIME Attack,” ekopary, 2012.

[7] T. Be'ery and A. Shulman, “A Perfec Crime? Only TIME Will Tell,” BlackHat, 2013.

[8] Y. Glick, N. Harris and A. Prado, “BREACH: REVIVING THE CRIME ATTACK,” BlackHat, 2013.

[9] AlFardan and Paterson, “Lucky Thirteen: Breaking the TLS and DTLS, IEEE Security&Privacy,” 2013.

[10] “JVNVU#120541:SSL および TLS プロトコルに脆弱性,” 11 2009.: http://jvn.jp/cert/JVNVU120541/.

[11] S. Joe , R. Eric, “TLS Renegotiation Vulnerability,: http://tools.ietf.org/agenda/76/slides/tls-7.pdf.

[12] Internet Initiative Japan, "1.4.2 MITM Attacks Using a Vulnerability in the SSL and TLS Renegotiation", Internet Infrastructure Review vol.6, 2010.

[13] A. Nagao, T. Ohigashi, T. Isobe and M. Morii, “New Classes of Weak Keys on RC4 using Predictive State,” Computer Security Symposium 2012 (CSS2012), 2012.

[14] A. Nagao, T. Ohigashi, T. Isobe and M. Morii, “Expanding Weak-Key Space of RC4,” 2013 年暗号と情報セキュリティシンポジウム(SCIS2013), 2013.

[15] A. Nagao, T. Ohigashi, T. Isobe and M. Morii, "Expanding Weak-Key Space of RC4," Journal of Information Processing, vol.22, no.2, 2014.

[16] T. Isobe, T. Ohigashi, Y. Watanabe and M. Morii, “Comprehensive Analysis of Initial Keystream Biases of RC4,” IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, 2014.

[17] Y. Watanabe, T. Isobe, T. Ohigashi, M. Morii, “Vulnerability of RC4 in SSL/TLS,”

情報通信システムセキュリティ(ICSS)研究会, 2013.

[18] CRYPTREC, “「CRYPTREC Report 2012 暗号方式委員会報告書」,” 2012.

[19] T. Ohigashi, T. Isobe, Y. Watanabe , M. Morii, “How to Recover Any Byte of Plaintext on RC4,” SAC, 2013.

[20] N. AlFardan, D. J. Bernstein, K. G. Paterson , J. C. Schuldt, “On the Security of RC4 in TLS,” USENIX, 2013.

[21] “CVE Details,”: http://www.cvedetails.com/cve/CVE-2011-3389.

[22] “Mozilla Firefox,”: https://developer.mozilla.org/en-US/docs/Security_in_Firefox_2.

[23] “Google Chrome,”: https://code.google.com/p/chromium/issues/detail?id=90392.

[24] “Microsoft Security Bulletin - MS2-006 - Important,”: http://technet.microsoft.com/en-us/security/bulletin/ms12-006.

[25] “Oracle,”: http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html.

[26] “List of browsers support for different TLS version,”: https://en.wikipedia.org/wiki/Transport_Layer_Security#Web_browsers.

付録６

CRYPTREC 暗号技術ガイドライン (SHA-1)

2014 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

目次

1. 本書の位置付け

1.1. 本書の目的

本書は、電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、CRYPTREC 暗号リストの運用監視暗号リストに記載されているハッシュ関数 SHA-1 を利用する際に必要となる情報を示すものである。

1.2. 本書の構成

本書では、2 章で SHA-1 に関する非推奨及び許容事項を、3 章で参考情報を示す。

1.3. 注意事項

本書の内容は2014年3月31日時点の情報に基づき構成されている。従って、今後、CRYPTREC 暗号リストの改定や攻撃方法の研究動向等によって、本書に掲載される内容が現実にそぐわないケースが発生する可能性がある。

2. ハッシュ関数 SHA-1 の利用について

2.1. 推奨されない利用範囲

(1)電子署名における署名生成

2012 年度に策定した CRYPTREC 暗号リスト(2013 年 3 月 1 日付) [1]の運用監視暗号リストに記載されている。なお、2008 年 4 月に NISC から「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」 [5]が策定されているため、CRYPTREC 暗号リスト [1]では、RSA-PSS 及び RSASSA-PKCS1-v1_5 には下記の(注 1)が付記されている。

(注 1) 「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」(平成 20 年 4 月 情報セキュリティ政策会議決定、平成 24 年 10 月 情報セキュリティ対策推進会議改定)を踏まえて利用すること。 http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf (平成 25 年 3 月 1 日現在)

2.2. 許容される利用範囲

(1) 電子署名における署名検証

2012 年度に策定した CRYPTREC 暗号リスト(2013 年 3 月 1 日付) [1]の運用監視暗号リストに記載されている。なお、一定の検証要件を満たすことにより、電子署名やタイムスタンプの有効期間を超えた後でも、それらの有効性を確認可能な長期署名フォーマット(CMS 及び XML に対応)が標準化(JIS 及び ISO)されている。

(2) The Keyed-Hash Message Authentication Code (HMAC)

NIST FIPS PUB 198-1[7]の仕様に基づく HMAC が CRYPTREC 暗号リスト [1]に記載されている。安全性について特段の問題点は指摘されていない [8]。

(3) Key Derivation Functions (KDFs)

NIST SP 800-56A、ANS X9.42、SEC 1 v1.0 で使用される KDF の安全性について、特段の問題点は指摘されていない [9,10]。

(4) 擬似乱数生成系

・ 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

の3つの方式が2002年度に策定した改定前の電子政府推奨暗号リスト [2]に記載されている。
また、NIST Special Publication 800-90A [13]にある

・ Hash_DRBG、
・ HMAC_DRBG、
・ CTR_DRBG

の3つの方式が2009年度版リストガイド [14]に記載されている。

(5) パスワード・ハッシングやチェックサムの計算としての利用(hash-only applications)

3. 参考情報

(1)電子署名における署名生成

2002 年度に策定した改定前の電子政府推奨暗号リスト(2003 年 2 月 20 日付) [2]では、ハッシュ関数の SHA-1 は注釈において、『(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。』と規定していた。また、暗号技術監視委員会(当時)は「SHA-1 の安全性に関する見解」(2006 年 6 月 28 日付け) [3,4]において、『電子署名やタイムスタンプのように長期間にわたって利用するシステムでは、新規(更新を含む)に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、256 ビット以上のハッシュ関数の使用を薦める。』と報告していた。

NIST Special Publication 800-131A [6]では、

Digital Signature Process	Use	
Digital Signature Generation	80 bits of security strength: DSA: (($\|p\| \geq 1024$) and ($\|q\| \geq 160$)) and (($\|p\| < 2048$) OR ($\|q\| < 224$)) RSA: $1024 \leq \|n\| < 2048$ EC: $160 \leq \|n\| < 224$	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	≥ 112 bits of security strength: DSA: $\|p\| \geq 2048$ and $\|q\| \geq 224$ RSA: $\|n\| \geq 2048$ EC: $\|n\| \geq 224$	Acceptable

とされている。

(2) 電子署名における署名検証

NIST Special Publication 800-131A [6]では、

Digital Signature Process	Use	
Digital Signature Verification	80 bits of security strength: DSA: (($\|p\| \geq 1024$) and ($\|q\| \geq 160$)) and (($\|p\| < 2048$) OR ($\|q\| < 224$)) RSA: $1024 \leq \|n\| < 2048$ EC: $160 \leq \|n\| < 224$	Acceptable through 2010 Legacy-use after 2010
	≥ 112 bits of security strength: DSA: $\|p\| \geq 2048$ and $\|q\| \geq 224$	Acceptable

	RSA: $\|n\| \geq 2048$ EC: $\|n\| \geq 224$	

Acceptable is used to mean that the algorithm and key length is safe to use; no security risk is currently known.
Legacy-use means that the algorithm or key length may be used to process already protected information (e.g., to decrypt ciphertext data or to verify a digital signature), but there may be risk in doing so. Methods for mitigating this risk should be considered.

とされている。

(3) Key Derivation Functions (KDFs)

NIST Special Publication 800-135 Revision 1 [11]を含む、一般的なアプリケーションで利用される KDF については、「2012 年度版リストガイド(KDF に関する調査)」に記載されている [12]。

(4) 擬似乱数生成系

現在、NIST Special Publication 800-90A Revision 1 [15]、800-90B [16]及び800-90C [17]はドラフト版になっている。

なお、NIST Special Publication 800-131A [6]では、FIPS 186-2 や ANS X9.62-1998 で指定されている擬似乱数生成系に関する移行指針が下記の通り記載されている。

The use of the RNGs specified in FIPS 186-2, [X9.31] and ANS [X9.62] is **deprecated** from 2011 through December 31, 2015, and disallowed after 2015.

Deprecated means that the use of the algorithm and key length is allowed, but the user must accept some risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection to data (e.g., encrypting or generating a digital signature).

(5) パスワード・ハッシングやチェックサムの計算としての利用(hash-only applications)

NIST Special Publication 800-131A [6]に記載がある。

4. 参考文献

[1] 総務省・経済産業省、電子政府における調達のために参照すべき暗号のリスト (CRYPTREC 暗号リスト)、2013 年 3 月 1 日

[2] 総務省・経済産業省、電子政府における調達のために参照すべき暗号のリスト(電子政府暗号リスト)、2003 年 2 月 20 日

[3] CRYPTREC Report 2005 (第 2 版)[1]、2006 年 5 月 17 日

[4] 暗号技術検討会報告書(2006 年度)[2]、2007 年 3 月

[5] 内閣官房情報セキュリティセンター (NISC)、政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針[3]、2008 年 4 月 22 日

[6] NIST Special Publication 800-131A[4]、2011 年 1 月

[7] NIST FIPS PUB 198-1[5]、2008 年 7 月

[8] Mihir Bellare, New Proofs for NMAC and HMAC: Security Without Collision-Resistance[6], CRYPTO 2006, LNCS 4117, pp. 602-619, 2006.

[9] CRYPTREC Report 2007, 2008 年 3 月

[10] 2007 年度電子政府推奨暗号の利用方法に関するガイドブック[7]、2008 年 3 月

[11] NIST Special Publication 800-135 Revision 1[8], 2011 年 12 月

[12] CRYPTREC Report 2012[9], 2013 年 3 月

[13] NIST, Special Publication 800-90A[10], 2012 年 1 月

[14] 2009 年度版リストガイド[11]、2010 年 3 月 ([1]で例示したもの、及び、[12]の Hash_DRBG、HMAC_DRBG、CTR_DRBG)

[15] NIST, Draft NIST Special Publication 800-90A Revision 1[12]

[16] NIST, Draft NIST Special Publication 800-90B[13]

[17] NIST, Draft NIST Special Publication 800-90C[14]

---

[1] http://www.cryptrec.go.jp/report/c05_wat_final.pdf
[2] http://www.cryptrec.go.jp/report/c06_kentou_final.pdf
[3] http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf
[4] http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
[5] http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
[6] https://eprint.iacr.org/2006/043
[7] http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf
[8] http://csrc.nist.gov/publications/nistpubs/800-135-rev1/sp800-135-rev1.pdf
[9] http://www.cryptrec.go.jp/report/c12_sch_web.pdf
[10] http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf
[11] http://www.cryptrec.go.jp/report/c09_guide_final.pdf
[12] http://csrc.nist.gov/publications/drafts/800-90/draft_sp800_90a_rev1.pdf
[13] http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf

[14] http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90c.pdf

付録 7

暗号技術調査 WG(暗号解析評価)
2013 年度報告書

格子問題等の困難性に関する調査

離散対数問題の困難性に関する調査

2014 年 3 月

格子問題等の困難性に関する調査

2014 年 3 月

目次

第 1 章

調査の目的

公開鍵暗号の安全性は, 素因数分解の困難性や離散対数問題の困難性などさまざまな数学的問題に依存している. 本ワーキンググループではこれまで, 素因数分解の困難性及び離散対数問題等の困難性に関する調査を行ってきたが, 量子計算機が実現しても安全性が保たれると期待されている「耐量子計算機暗号」を支える数学的問題の困難性の中でも, 特に近年活発に研究されてきている, 格子に係る数学的問題等に注目して調査を行った.

1.1 2013 年度 暗号技術調査ワーキンググループ (暗号解析評価) の委員構成

主査	高木 剛	国立大学法人九州大学 マス・フォア・インダストリ研究所 教授
委員	青木 和麻呂	日本電信電話株式会社 NTT セキュアプラットフォーム研究所 主任研究員
委員	石黒 司	株式会社 KDDI 研究所 情報セキュリティ G 研究員
委員	太田 和夫	国立大学法人電気通信大学 大学院 情報理工学研究科 総合情報学専攻 (セキュリティ情報学コース) 教授
委員	草川 恵太	日本電信電話株式会社 NTT セキュアプラットフォーム研究所 研究員
委員	國廣 昇	国立大学法人東京大学大学院 新領域創成科学研究科複雑理工学専攻 准教授
委員	下山 武司	株式会社富士通研究所 ソフトウェアシステム研究所 セキュアコンピューティング研究部 主任研究員
委員	安田 雅哉	株式会社富士通研究所 ソフトウェアシステム研究所 セキュアコンピューティング研究部

1.2 調査の概要

各章の執筆担当者及び調査内容は下表の通りである.

章	執筆委員名	内容
第 1 章	事務局	調査の目的, 調査の概要など
第 2 章	石黒 司 委員	General な攻撃に関する総論
第 3 章	下山 武司 委員 安田 雅哉 委員	各問題について以下の項目を記述 (1) 公開鍵方式からの帰着, 証明の有無, 追加の問題・制約など
第 4 章	草川 恵太 委員	(2) 攻撃や量子アルゴリズム - General な攻撃との関係
第 5 章	國廣 昇 委員	- 固有の攻撃 - 量子アルゴリズムとの関係

第 2 章から第 5 章までの調査内容をまとめると, 下記の通りとなる.

1. 格子の SVP(近似版を含む) のうち, 近似因子が次元の多項式で表される場合に適用される, 4 つの解読アルゴリズム (LLL,BKZ, 篩, ボロノイセル) の計算量等に関する概説を行った. 計算機実験 (SVP Challenge, Lattice Challenge, Ideal Lattice Challenge) に関しては, 日本の研究者らからの実験結果もいくつかなされている.
2. LWE 問題は,GapSVP 及び SIVP の困難性に関する仮定のもとで解くことが困難であることが知られており, 効率的に解くことが困難であると予想されている. 完全準同型暗号スキームをはじめ,LWE 問題ベースの暗号スキームが提案されてきている. 実際の構成の際には,BKZ アルゴリズム等の格子縮約アルゴリズムに対し耐性を持つようにパラメータ設定を行う必要があり, 安全な LWE パラメータを選択することは今後の課題である.
3. 総当たり法で解く他に,LPN 問題を解くアルゴリズムを大別すると,3 つの解読アルゴリズム (BKW,Arora-Ge による再線形化, シンドローム復号 (SD) 問題を経由するもの) が知られている.McEliece 暗号や Niederreiter 暗号をはじめ, 90 年代から様々な暗号スキームが提案されてきている. BKW アルゴリズムの改良版である LF アルゴリズムの計算機実験例や SD 問題の高速化によるパラメータの評価例がある.
4. ACD 問題を, 素因数分解を直接的に経由しないで解くアルゴリズムは, 大別すると, 組み合わせ論に基づく方法と格子理論に基づく方法がある. 前者については, 最近提案された Chen-Nguyen のアルゴリズムを使って, 実際に提案論文で書かれた推奨パラメタのいくつかが解読されているため, 今後の研究の動向に注視する必要がある.

第 2 章

総論

2.1 一般的な攻撃に関する総論

本章では，一般的な攻撃に関する攻撃についてまとめる．格子に関する困難性問題の中でベースとなる問題は格子の最短ベクトル問題 (SVP) である．本章では，この格子の最短ベクトル問題の定義と，それに関連するアルゴリズムについてまとめる．更に，実際の計算機環境における解析の現状についてまとめる．最短ベクトル問題は，格子暗号における重要な困難性問題の一つであり，この問題が解けると，次章以降で説明する LWE 問題などの格子問題も解けるため計算量解析がとりわけ重要である。

本章で使用する記号・用語を以下にまとめる．$\boldsymbol{b}_i = (b_1, b_2, \ldots, b_n) \in \mathbb{R}^n$ を n 個の一次独立なベクトルとする $(1 \leq i \leq n)$．$\boldsymbol{b}_i$ を列ベクトルとする行列を $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n) \in \mathbb{R}^{n \times n}$ とする． この時，

$$\mathcal{L}(\mathrm{B}) = \mathcal{L}(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n) = \left\{ \sum_{1 \leq i \leq n} x_i \boldsymbol{b}_i, x_i \in \mathbb{Z} \right\}$$

を格子とする．また，B を格子基底と呼ぶ．本章では格子の次元を n とする．ベクトル $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$ のノルム (長さ) を，$||\boldsymbol{v}|| = (\sum_{1 \leq i \leq n} v_i^2)^{1/2}$ とする．また，基底 B の最短ベクトルかつ非零ベクトルのノルムを $\lambda_1(\mathrm{B})$ あるいは単に λ_1 と表す．格子 B のグラムシュミット直交化基底を $\mathrm{B}^* = (\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \ldots, .\boldsymbol{b}_n^*)$ とする．$\boldsymbol{b}_i^*$ は，$\boldsymbol{b}_1^* = \boldsymbol{b}_1$ として，$2 \leq i \leq n$ について以下のように帰納的に定義される．

$$\boldsymbol{b}_i^* = \boldsymbol{b}_i - \sum_{1 \leq j \leq i-1} \mu_{i,j} \boldsymbol{b}_j^*, \quad \mu_{i,j} = \frac{\langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle}{||\boldsymbol{b}_j^*||}$$

$\mu_{i,j}$ をグラムシュミット係数とよぶ．基底 $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n), i \in \{1, 2, .., n\}$ における直交射影 $\pi_i : \mathbb{R}^n \to \mathbb{R}^n$ を $(\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{i-1})$ が生成する部分空間の直交補空間への射影写像とし，$\pi_i(\boldsymbol{v}) = \sum_{1 \leq i \leq n} a_i \boldsymbol{b}_i^*$ と表す．$i \leq j$ となる基底ベクトル $\boldsymbol{b}_j$ に対して $\pi_i(\boldsymbol{b}_j) = \boldsymbol{b}_j^{(i)}$ と表す．また，格子の射影部分格子を $\mathcal{L}_{[j,k]} = \mathcal{L}((\boldsymbol{b}_i^{(j)})_{j \leq i \leq \min(j+k-1, n)})$ とする．

2.1.1 最短ベクトル問題 (SVP)

格子の最短ベクトル問題を SVP(Shortest Vector Probrem) とよぶ．これはある格子の基底が与えられた時に，その格子上のベクトルの中で長さが最小となる非零ベクトルを探索する問題である．一般に，最短ベクトルは必ずしも一つではないため，最短ベクトルの中の一つのベクトルを見出せば SVP の解となる．また，長さが最短ベクトルの α 倍以下となるベクトルのうちの一つを探索する問題を近似版最短ベクトル問題 (α-SVP) とよぶ．以下にそれぞれ詳細な定義を示す．

定義 2.1 (最短ベクトル問題 (SVP)) 格子 $\mathcal{L}(\mathrm{B})$ が与えられて，格子に含まれるベクトル $\boldsymbol{v} \in \mathcal{L}(\mathrm{B})$ のうちでノルムが最小の非零ベクトル *(つまり，$|\boldsymbol{v}| = \lambda_1$)* の一つを求める問題を最短ベクトル問題 *(SVP)* と呼ぶ．

最短ベクトルのノルムについて以下の定理が知られている．

定理 2.2 (ミンコフスキーの第 1 定理) 格子 $\mathcal{L}(\mathrm{B})$ に対して最短ベクトルのノルムは，$\sqrt{n}(\mathrm{vol}(\mathcal{L}(\mathrm{B})))^{\frac{1}{n}}$ 未満となる．

また，より精緻な見積りとしてガウスヒューリスティックスが知られている．ガウスヒューリスティックスによって格子 $\mathcal{L}(\mathrm{B})$ の最短ベクトルのノルムは $GH(\mathcal{L}(\mathrm{B})) = (1/\sqrt{\pi})\Gamma(\frac{n}{2}+1)^{\frac{1}{n}} \cdot |\det(\mathcal{L}(\mathrm{B}))^{\frac{1}{n}}|$ 程度と見積もられる．ここで，$\Gamma(x)$ はガンマ関数を表す．最短ベクトル問題は，上記の通り厳密解を求める問題として定義されている．一方，暗号アルゴリズムでは最短ベクトルの近似解を求める問題の困難性をベースとして構成される場合もある．以下に近似版最短ベクトル問題 (α-SVP) を定義する．

定義 2.3 (近似版最短ベクトル問題 (α-SVP)) 格子 $\mathcal{L}(\mathrm{B})$ が与えられて，格子に含まれるベクトル $\boldsymbol{v} \in \mathcal{L}(\mathrm{B})$ のうちでノルムが $||\boldsymbol{v}|| < \alpha\lambda_1$ となるベクトルの一つを求める問題を近似版最短ベクトル問題 *(α-SVP)* と呼ぶ．また，α を近似因子と呼ぶ．

2.1.2 求解アルゴリズムと計算量

SVP は Ajtai によって，ランダム帰着の元で NP 困難問題であることが示されている [1]．α-SVP については，近似因子 $1 < \alpha < \sqrt{2}$ となる範囲ではランダム帰着の元で NP-困難であることが Micciancio[18] によって示され，任意の定数 α の元での NP 困難性が Khot によって証明されている [16, 17]．一方，近似因子が格子の次元 n の多項式となる場合，すなわち $\alpha = poly(n)$ の場合の NP 困難性については証明されておらず，重要な研究課題となっている．本節では，SVP，α-SVP それぞれについて求解アルゴリズムを解説する．

■α-SVP　α-SVP を解くアルゴリズムとして, LLL[12], BKZ[31] アルゴリズムがある．LLL アルゴリズムは, Lenstra, Lenstra, Lovász 等によって提案されたアルゴリズムである．LLL アルゴリズムは格子の基底を入力とし，LLL 簡約基底とよばれる入力された基底と同じ格子を張る別の基底を求めるアルゴリズムである．この LLL 簡約基底は，基底ベクトルのノルムに制約がある格子基底となっており，以下のように定義される．

定義 2.4 (簡約基底) 格子基底を B とする．このとき B^* のグラムシュミット係数 $\mu_{i,j}(1 \leq j < i \leq n)$ が $|\mu_{i,j}| < \frac{1}{2}$ を満足するとき，B は簡約基底という．

定義 2.5 (δ-LLL 簡約基底) 格子基底を $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ とし，$\delta \in (0.25, 1]$ とする．格子 B が簡約基底であり，かつ

$$\delta||\boldsymbol{b}^*_{i-1}||^2 \leq ||\boldsymbol{b}^*_i||^2 + \mu^2_{i,i-1}||\boldsymbol{b}^*_{i-1}||^2$$

という条件を満足するとき，B は *δ-LLL* 簡約基底という．また，この条件を *Lovász* 条件とよぶ．

LLL 簡約アルゴリズムを用いると，LLL 簡約基底を求めることができ，基底ベクトルがノルムの大きさが小さい方から順番に整列される．このとき，$||\boldsymbol{b}_1|| \leq (\frac{2}{\sqrt{3}})^n\lambda_1$ となることが証明されているため，近似因子 $\alpha = (\frac{2}{\sqrt{3}})^n$ における α-SVP の解とすることができる．

LLL アルゴリズムの概要を以下に示す．入力は，格子基底 $\mathrm{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ とし δ-LLL 簡約基底を出力する．LLL アルゴリズムは $\boldsymbol{b}_1$ から順に $\boldsymbol{b}_n$ に向かって簡約を行う．まず，$\boldsymbol{b}_j$ を簡約基底の条件を満足するために $k < j$ に対して，

$\boldsymbol{b}_j = \boldsymbol{b}_j - \lceil \mu_{j,k} \rfloor \boldsymbol{b}_k$ を計算し，$\boldsymbol{b}_j$ に合わせて $\mu_{j,k}$ を再計算する．次に，$\boldsymbol{b}_j$ が Lovász 条件を満足しない場合には $\boldsymbol{b}_j$ と $\boldsymbol{b}_{j-1}$ を入れ替え，$j = j-1$ として上記を繰り返す．この処理によって $j = 1$ から $j = n$ まで $\boldsymbol{b}_j$ を簡約する．LLL アルゴリズムは多項式回のループで停止することが示されており，計算量は $O(n^4 \log(\max_{1 \le i \le n} ||\boldsymbol{b}_i||^2))$ となる．また，出力される基底の第一ベクトルのノルムは $||\boldsymbol{b}_1|| \le (\frac{2}{\sqrt{3}})^n \lambda_1$ となることが証明されている [12]．計算機実験上はこの見積りよりも短いベクトルが出力されることが多く，特に小さい次元の場合には LLL アルゴリズムを用いて最短ベクトルを求めることができる．

LLL を改良したアルゴリズムとして BKZ アルゴリズムが Schnor 等によって提案されている．BKZ アルゴリズムは BKZ 簡約基底を出力するアルゴリズムである．BKZ 簡約基底は LLL 簡約基底よりも広い定義となっており，以下のように定義される．

定義 2.6 (β-BKZ 簡約基底) 格子基底を $\mathrm{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ とし，$\beta \in [2, n]$ とする．格子 B が *LLL* 簡約基底であり，かつ $1 \le j \le n$ について $||\boldsymbol{b}_j^*|| = \lambda_1(\mathcal{L}_{[j,\beta]})$ を満足するとき，B は β-*BKZ* 簡約基底という．

β-BKZ 簡約基底は LLL 簡約基底を拡張したものであり，$\beta = 2$ の場合には LLL 簡約基底そのものになる．BKZ アルゴリズムの概要を以下に示す．BKZ アルゴリズムの入力は，LLL 簡約基底 $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ とし β-BKZ 簡約基底を出力する．まず，$i = 1, 2, \ldots, n-1$ について $\pi_i(\boldsymbol{b})$ が $\mathcal{L}_{[i,\beta]}$ で最短ベクトルとなるような $\boldsymbol{b} \in \mathcal{L}(\mathrm{B})$ を探索する．このようなベクトルは次節で説明する SVP を解くアルゴリズムを用いて求めることができる．次にこの $||\pi_i(\boldsymbol{b})|| < ||\boldsymbol{b}_i^*||$| となる場合には基底 B にベクトル $\boldsymbol{b}$ を i 番目に挿入し基底 $\mathrm{B}' = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i, \boldsymbol{b}, \boldsymbol{b}_{i+1}, \ldots, \boldsymbol{b}_n)$ を構成する．これに LLL 簡約基底を適用し，新たな基底とする．新たな基底に対して上記を繰り返し，基底が更新されなくなるまで繰り返すことによって基底簡約を行う．BKZ アルゴリズムの停止性や計算量は証明されていないが，計算機実験上は高速に動作し，LLL アルゴリズムよりも大きな次元に対して適用することができる．BKZ アルゴリズムを改良したアルゴリズムとして BKZ2.0 アルゴリズム [CN11, 4] が提案されており，より大きな次元の α-SVP が解けることが示されている．また，ランダムに短いベクトルを生成して基底に挿入し，そこに BKZ アルゴリズムを適用することによって基底を簡約する RSR アルゴリズムも提案されている [34, 13].

■SVP　SVP を解くアルゴリズムとして以下のいくつかの種類のアルゴリズムが提案されている．代表的な求解手法として，格子基底簡約アルゴリズム，列挙アルゴリズム，ボロノイセルアルゴリズム，篩アルゴリズムがある．

格子基底簡約アルゴリズムは，上記で説明した LLL,BKZ アルゴリズムなどの基底簡約アルゴリズムであり，格子基底に適用することによって SVP を解くことができる．代表的な格子基底簡約アルゴリズムとして LLL アルゴリズム [12]，BKZ アルゴリズム [31]，L^2 アルゴリズム [21, 22]，BKZ2.0[9, 4] がある．

列挙アルゴリズムは，所謂全数探索で可能性のある係数の総当り探索を行い，最短ベクトルを見つけるアルゴリズムである．格子ベクトル $\boldsymbol{v} \in \mathcal{L}(\mathrm{B})$ は，基底ベクトル $\boldsymbol{b}$ を用いて，$\boldsymbol{v} = \sum_{1 \le i \le n} u_i \boldsymbol{b}_i$ と表せる．したがって，可能性のある全ての係数 $[u_1, u_2, \ldots, u_n]$ を列挙することによって最短ベクトルを見つける事ができる．列挙アルゴリズムは，Schnorr によって示され [32]，更に探索範囲を削減する枝刈り列挙 ([33, 9, 20]) アルゴリズムが提案されている．現時点で最も高速な枝刈り列挙アルゴリズムは Gama, Nguyen, Regev によって提案された Extream Pruning Enumeration アルゴリズムである [9]．このアルゴリズムの時間計算量は $2^{O(n)}$ である．列挙アルゴリズムは特に比較的小さい次元において高速に SVP を解くことができるため，BKZ アルゴリズムの内部関数としても用いられている．列挙アルゴリズムの計算量を表 2.1 に示した．列挙アルゴリズムは並列化が容易であることから，GPU 上での高速実装や，クラウドコンピューティングを用いた大規模並列計算によって大きな次元の SVP の求解報告がなされている [27].

Micciancio によってボロノイセルアルゴリズムが提案されている [19]．ボロノイセルアルゴリズムは決定的アルゴ

表 2.1　列挙アルゴリズムの計算量

アルゴリズム	時間	空間	文献
ENUM	$2^{O(n^2)}$	$O(n)$	文献 [32]
Extream Pruning Enumeration	$2^{O(n)}$	$O(n)$	文献 [9]

表 2.2　篩アルゴリズムの計算量

アルゴリズム	時間計算量	空間計算量	文献
AKS Sieve	$O(2^{5.90n})$	$O(2^{2.95n})$	文献 [3]
AKS Sieve without perturbation	$O(2^{0.41n})$	$O(2^{0.21n})$	文献 [23]
List Sieve	$O(2^{3.199n})$	$O(2^{1.325n})$	文献 [19]
Gauss Sieve	$O(2^{0.52n})$	$O(2^{0.21n})$	文献 [19]
List Sieve Birthday	$O(2^{2.465n})$	$O(2^{1.233n})$	文献 [26]
NV Sieve	$O(2^{0.3836n})$	$O(2^{0.2557n})$	文献 [23, 35]

リズムであり，$2^{O(n)}$ の時間計算量，空間計算量となることが示されている．しかし，現在のところボロノイセルアルゴリズムの実装例は知られていない．

篩アルゴリズムは SVP を解く確率的アルルゴリズムである．2001 年に Ajtai 等によって AKS Sieve[3] が提案され，それ以降，より計算量を削減したアルゴリズムが提案されている [23, 6, 5, 19, 26, 35]．一般に篩アルゴリズムの時間・空間計算量は $2^{O(n)}$ である．現在，理論上最も高速な古いアルゴリズムは NV Sieve であり，時間計算量は $O(2^{0.3836n})$，空間計算量は $O(2^{0.2557n})$ となっている．篩アルゴリズムの計算量を表 2.2 に示した．

2.1.3　計算機実験

本章では，計算機実験によって実際に解かれた SVP についてまとめる．現在，ダルムシュタット大学によって SVP に関するコンテストが開催されている．このコンテスによって統一された問題設定においてアルゴリズム・実装性能の評価が可能となっている．しかし実験環境，計算機環境についての制限はないため，アルゴリズムや実装手法以外にも，計算機性能や実験規模などが異なることに注意する必要がある．

SVP Challenge[30] はランダムに与えられた格子基底に対して SVP を解き，より大きい次元について，より短いベクトルを求めることによって順位が競われている．コンテストのサイトには，実際に解かれたベクトルが掲載されている．ただし，掲載されているベクトルは必ずしも最短のベクトルではないことに注意されたい．Lattice Challenge[29] は与えられた格子基底について α-SVP を解き，SVP チャレンジと同様により大きい次元，より短いベクトルを解くことが競われている．Ideal Lattice Challenge[24] は，イデアル格子と呼ばれる，暗号で用いられることが多い特殊な格子 [11, 8, 10] に対する SVP，α-SVP の問題が掲載されている．コンテストに掲載されている問題の設定については文献 [25] を参照にされたい．

α-SVP に対する実験結果を表 2.3 に表す．現在，α-SVP の求解は BKZ2.0 アルゴリズム [9]，あるいはその改良方式 [CN11, 4] が用いられており，825 次元までの α-SVP が解かれている．詳細なアルゴリズム，計算機環境についてはそれぞれの文献を参照されたい．また，SVP に対する実験結果を 2.3 に示す．SVP Challenge の結果として

表 2.3　α-SVP の求解 (Lattice Challenge[29])

	次元	ノルム	アルゴリズム	時期	文献
Chen, Nguyen	825	120.37	BKZ2.0 の改良	2013-3	文献 [CN11]
Aono, Naganuma	825	122.38	BKZ2.0 の改良	2012-10	文献 [4]
Chen, Nguyen	800	106.60	BKZ2.0 の改良	2013-3	文献 [CN11]
Aono, Naganuma	800	117.69	BKZ2.0 の改良	2012-10	文献 [4]
Chen, Nguyen	775	100.14	BKZ2.0 の改良	2013-3	文献 [CN11]
Aono, Naganuma	775	106.68	BKZ2.0 の改良	2012-10	文献 [4]
Chen, Nguyen	750	87.76	BKZ2.0 の改良	2013-3	文献 [CN11]
Chen, Nguyen	725	80.65	BKZ2.0 の改良	2013-3	文献 [CN11]
Aono, Naganuma	725	83.61	BKZ2.0 の改良	2012-9	文献 [4]
Chen, Nguyen	700	72.46	BKZ2.0 の改良	2013-3	文献 [CN11]
Aono, Naganuma	700	76.17	BKZ2.0 の改良	2012-9	文献 [4]

表 2.4　SVP の求解 (SVP Challenge[30], Ideal Lattice Challenge[24])

	次元	ノルム	アルゴリズム	時期	文献
Kashiwabara, Fukase	130	3025	RSR アルゴリズムの改良	2013-11	文献 [15]
Kashiwabara, Fukase	128	2984	RSR アルゴリズムの改良	2013-9	文献 [15]
Kashiwabara, Fukase	126	2944	RSR アルゴリズムの改良	2013-9	文献 [15]
Chen, Nguyen	126	2969	BKZ2.0 の改良	2013-4	文献 [CN11]
Chen, Nguyen	124	2884	BKZ2.0 の改良	2013-3	文献 [CN11]
Chen, Nguyen	122	2884	BKZ2.0 の改良	2013-3	文献 [CN11]
Aono, Naganuma	120	2756	BKZ2.0 の改良	2013-3	文献 [4]
Kashiwabara, Fukase	120	2830	RSR アルゴリズムの改良	2013-9	文献 [15]
Ishiguro, Kiyomoto, Miyake, Takagi	128	2959	Gauss Sieve の改良	2013-4	文献 [14]

Kashiwabara らの RSR アルゴリズムの改良手法 [15]，BKZ2.0[9] が有効であることが示されており最も大きな次元に対する求解は Kashiwabara らによる RSR アルゴリズムの改良方式である [15]．彼らの手法は，短いベクトルの統計的な情報から，最短ベクトルの分布を予測し高速に短いベクトルを生成するように改良している。

また，Ideal Lattice Challenge においては 128 次元の SVP が解かれている [14]．彼らの手法は，篩アルゴリズムの一つである Gauss Sieve アルゴリズムの並列化によって 84 台の計算機を用いて 128 次元の SVP を求めている。Gauss Sieve アルゴリズムはイデアル格子の性質を用いて次元が 2 の冪乗となる場合に高速化できることが示されている。更に、イデアル格子のいくつかの次元において Gauss Sieve を高速化できる条件も見つかっているが、一般のイデアル格子の性質を用いた高速化手法は、他の求解手法も含めて見つかっていないため、格子暗号の安全性を議論する上で重要な研究課題となっている。

第 2 章の参照文献

[1] M. Ajtai. The Shortest Vector Problem in L^2 is NP-hard for Randomized Reductions (Extended Abstract). In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, STOC'98, pages 10–19. ACM, 1998.

[2] M. Ajtai and C. Dwork. A Public-key Cryptosystem with Worst-case/average-case Equivalence. In *Proceedings of the 29th Annual ACM Symposium on Theory of Computing*, STOC'97, pages 284–293. ACM, 1997.

[3] M. Ajtai, R. Kumar, and D. Sivakumar. A Sieve Algorithm for the Shortest Lattice Vector Problem. In *Proceedings of the 33th Annual ACM Symposium on Theory of Computing*, STOC'01, pages 601–610. ACM, 2001.

[4] 青野，長沼BKZ2.0 アルゴリズムの実装と改良. 信学技報, vol. 112, no. 211, ISEC2012-45, pp. 15–22, 2012.

[5] V. Arvind and P. S. Joglekar. Some Sieving Algorithms for Lattice Problems. In *Proceedings of the IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science*, FSTTCS'08, volume 2 of *LIPIcs*, pages 25–36. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2008.

[6] J. Blömer and S. Naewe. Sampling Methods for Shortest Vectors, Closest Vectors and Successive Minima. *Journal of Theoretical Computer Science*, volume 410, issue 18, pages 1648–1665, 2009.

[7] Y. Chen, and N. Nguyen. BKZ 2.0: Better Lattice Security Estimates. In *Proceedings of the 19th Annual International Conference on Theory and Application of Cryptology and Information Security.*, ASIACRYPT'11, volume 7073 of *LNCS*, pages 1-20. Springer, 2011.

[8] S. Garg, C. Gentry, and S. Halevi. Candidate Multilinear Maps from Ideal Lattices. Cryptology ePrint Archive, Report 2012/610, 2012.

[9] N. Gama, P. Nguyen, and O. Regev. Lattice Enumeration Using Extreme Pruning. In *Proceedings of the 29th Annual International Conference on Theory and Application of Cryptographic Techniques*, Eurocrypt'10, volume 6110 of *LNCS*, pages 257–278. Springer, 2010.

[10] C. Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In *Proc of the 41st Annual ACM Symposium on Theory of Computing*, STOC'09, pages 169–178. ACM, 2009.

[11] J. Hoffstein, J. Pipher, and J. Silverman. NTRU: A Ring-based Public Key Cryptosystem. In *Algorithmic Number Theory*, volume 1423 of *LNCS*, pages 267–288. Springer, 1998.

[12] A. Lenstra, H. Lenstra, and L. Lovász. Factoring Polynomials with Rational Coefficients. *Journal of Mathematische Annalen*, volume 261, issue 4, pages 515–534, 1982.

[13] J. Buchmann and C. Ludwig In *Proceedings of the 7th International Symposium*, ANTS-VII, volume 4076 of *LNCS*, pages 222–237, Springer, 2006.

[14] T. Ishiguro, S. Kiyomoto, Y. Miyake and T. Takagi. Parallel Gauss Sieve Algorithm: Solving the SVP Challenge over a 128-Dimensional Ideal Lattice. Cryptology ePrint Archive, Report 2013/388, 2013.

[15] 柏原 賢二 格子の最短ベクトル問題の新しいアルゴリズム. 第 5 回暗号及び情報セキュリティと数学の相関ワークショップ, CRISMATH2013, 2013. http://www.risec.aist.go.jp/events/2013/1226-ja.html.

[16] S. Khot Hardness of Approximating the Shortest Vector Problem in Lattices, *Journal of the ACM*, Vol. 52, No. 5, pages 789–808, Springer, 2005.

[17] S. Khot Inapproximability Results for Computational Problems on Lattices, *Information Security and Cryptography - The LLL Algorithm*, pages 453–473, Springer, 2010.

[18] D. Micciancio. The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, FOCS'98, pages 92–98. IEEE Computer Society, 1998.

[19] D. Micciancio and P. Voulgaris. A Deterministic Single Exponential Time Algorithm for Most Lattice Problems Based on Voronoi Cell Computations. In *Proceedings of the 42nd ACM Symposium on Theory of Computing*, STOC'10, pages 351–358. ACM, 2010.

[20] D. Micciancio and P. Voulgaris. Faster Exponential Time Algorithms for the Shortest Vector Problem. In *Proceedings of the 21st Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA'10, volume 65, pages 1468–1480. SIAM, 2010.

[21] P. Q. Nguyen and T. Vidick. Floating-point LLL Revisited. In *Proceedings of the 24th Annual Eurocrypt Conference*, volume 3495 of *LNCS*, pages 215–233, Springer, 2005.

[22] P. Q. Nguyen and T. Vidick. LLL on the Average. In *Proceedings of the 7th International Symposium*, ANTS-VII, volume 4076 of *LNCS*, pages 238–256, Springer, 2006.

[23] P. Q. Nguyen and D. Stehlé. Sieve Algorithms for the Shortest Vector Problem Are Practical. *Journal of Mathematical Cryptology*, volume 2, pages 181–207, 2008.

[24] T. Plantard and M. Schneider. Ideal Lattice Challenge. http://www.latticechallenge.org/ideallattice-challenge/.

[25] T. Plantard and M. Schneider. Creating a Challenge for Ideal Lattices. Cryptology ePrint Archive, Report 2013/039, 2013.

[26] X. Pujol and D. Stehle Solving the Shortest Lattice Vector Problem in Time $2^{2.465n}$. Cryptology ePrint Archive, Report 2009/605, 2009.

[27] M. Schneider. *Computing Shortest Lattice Vectors on Special Hardware*. PhD thesis, Technische Universität Darmstadt, 2011.

[28] M. Schneider. Sieving for Shortest Vectors in Ideal Lattices. Cryptology ePrint Archive, Report 2011/458, 2011.

[29] M. Schneider and N. Gama. Lattice Challenge. http://www.latticechallenge.org/.

[30] M. Schneider and N. Gama. SVP Challenge. http://www.latticechallenge.org/svp-challenge/.

[31] C.-P. Schnorr. A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms. *Journal of Theoretical Computer Science*, volume 53, issue 2-3, pages 201–224, 1987.

[32] C.-P. Schnorr. Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems. *Journal of Mathematical programming*, pages 181–191. Springer, 1993.

[33] C.-P. Schnorr and H. H. Horner. Attacking the Chor-Rivest Cryptosystem by Improved Lattice Reduc-

tion. In *Proceedings of the 14th annual international conference on Theory and application of cryptographic techniques*, Eurocrypt'95, pages 1–12. Springer, 1995.

[34] C.-P. Schnorr. Lattice reduction by random sampling and birthday methods. In *Proceedings of the 20th Annual Symposium on Theoretical Aspects of Computer Science*, STACS'03, pages 145–156. Springer, 1995.

[35] X. Wang, M. Liu, C. Tian and J. Bi Improved Nguyen-Vidick Heuristic Sieve Algorithm for Shortest Vector Problem. Cryptology ePrint Archive, Report 2010/647, 2010.

第 3 章

LWE

3.1 LWE の概説

近年、2005 年に Regev[Reg05] によって紹介された LWE (Learning with Errors) 問題の計算量困難性に依存した暗号技術がこれまで数多く提案されている。ここでは、主に LWE 問題を用いた様々な暗号技術へのアプリケーションの紹介と、LWE 問題の計算量困難性についてまとめる（本章をまとめるにあたり、文献 [Reg] を主に参考にした)。

3.1.1 LWE とは

LWE 問題とは、Machine Learning (機械学習理論) から派生した、解くことが難しいとされている問題の一種である。簡単に説明すると、秘密情報 $\vec{s} \in \mathbb{F}_q^n$ に関するランダムな線形 “近似値”の列が与えられたときに、その秘密情報 $\vec{s}$ を復元する問題のことをいう。具体的な数値例として、変数 $\vec{s} = (s_1, s_2, s_3, s_4)$ に関する線形近似値の列

$$
\begin{aligned}
14s_1 + 15s_2 + 5s_3 + 2s_4 &\approx 8 \pmod{17} \\
13s_1 + 14s_2 + 14s_3 + 6s_4 &\approx 16 \pmod{17} \\
6s_1 + 10s_2 + 13s_3 + s_4 &\approx 12 \pmod{17} \\
10s_1 + 4s_2 + 12s_3 + 16s_4 &\approx 12 \pmod{17} \\
9s_1 + 5s_2 + 9s_3 + 6s_4 &\approx 9 \pmod{17} \\
3s_1 + 6s_2 + 4s_3 + 5s_4 &\approx 16 \pmod{17} \\
&\vdots \\
6s_1 + 7s_2 + 16s_3 + 2s_4 &\approx 3 \pmod{17}
\end{aligned}
$$

が与えられたとする（ただし、各線形方程式の誤差は ± 1 程度とする)。このとき、上記の方程式の列の解 $\vec{s} = (s_1, s_2, s_3, s_4)$ を求めるのが LWE 問題の例である（実際、上記の数値例では、$\vec{s} = (0, 13, 9, 11) \in \mathbb{F}_{17}^4$ が解となる)。ここで注意しておかなくてはいけない事は、上記の線形方程式で誤差がない場合は、ガウスの消去法（または掃出し法ともいう）を用いれば多項式時間で簡単に解を求めることができる点である。つまり、与えられる誤差の度合いが LWE 問題をより難しくしている。ここで、LWE 問題の定義を与えておく。

定義 3.1 (LWE 問題 [Reg05]) サイズパラメータ $n \geq 1$, 剰余パラメータ $q \geq 2$, $\mathbb{F}_q$ 上の誤差に関する確率分布 χ が与えらたとする。このとき、$A_{\vec{s},\chi}$ を

$$
A_{\vec{s},\chi} = \left\{ (\vec{a}, \langle \vec{a}, \vec{s} \rangle + e) \in \mathbb{F}_q^n \times \mathbb{F}_q \mid \vec{a} \leftarrow \mathbb{F}_q^n, e \leftarrow \chi \right\}
$$

で定義される確率分布とする（ただし、$\vec{a}$ は $\mathbb{F}_q^n$ 上一様ランダムに選ばれた元とし、$\langle \vec{a}, \vec{s} \rangle$ は 2 つのベクトル間の内積値とする)。秘密情報 $\vec{s} \in \mathbb{F}_q^n$ に対し、$A_{\vec{s},\chi}$ からサンプリングされた任意個数の元が与えられた時に、秘密情報 $\vec{s}$ を求める問題を LWE 問題という。

上記で定義した LWE 問題は、ランダム線形符号の復号問題、または、格子上ランダムな bounded distance decoding(BDD) 問題として見なすことができる。さらに、$q = 2$ のとき、LWE 問題は learning parity with noise (LPN) 問題に対応する（LPN 問題については、第 4 章で説明)。上記の定義において、確率分布 χ としてガウス分布を用いる場合がほとんどであったが、近年では一様分布を用いた場合の研究も進み始めている [DQ13, MP13]。

またこの節で、上記で定義した LWE の変形問題である ring-LWE 問題も紹介しておく（以下の定義では、2 べき整数 n の場合しか説明しないが、近年では一般の整数 n を用いた ring-LWE 問題も紹介され、色々な暗号方式を構成する際に応用されている。参考文献として [LPR13] を参照することを勧める)。

定義 3.2 (ring-LWE 問題 [LPR10]) n を 2 べき整数とし、q を $q \equiv 1 \bmod 2n$ を満たす素数とする。また、R_q を環 $\mathbb{F}_q[x]/(x^n+1)$ と定め、R_q 上の誤差に関する確率分布 χ を固定しておく。ただし、写像 $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mapsto (a_0, a_1, \ldots, a_{n-1})$ より環 R_q は n-次元ベクトル空間 $\mathbb{F}_q^n$ と同一視することができ、R_q の元を $\mathbb{F}_q^n$ の元として見なすことができる。ring-LWE 問題では、$\vec{a} \bullet \vec{s}$ を R_q 上の乗算とした時、秘密情報 $\vec{s} \in R_q \simeq \mathbb{F}_q^n$ に対して、集合

$$\left\{ (\vec{a}, \vec{b} = \vec{a} \bullet \vec{s} + \vec{e}) \in R_q \times R_q \mid \vec{a} \leftarrow R_q, \vec{e} \leftarrow \chi \right\}$$

からサンプリングされた元たちが与えられた時に、秘密情報 $\vec{s}$ を求める問題を ring-LWE 問題と呼ぶ。

通常の LWE 問題に比べて、ring-LWE 問題は格子ベースの暗号スキームをより効率的にすることができ、近年では ring-LWE 問題をベースとした (主に準同型) 暗号スキームが数多く提案されている。

3.1.2 LWE の一般的な利点（アプリケーション）

一般的に、LWE 問題は暗号技術の様々な分野に応用することが可能で、これまでに様々な研究者によって提案されている。代表的な応用例として以下のものが知られている。

- 公開鍵暗号スキームの構成
  - 選択平文攻撃に対して安全な方式 [Reg05, KTX07, PVW08]
  - 選択暗号文攻撃に対して安全な方式 [PW08, Pei09]
- 紛失通信プロトコル [PVW08]
- identity-based encryption (IBE) スキームの構成 [GPV08, CHKP10, ABB10]
- leakage-resilient 暗号の構成 [AGV09, ACPS09, DGK10, GKPV10]

さらに、2009 年の Gentry[Gen09] の完全準同型暗号の構成に関する結果以降では、特に ring-LWE 問題ベースの（完全 or somewhat）準同型暗号スキームが数多く提案されており、代表的な完全準同型暗号スキームに関するものとして、[SV11, BGV12, GHS12a, GHS12b, GHPS12] の結果が知られている。

3.2 LWE 問題の困難性について

ここでは、LWE 問題の困難性に簡単について説明する。ここでは、他の格子問題への帰着という理論的な困難性に関するものと、実際の攻撃実験による困難性評価に関するものの 2 つの面による結果を説明する。

3.2.1 他の格子問題への帰着とその困難性

文献 [Reg] でも説明されているように、以下に挙げる 3 つの理由から現在 LWE 問題を解くことは難しいと信じられている。

(A) まず、LWE 問題を解く、知られているものの中で最良のアルゴリズムは指数時間アルゴリズムである（量子アルゴリズムを用いた場合でさえも難しい)。
(B) §3.1.1 で説明したように、LWE 問題は LPN 問題の一般化であり、LPN 問題自体が格子理論において解くのが困難な問題と予想されている。さらに、LPN 問題はランダム線形バイナリ符号の復号問題として定式化可能であり、LPN 問題を効率的に解くこと自体符号理論におけるブレークスルーである（LPN 問題については、第 4 章を参照)。
(C) さらに最も重要なこととして、GapSVP(the decision version of the shortest vector problem) や SIVP(the shortest independent vectors problem) のような標準的な格子問題の最悪ケースの困難性に関するある仮定のもとで、LWE 問題は困難であることが知られている [Reg05, Pei09]。

ここで、上記の (A) と (C) の点について具体的に説明した定理を挙げておく。

定理 3.3 ([Reg09] における Theorem 1.1) n, q を *2* つの整数とし、$\alpha \in (0,1)$ は $\alpha q > 2\sqrt{n}$ を満たすとする。もし $\mathsf{LWE}_{n,q,\bar{\Phi}_\alpha}$ *(§3.2.2 の定義 3.4 を参照)* を解く効率的なアルゴリズムが存在するなら、最悪時の因子 $\gamma = \tilde{O}(n/\alpha)$ を持つ GapSVP_γ と SIVP_γ を効率的に解くことができる量子アルゴリズムが存在する。ただし、Φ_α は平均値が 0 で標準偏差が $\frac{\alpha}{\sqrt{2\pi}}$ を持つ確率分布で、$\bar{\Phi}_\alpha$ は Φ_α を離散化した確率分布とする。

別の言い方をすると、上記の定理は GapSVP と SIVP を効率的に解く量子アルゴリズムが存在しないなら、LWE 問題を効率的に解くアルゴリズムは存在しないことを示している。また一方で、任意の多項式因子 γ を持つ GapSVP_γ と SIVP_γ を解く多項式時間を持つ量子アルゴリズム [NC00] は存在しないと予想されており、このことから LWE 問題を解くことは困難であると予想されている。

ちなみに GapSVP_γ 問題とは、n 次元格子 L と与えらえた値 $d > 0$ に対し、$\lambda_1(L)$ を各々 L の最小ベクトルの長さ、$\lambda_n(L)$ を n 個の一次独立なベクトル集合に含まれる最大ベクトル長の最小値、$\gamma = \gamma(n)$ を 1 以上の近似因子として、$\lambda_1(L) \leq d$ なら Yes を, $\lambda_1(L) > \gamma(n)d$ なら No を返す問題であり、SIVP_γ とは、同じく L に対して、長さ $\gamma(n) \cdot \lambda_n(L)$ 以下の n 個の一次独立なベクトルを求める問題である。

その他、安全性証明に関連する結果として、文献 [LMSV12] では、ring-LWE 問題をベースとした Somewhat Homomorphic Encryption スキーム (演算回数に制約がある準同型暗号スキームで、完全準同型暗号スキームの構成要素) が IND-CCA1 を満たすことが示されている。

3.2.2 LWE 問題の困難性の実験評価

Lindner と Peikert [LP11] は、LWE 問題の困難性について NTL ライブラリ (具体的には、NTL ライブラリ内の BKZ アルゴリズムを利用) を用いて実際の攻撃実験を行い、その困難性評価指標を定めている。ここでは、彼らの困難性評価指標について、簡単にまとめておく。まず、彼らが評価対象とした decision version の LWE 問題を以下で正確に定義する。

定義 3.4 (decision version, $\mathsf{LWE}_{n,q,\chi}$) 定義 *3.1* で与えたように、$n \geq 1$ と $q \geq 2$ と、$\mathbb{F}_q$ 上の確率分布 χ を考える（ただし、文献 *[LP11]* では、確率分布 χ は $\mathbb{Z}$ 上の標準偏差 σ を持つ離散ガウス分布 $D_{\mathbb{Z},\sigma}$ から生成されたものにしている)。このとき、秘密情報 $\vec{s} \in \mathbb{F}_q^n$ に対し、定義 *3.1* で紹介した $A_{\vec{s},\chi}$ からランダムにサンプリングされた元 $(\vec{a}, \langle \vec{a}, \vec{s} \rangle + e)$ と、$\mathbb{F}_q^n \times \mathbb{F}_q$ 上の一様分布で得られる元とを区別する問題を $\mathsf{LWE}_{n,q,\chi}$ と定義する。

上記で定義した $\mathsf{LWE}_{n,q,\chi}$ 問題に対して、文献 [LP11] で Lindner-Peikert は 2 つの効率的な攻撃手法を紹介している。

- distinguishing attack（Micciancio-Regev[MR07] が提案）
- decoding attack（Lindner-Peikert 自身が文献 [LP11] で提案）

文献 [LP11] によると、decoding attack よりも distinguishing attack の方が常に効率的であるが、実際の攻撃評価結果 [LP11, Figure 4 in Section 6] を比べてみると、$\varepsilon = 2^{-32}$ または $\varepsilon = 2^{-64}$ 程度の実用的なレベルの advantage を想定した場合には、上記 2 つの攻撃の効率性は同程度であったという結果を得たとのこと。

■Distinguishing attack による攻撃原理　そこで、以下では $\mathsf{LWE}_{n,q,\chi}$ 問題に対する distinguishing attack の攻撃原理を少し紹介しておく。秘密情報 $\vec{s} \in \mathbb{F}_q^n$ に対し、集合 $A_{\vec{s},\chi}$ からランダムにサンプリングされた元

$$\vec{a}_i \in \mathbb{F}_q^n,\ b_i = \langle \vec{a}_i, \vec{s} \rangle + e_i \in \mathbb{F}_q \tag{3.1}$$

を数多く (ここでは m 個) 集めることで、以下の情報を得ることができる（ここでは、すべてのベクトルは n-次元の行ベクトルで表記したとする)：

$$\mathbf{A} = (\vec{a}_1^T, \vec{a}_2^T, \ldots, \vec{a}_m^T) \in \mathbb{F}_q^{n \times m}, \vec{b} = (b_1, b_2, \ldots, b_m) \in \mathbb{F}_q^m, \vec{e} = (e_1, e_2, \ldots, e_m) \in \mathbb{Z}^m$$

すると、上記の記法を用いると、関係式 (3.1) から

$$\vec{b} = \vec{s} \cdot \mathbf{A} + \vec{e} \pmod{q}$$

という関係式を得ることができる。そこで、$\mathbb{F}_q^n \times \mathbb{F}_q$ 上の一様分布で得られる元と区別するために、攻撃者はまず (scaled な) 双対格子

$$\Lambda^{\perp}(\mathbf{A}) := \left\{ \vec{v} \in \mathbb{Z}^m \mid \vec{v} \cdot \mathbf{A}^T \equiv 0 \pmod{q} \right\}$$

の最短ベクトル $\vec{v} \neq \vec{0} \in \mathbb{Z}^m$ を見つけたとする。ここで、その攻撃者は内積値 $\langle \vec{v}, \vec{b} \rangle \pmod{q}$ が 0 に十分近いかどうかで $\mathbb{F}_q^n \times \mathbb{F}_q$ 上一様分布にサンプリングされた元かどうか判定することができる。その理由は、ベクトル $\vec{v}$ は $\vec{v} \cdot \mathbf{A}^T \equiv 0 \pmod{q}$ を満たすので、

$$\langle \vec{v}, \vec{b} \rangle \equiv \langle \vec{v}, \vec{s} \cdot \mathbf{A} + \vec{e} \rangle \equiv \langle \vec{v}, \vec{s} \cdot \mathbf{A} \rangle + \langle \vec{v}, \vec{e} \rangle \equiv \langle \vec{v}, \vec{e} \rangle \pmod{q}$$

となる。さらに、ベクトル $\vec{e} \in \mathbb{Z}$ の各成分 e_i は $\chi = D_{\mathbb{Z},\sigma}$ からサンプリングされた元なので、そのサイズは σ 程度となり、上記の内積値 $\langle \vec{v}, \vec{b} \rangle$ のサイズはおよそ $\sigma \cdot ||\vec{v}||$ 程度となることが分かる。よって、攻撃者は十分小さなベクトル $\vec{v} \in \Lambda^{\perp}(\mathbf{A})$ を見つけることができた場合、上記の内積値の小ささを測ることで、$\mathbb{F}_q^n \times \mathbb{F}_q$ 上一様にサンプリングされた元か $A_{\vec{s},\chi}$ からサンプリングされた元か区別することができる。

■Distinguishing attack に対する解読計算量評価　さらに、文献 [MR07] によると、advantage ε を持つ攻撃者は双対格子 $\Lambda^{\perp}(\mathbf{A})$ から長さ $c \cdot q/\sigma$ を持つ格子元を見つけることができた場合、distinguishing attack を成功することができると示している（詳細は、[LP11, Section 6] を参照)。ただし、$c \approx \sqrt{\log_2(1/\varepsilon)/\pi}$ とする。また一方、格子縮約アルゴ

表 3.1　$\log_2(T_{\mathrm{BKZ}})$ と δ_{BKZ} の関係 [DPSZ12, Appendix D]

$\log_2(T_{\mathrm{BKZ}})$	80	100	128	192	256
δ_{BKZ}	1.0066	1.0059	1.0052	1.0041	1.0034

リズムはある格子の中からかなり短い格子元を出力するアルゴリズムで、その格子縮約アルゴリズムがどのくらい短い格子元を出力することが可能かを図る指標として、*root Hermite factor* という指標がよく用いられる（root Hermite factor の説明については、[GN08] を参照)。d-次元の格子 L に対して、

$$\delta := \left(\frac{||\vec{b}_1||}{|\det(L)|^{1/d}} \right)^{1/d}$$

の値を格子縮約アルゴリズムの root Hermite factor と呼ぶ。ただし、格子縮約アルゴリズムを出力される格子基底を $\{\vec{b}_1, \ldots, \vec{b}_d\}$ とし、その長さを $||\vec{b}_i||$ と表す（さらに、$||\vec{b}_1|| \leq ||\vec{b}_2|| \leq \cdots$ と仮定)。そこで、distinguishing attack を用いて、$\mathsf{LWE}_{n,q,\chi}$ 問題を解くためには、攻撃に利用する格子縮約アルゴリズムの root Hermite factor δ は

$$c \cdot q/\sigma = \delta^m \cdot |\det(\Lambda^{\perp}(\mathbf{A}))|^{1/m} = \delta^m \cdot q^{n/m}$$

の条件を満たす必要がある。さらに、distinguishing attack に最適な格子次元 $m = \sqrt{n \log_2(q)/\log_2(\delta)}$ を想定した場合、上記の関係式から

$$c \cdot q/\sigma = 2^{2\sqrt{n \log_2(q) \log_2(\delta)}} \tag{3.2}$$

という n, q, σ の関係式を新たに得ることができる。

一方、BKZ アルゴリズムは効率的な格子縮約アルゴリズムことが知られている。そこで、Lindner-Peikert [LP11] は NTL ライブラリで実装済みの BKZ アルゴリズムを利用した場合の distinguishing attack の計算量 T_{BKZ} に対して、

$$\log_2(T_{\mathrm{BKZ}}) = \frac{1.8}{\log_2(\delta_{\mathrm{BKZ}})} - 110 \tag{3.3}$$

という見積もり値を示している。ただし、ここでの δ_{BKZ} は BKZ アルゴリズムの root Hermite factor で、その指標値は BKZ アルゴリズムのブロックサイズに関するパラメータにより定まる（ブロックサイズが大きくなるほど root Hermite factor は小さくなるため、distinguishing attack の計算量 T_{BKZ} は増大する)。表 3.1[*1]に、文献 [DPSZ12, Appendix D] で示されている T_{BKZ} と δ_{BKZ} の関係式を示した表を紹介しておく。表 3.1 から分かることは、BKZ アルゴリズムを利用した攻撃に対して $\mathsf{LWE}_{n,q,\chi}$ 問題のセキュリティレベルを 80-bit 程度以上に保つためには、root Hermite factor $\delta = 1.0066$ に対し、関係式 (3.2) を満たすように $n, q, \chi = D_{\mathbb{Z},\sigma}$ のパラメータを選択する必要があることを示している。しかし、Lindner-Peikert による見積もり攻撃評価 (3.3) は、NTL ライブラリ実装による BKZ アルゴリズムに関するもので、すでに最新の実装結果ではないことに注意。現在知られている BKZ アルゴリズムは、Chen-Nguyen ら [CN11] が実装した BKZ 2.0 というアルゴリズムが代表的で、彼ら自身のアルゴリズム評価によると、80-bit セキュリティを得るためには、BKZ アルゴリズムの root Hermite factor が 1.0050 程度以下を想定する必要があることを示している。

[*1] 表 3.1 における $\log_2(T_{\mathrm{BKZ}})$ の 192 は元論文では 196 と記載されているが、誤植であろうと考えられる。

3.2.3 アプリケーションのためのパラメータ設定について

LWE 問題を用いた暗号技術応用において、LWE 問題の困難性を十分保ちながら暗号プロトコルなどを正しく動作させるためのパラメータ設定は一般的にかなり難しい問題である。ここでは、これまで知られている LWE 問題におけるパラメータ設定の代表例を挙げておく：

- Lindner-Peikert らは、[LP11, Section 3] で Micciancio[Mic10] が概要を示した LWE 問題ベースの公開鍵暗号方式の具体的な構成方法を示し、さらに彼らは [LP11, Section 6] でその暗号方式に対する具体的なパラメータ例を [LP11, Figure 3] に示している。また近年では、青野らは表 [ABPW13, Table 2] で [LP11] で挙げたパラメータの安全性を再評価する一方で、LWE ベースの proxy re-encryption(PRE) スキームの具体的なパラメータを [ABPW13, Table 1] で示し、その各パラメータの安全性を [ABPW13, Table 3] で評価している。
- LWE 問題をベースとした準同型暗号方式に関しては、AES 回路を暗号化したまま行うために、Gentry-Halevi-Smart ら [GHS12b] が [BGV12] で提案されたレベル付き完全準同型暗号の具体的なパラメータ設定方法を示している。一方、完全準同型暗号ではなく限定回の加算と乗算が可能な somewhat 準同型暗号の具体的なパラメータとして、Lauter-Naehrig-Vaikuntanathan ら [LNV11] が [BV11] で提案された somewhat 準同型暗号を利用して、平均・標準偏差・ロジスティック回帰などの統計計算を暗号化したまま行うための具体的なパラメータを表 [LNV11, Table 1] で示している。

3.3 まとめ

LWE (Learning with Errors) 問題は、Machine Learning(機械学習理論) から派生した問題で、GapSVP 及び SIVP の困難性に関する仮定のもとで解くことが難しいことが知られており、本問題を効率的に解くことは困難であると予想されている。現在までに完全準同型暗号スキームをはじめとした、様々な公開鍵暗号スキームのベースがこの LWE 問題をベースとして提案されており、今後も安全な暗号を構成する上で重要な要素となると考えられる。現在までに知られている LWE 問題を解く最良アルゴリズムは指数時間の計算量を持っている。ただし、実際の LWE 問題をベースとした暗号スキームの構成の際には、BKZ アルゴリズムなどの格子縮約アルゴリズムに対し耐性を持つようにパラメータ設定を行う必要があり、安全でかつ演算機能等の要件を満足するような LWE パラメータを選択するための、統一的な方法は知られておらず、今後の課題となっている。また、LWE 問題に対する攻撃実験評価に関する結果もあまり知られていないため、今後は計算機実験に関する研究も非常に重要になると思われることから、安全性理論評価はもちろん攻撃実験評価の視点からも、今後の動向に注意する必要がある。

第 3 章の参照文献

[ABB10] S. Agrawal, D. Boneh and X. Boyen, "Efficient lattice (H)IBE in the standard model", In *Advances in Cryptology–EUROCRYPT 2010*, Springer LNCS 6110, 553–572, 2010.

[ABPW13] Y. Aono, X. Boyen, L.T. Phong and L. Wang, "Key-private re-encryption under LWE", In *Progress in Cryptology–INDOCRYPT 2013*, Springer LNCS 8250, 1–18, 2013.

[ACPS09] B. Applebaum, D. Cash, C. Peikert and A. Sahai, "Fast cryptographic primitives and circular-secure encryption based on hard learning problems", In *Advances in Cryptology–CRYPTO 2009*, Springer LNCS 5677, 595–618, 2009.

[AGV09] A. Akavia, S. Goldwasser and V. Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks", In *Theory of Cryptography–TCC 2009*, Springer LNCS 5444, 474–495, 2009.

[BGV12] Z. Brakerski, C. Gentry and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping", In *Innovations in Theoretical Computer Science–ITCS 2012*, ACM, 309–325, 2012.

[BV11] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-LWE and security for key dependent messages", In *Advances in Cryptology–CRYPTO 2011*, Springer LNCS 6841, 505–524, 2011.

[CHKP10] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert, Bonsai trees, or how to delegate a lattice basis, Journal of Cryptology, **25**(4) (2012), 601–639 (Preliminary version was presented at EUROCRYPT 2010), 2012.

[CN11] Y. Chen and P.Q. Nguyen, "BKZ 2.0: better lattice security estimates", In *Advanecs in Cryptology–ASIACRYPT 2011*, Springer LNCS 7073, 1–20, 2011.

[DGK10] Y. Dodis, S. Goldwasser, Y. Kalai, C. Peikert and V. Vaikuntanathan, "Public-key encryption schemes with auxiliary inputs", In *Theory of Cryptography–TCC 2010*, Springer LNCS 5978, 361–381, 2010.

[DPSZ12] I. Damgård, V. Pastro, N.P. Smart and S. Zakarias, "Multiparty computation from somewhat homomorphic encryption", In *Advances in Cryptology–CRYPTO 2012*, Springer LNCS 7417, 643–662, 2012.

[DQ13] N. Döttling and J. Müller-Quade, "Lossy codes and a new variant of the learning-with-errors problem", In *Advances in Cryptology–EUROCRYPT 2013*, Springer LNCS 7881, 18–34, 2013.

[GN08] N. Gama and P.Q. Nguyen, "Predicting lattice reduction", In *Advances in Cryptolog–EUROCRYPT 2008*, Springer LNCS 4965, 31–51, 2008.

[Gen09] C. Gentry, "Fully homomorphic encryption using ideal lattices", In *Proc. 41st ACM Symp. on Theory of Computing–STOC 2009*, ACM, 169–178, 2009.

[GHS12a] C. Gentry, S. Halevi and N.P. Smart, "Fully homomorphic encryption with polylog overhead", In *Advances in Cryptology–EUROCRYPT 2012*, Springer LNCS 7237, 465–482, 2012.

[GHS12b] C. Gentry, S. Halevi and N.P. Smart, "Homomorphic evaluation of the AES circuit", In *Advances in Cryptology–CRYPTO 2012*, Springer LNCS 7417, 850–867, 2012.

[GHPS12] C. Gentry, S. Halevi, C. Peikert and N.P. Smart, "Ring switching in BGV-style homomorphic encryption", In *Security and Cryptography for Networks–SCN 2012*, Springer LNCS 7485, 19–37, 2012.

[GKPV10] S. Goldwasser, Y. Kalai, C. Peikert and V. Vaikuntanathan, Robustness of the learning with errors assumption, Tsinghua University Press, 2010.

[GPV08] C. Gentry, C. Peikert and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions", In *Proc. 40th ACM Symp. on Theory of Computing–STOC 2008*, ACM, 197–206, 2008.

[KTX07] A. Kawachi, K. Tanaka and K. Xagawa, "Multi-bit cryptosystems based on lattice problems", In *Public Key Cryptography–PKC 2007*, Springer LNCS 4450, 315–329, 2007.

[LMSV12] J. Loftus, A. May, N.P. Smart, F. Vercauteren, "On CCA-Secure Somewhat Homomorphic Encryption", In *Selected Areas in Cryptology–SAC 2011*, LNCS 7118, pp. 55–72. 2012.

[LNV11] K. Lauter, M. Naehrig and V. Vaikuntanathan, "Can homomorphic encryption be practical?", In *ACM workshop on Cloud computing security workshop–CCSW 2011*, ACM, 113–124, 2011.

[LP11] R. Lindner and C. Peikert, "Better key sizes (and attacks) for LWE-based cryptography", In *RSA Conference on Topics in Cryptology–CT-RSA 2011*, Springer LNCS 6558, 319–339, 2011.

[LPR10] V. Lyubashevsky, C. Peikert and O. Regev, "On ideal lattices and learning with errors over rings", In *Advances in Cryptology–EUROCRYPT 2010*, Springer LNCS 6110, 1–23, 2010.

[LPR13] V. Lyubashevsky, C. Peikert and O. Regev, "A toolkit for ring-LWE cryptography", In *Advances in Cryptology–EUROCRYPT 2013*, Springer LNCS 7881, 35–54, 2013.

[Mic10] D. Micciancio, "Duality in lattice cryptography", Invited talk at Public Key Cryptography–PKC 2010.

[MP13] D. Micciancio and C. Peikert, "Hardness of SIS and LWE with Small Parameters", In *Advances in Cryptology–CRYPTO 2013*, Part I, Springer LNCS 8042, 21–39, 2013.

[MR07] D. Micciancio and O. Regev, Worst-case to average-case reduction based on gaussian measures, SIAM J. Computing **37**(1) (2007), 267–302, 2007.

[NC00] M.A. Nielsen and I.L. Chuang, Quantum computation and quantum information, Cambridge University Press, 2000.

[Pei09] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problems", In *Proc. 41st ACM Symp. on Theory of Computing–STOC 2009*, ACM, 333–342, 2009.

[PVW08] C. Peikert, V. Vaikuntanathan and B. Waters, "A framework for efficient and composable oblivious transfer", In *Advances in Cryptology–CRYPTO 2008*, Springer LNCS 5157, 554–571, 2008.

[PW08] C. Peikert and B. Waters, "Lossy trapdoor functions and their applications", In *Pro. 40th ACM Symp. on Theory of Computing–STOC 2008*, ACM, 187–196, 2008.

[Reg05] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, J. ACM, **56**(6) (2009), 1–40 (Preliminary version was presented at STOC 2005), 2009.

[Reg] O. Regev, The learning with errors problem, survey paper, available at `http://www.cims.nyu.edu/~regev/papers/lwesurvey.pdf`.

[Reg09] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, (2009), available at `http://www.cims.nyu.edu/~regev/papers/qcrypto.pdf`.

[SV11] N.P. Smart and F. Vercauteren, Fully homomorphic SIMD operations, Designs, Codes and Cryptography, preprint, July 2012, doi:10.1007/s10623-012-9720-4, 2012.

第 4 章

LPN

4.1 Learning Parity with Noise (LPN) 問題の概説

本章では Learning with Parity Noise (LPN) 問題や符号に関連する問題の困難性について調査結果を述べる.

4.1.1 LPN 問題とは

LPN 問題とはノイズ付きの線型方程式を解けるかどうかという問題である. 1993 年に, Blum, Furst, Kearns, Lipton [BFKL93] が困難と思われる問題として挙げ, 定式化を行った. 第 3 章において, この問題を一般化した LWE 問題を既に扱っている.

以下では $\mathbb{F}_q$ で位数が q の有限体を表す. Ber_τ でパラメータ τ のベルヌーイ分布を表すことにする. (確率 τ で 1, 確率 $1-\tau$ で 0 となる $\mathbb{F}_2$ 上の分布である.) また, 自然数 $k \geq 1$ について, Ber_τ^k で, Ber_τ から独立に k 個サンプルを取ったときの $\mathbb{F}_2^k$ 上の分布を表す.

■**LPN 問題**: $\mathbb{F}_2$ 上の分布 χ および $\vec{s} \in \mathbb{F}_2^n$ について, オラクル $\mathcal{O}_{\vec{s},\chi}$ を以下で定義する. (1) $\vec{a}$ を $\mathbb{F}_2^n$ からランダムに選び, (2) e を分布 χ に従い選び, (3) $b = \vec{s} \cdot \vec{a}^\top + e$ と計算し, (4) $(\vec{a}, b)$ を出力する. 定義より, このオラクルは第 3 章定義 3.1 で定義される分布 $A_{\vec{s},\chi}$ からのサンプル $(\vec{a}, b) \in \mathbb{F}_2^{n+1}$ を返す. また, オラクル $\mathcal{U}$ を $(\vec{a}, b) \leftarrow \mathbb{F}_2^{n+1}$ とランダムな組を出力するオラクルとして定義する.

定義 4.1 (探索版 LPN 問題) 探索版 LPN 問題とは, オラクル $\mathcal{O}_{\vec{s},\chi}$ へのアクセスが可能なときに, $\vec{s}$ を出力する問題である.

特に $\chi = \mathsf{Ber}_\tau$ のとき, $\mathsf{LPN}_{n,\tau}$ 問題と呼ぶ. また $\mathsf{LPN}_{n,\tau}$ 問題でオラクルからのサンプル数が $m = m(n)$ に制限されるものを, $\mathsf{LPN}_{n,m,\tau}$ 問題と呼ぶ.

定義 4.2 (探索版 LPN 仮定) $\mathbb{F}_2$ 上の確率分布 χ について, 敵 $\mathcal{A}$ の優位性を

$$\mathsf{Adv}_{\mathcal{A}}(n) = \Pr_{\vec{s} \leftarrow \mathbb{F}_2^n}[\mathcal{A}^{\mathcal{O}_{\vec{s},\chi}}(1^n) = \vec{s}]$$

で定義する. 任意の多項式時間の敵 $\mathcal{A}$ について, その優位性が無視できるとき, 探索版 LPN 仮定が成立するという.

暗号プリミティブや暗号プロトコルの安全性証明のために, 判定版 LPN 仮定を用いることも多い. 判定版 LPN 問題と判定版 LPN 仮定は以下で定義される.

定義 4.3 (判定版 LPN 問題) 判定版 LPN 問題とは, オラクル $\mathcal{O}_{\vec{s},\chi}$ またはオラクル $\mathcal{U}$ へのアクセスが与えられたときに, どちらのオラクルにアクセスしているかを判定する問題である.

定義 4.4 (判定版 LPN 仮定) $\mathbb{F}_2$ 上の確率分布 χ について, 敵 $\mathcal{A}$ の優位性を

$$\mathsf{Adv}_{\mathcal{A}}(n) = \left| \Pr_{\vec{s}\leftarrow\mathbb{F}_2^n}[\mathcal{A}^{\mathcal{O}_{\vec{s},\chi}}(1^n) = 1] - \Pr[\mathcal{A}^{\mathcal{U}}(1^n) = 1] \right|$$

で定義する. 任意の多項式時間の敵 $\mathcal{A}$ について, その優位性が無視できる関数であるとき, 判定版 LPN 仮定が成立するという.

探索版 LPN 問題にはランダム自己帰着が存在する [BFKL93]. すなわち, ランダムに選ばれた $\vec{s} \in \mathbb{F}_2^n$ について探索版 LPN 問題を解けるならば, 任意の $\vec{s} \in \mathbb{F}_2^n$ について探索版 LPN 問題を解くことが出来る.

Katz, Shin, Smith [KSS10] によれば, [BFKL93, Reg09] と同様に判定版 LPN 仮定を探索版 LPN 仮定に帰着することが出来る.

定理 4.5 ([KSS10]) 判定版 $\mathsf{LPN}_{n,\tau}$ 仮定を破る t ステップ, m 回のクエリ, 優位性 δ の敵が存在すると仮定する. このとき, 探索版 $\mathsf{LPN}_{n,\tau}$ 仮定を破る t' ステップ, m' 回のクエリ, 優位性 δ' の敵が存在する. ここで,

$$t' = O(\delta^{-2} tn \log n), m' = O(\delta^{-2} m \log n), \delta' \geq \delta/4.$$

■変種: 以上に列挙した LPN 問題・仮定では, 基礎となる体として $\mathbb{F}_2$ を用いていた. 体を $\mathbb{F}_q$ に変更した LPN 問題・仮定が用いられることもある. この場合 LWE 問題と非常によく似た問題・仮定となるが, 分布 χ の定義が異なることが多い.

LWE 問題では剰余環 $\mathbb{Z}_q$ を用いている. 応用の観点からは, 分布 χ からのサンプル x の絶対値が高い確率で小さいことが重視される.

一方, LPN 問題では有限体 $\mathbb{F}_q$ を用いている. また, 符号からの要求としてハミング重みを考えることが多いため, 分布 χ は 0 を取る確率が大きいことが求められる. たとえば, ベルヌーイ分布の一般化として, 確率 τ で 0 を確率 $1-\tau$ で $\mathbb{F}_q \setminus \{0\}$ のランダムな値を取る分布が用いられる. これは格子問題と符号問題のアナロジーとして考えることができる.

4.1.2 LPN 問題の拡張

4.1.2.1 復号問題

オラクルからのサンプル数を固定し $m = m(n)$ とする. $\mathsf{LPN}_{n,m,\tau}$ 問題での m 個のサンプル $(\vec{a}_1, b_1), (\vec{a}_2, b_2), \ldots, (\vec{a}_m, b_m)$ を行列・ベクトル表示して,

$$\boldsymbol{A} = [\vec{a}_1^\top \vec{a}_2^\top \ldots \vec{a}_m^\top] \in \mathbb{F}_2^{n\times m}, \vec{b} = \vec{s} \cdot \boldsymbol{A} + \vec{e}$$

とする. 符号理論の観点からは, ランダム行列 $\boldsymbol{A}$ を生成行列とする線形符号の受信語 $\vec{b}$ から元のメッセージ $\vec{s}$ を復元する問題と捉えることができる.

4.1.2.2 シンドローム復号問題

先ほど挙げた復号問題の “双対” として, シンドローム復号問題が挙げられる. シンドローム復号問題とは,

$$\boldsymbol{H} = [\vec{h_1}^\top \vec{h_2}^\top \ldots \vec{h_m}^\top] \in \mathbb{F}_2^{k\times m}, \vec{u} \in \mathbb{F}_2^k$$

および自然数 w が与えられた時に, $\vec{e} \cdot \boldsymbol{H}^\top = \vec{u}$ かつハミング重みが w 以下となる $\vec{e} \in \mathbb{F}_2^m$ を求める問題である.

$\boldsymbol{H}$ として $\boldsymbol{A}$ で生成される符号のパリティ検査行列を取り, $\vec{u}$ として $\vec{b} \cdot \boldsymbol{H}^\top (= \vec{e} \cdot \boldsymbol{H}^\top)$ をとれば, $\mathsf{LPN}_{n,m,\tau}$ 問題や復号問題をシンドローム復号問題に変換可能である.

4.1.2.3 Exact-LPN 問題

ノイズの分布として, $\vec{e} \leftarrow \mathsf{Ber}_\tau^m$ ではなく, ハミング重みが丁度 w のものだけを考える. このようにノイズの分布を変えた問題を Exact-LPN 問題と呼ぶ.

4.1.2.4 Sparse-LPN 問題

一部の暗号方式では, $\vec{s}$ のハミング重みが小さい, すなわち, スパースであることを要求する. Applebaum ら [ACPS09] は $\vec{s}$ をノイズの分布である χ^n から選んだ場合の LPN 問題と $\vec{s}$ を $\mathbb{F}_2^n$ からランダムに選んだ場合の問題とが等価であることを示している.

4.1.2.5 Subspace-LPN 問題

Pietrzak [Pie12a] は, 敵のオラクルへのクエリを強めた問題として, 以下の Subspace-LPN 問題を考察した. LPN 仮定で定義されたオラクルを $\mathcal{O}_{\vec{s},\chi}$ から以下で定義される $\mathcal{O}'_{\vec{s},\chi}$ に変更する. 二つの Affine 関数 $\phi_a(\vec{a}) = \vec{a}\boldsymbol{X}_a + \vec{x}_a$, $\phi_s(\vec{s}) = \vec{s}\boldsymbol{X}_s + \vec{x}_s$, $(\boldsymbol{X}_a, \boldsymbol{X}_s \in \mathbb{F}_2^{n \times n}, \vec{x}_a, \vec{x}_s \in \mathbb{F}_2^n,)$ をクエリとして受け取り, $\mathrm{rank}(\boldsymbol{X}_a^\top \boldsymbol{X}_s) \geq d + \delta$ ならば, $\vec{a} \leftarrow \mathbb{F}_2^n$ および $b = \phi_s(\vec{s}) \cdot \phi_a(\vec{a})^\top + e$ を出力する.

Peitrzak は, $2^{-\delta+1}$ が無視できるならば, 新しいオラクル $\mathcal{O}'_{\vec{s},\chi}$ を用いた Subspace-LPN 問題は, 次元 d の LPN 問題と困難性が等価であることを示した.

4.1.2.6 Toeplitz-LPN 問題

Gilbert, Robshaw, Seurin [GRS08] が認証プロトコルの効率化のために導入した.

行列 $\boldsymbol{A} = \{a_{i,j}\} \in \mathbb{F}_2^{n \times m}$ が Toeplitz 行列であるとは, 任意の i, j について $a_{i-1,j-1} = a_{i,j}$ が成立することである. Toeplitz 行列を表現するには左端の列ベクトルおよび最も上の行ベクトルがあれば良い. そのため $\boldsymbol{A}$ の表現は $n + m - 1$ ビットで可能である.

復号問題の節で, 探索版 LPN 問題でのサンプル $(\vec{a}_1, b_1), (\vec{a}_2, b_2), \ldots, (\vec{a}_m, b_m)$ を行列・ベクトル表示して,

$$\boldsymbol{A} = [\vec{a}_1^\top \vec{a}_2^\top \ldots \vec{a}_m^\top] \in \mathbb{F}_2^{n \times m}, \vec{b} = \vec{s} \cdot \boldsymbol{A} + \vec{e}$$

を考えた. オラクル $\mathcal{O}$ (および $\mathcal{U}$) を変更し, $\boldsymbol{A}$ が必ず Toeplitz 行列になる場合の LPN 問題を考える. これを Toeplitz-LPN 問題と呼ぶ.

4.1.2.7 Ring-LPN 問題

Heyse, Kiltz, Lyubashevsky, Paar, Pietrzak [HKL+12] は, Ring-LPN 問題を定義した. この問題は ring-LWE 問題 (定義 3.2) と同様に定義される.

定義 4.6 (探索版 Ring-LPN 問題) 適当な n 次の $\mathbb{F}_q$ 係数多項式 $f(x)$ を考え, 環 $R_q = \mathbb{F}_q[x]/(f(x))$ を固定する. R_q 上の確率分布 χ を固定する.

R_q 上の分布 χ および $s \in R_q$ について, オラクル $\mathcal{O}_{\vec{s},\chi}$ を以下で定義する. *(1)* a を R_q からランダムに選び, *(2)* e を分布 χ に従い選び, *(3)* $b = sa + e$ と計算し, *(4)* $(a, b) \in R_q^2$ を出力する.

探索版 Ring-LPN 問題とは, オラクル $\mathcal{O}_{s,\chi}$ へのアクセスが可能なときに, $s \in R_q$ を出力する問題である.

4.2 LPN 問題に対する評価

サンプル数を固定した場合, $\boldsymbol{A}$ および $\vec{b}$ の最悪時を考えると NP 困難になることが Berlekamp, McEliece, van Tilborg [BMvT78] によって示されている. また, Håstad [Hås01] により近似版 LPN 問題の NP 困難性も示されている.

$\mathsf{LPN}_{n,m,\tau}$ 問題を解くための素朴な方法として, 総当たり法がある. 閾値 $d \geq 1$ を固定する. $\vec{s} \in \mathbb{F}_2^n$ の候補ごとに, $\vec{e} = \vec{b} - \vec{s}\boldsymbol{A}$ を計算し, $\vec{e}$ のハミング重みが $(1+1/d)\tau m$ 以下であれば $\vec{s}$ を解として出力するというものである. Chernoff の補題から $\vec{e} \leftarrow \mathsf{Ber}_\tau^m$ としたとき, $d \geq 1$ について $\Pr[Hw(\vec{e}) \leq (1+1/d)\tau m] \leq \exp(-\tau m/3d^2)$ である. 従ってこの方法を用いると圧倒的な確率で $\mathsf{LPN}_{n,m,\tau}$ 問題を解くことが可能である.

以降では, $O(2^n)$ 以下の時間で解を求めるアルゴリズムについて考察する. 現在では, 大別して 3 つのアルゴリズムが知られている.

1. Blum, Kalai, Wasserman [BKW03] の BKW アルゴリズム,
2. Arora, Ge [AG11] の「再線形化」アルゴリズム,
3. シンドローム復号問題として解くアルゴリズム

である.

4.2.1 BKW アルゴリズムおよびその改良

Blum, Kalai, Wasserman [BKW03] は BKW アルゴリズムと呼ばれるアルゴリズムを提案した.

基本アイデアは以下である. オラクルからのサンプル $(\vec{a}, b)$ が常に $\vec{a} = (1, 0, \ldots, 0)$ という形であれば, $b = s_1 + e$ となる. このようなサンプルを大量に集めれば, s_1 を多数決法で求めることが出来る. 一般に $\vec{u}_j$ を j 番目の単位ベクトルとして, $(\vec{u}_j, b)$ という形のサンプルを集めれば s_j を多数決法で求められる. そこでオラクルからのサンプルを用いて, 上記のようなサンプルを生成することを目指す.

■BKW アルゴリズムの概要: $(a-1)b < n \leq ab$ を満たす適当な自然数 a, b を固定する. 以下では,

$$A_{\vec{s},\delta,i} := \{\vec{a} \leftarrow \mathbb{F}_2^{n-ib} \times \{0\}^{ib}, e \leftarrow \mathsf{Ber}_{(1+\delta)/2} : (\vec{a}, \vec{s} \cdot \vec{a}^\top + e)\}$$

というオラクルを考える. $A_{\vec{s},\delta,i}$ から得たサンプル $(\vec{a}, b)$ は $\vec{a}$ の末尾から ib 要素が必ず 0 である. $i = 0$, $\delta = 1 - 2\tau$ とすれば, $A_{\vec{s},\delta,i} = \mathcal{O}_{\vec{s},\tau}$ となる.

基本アルゴリズムは以下である.

1. $A_{\vec{s},\delta,i}$ からのサンプルを L_0 個用意する.
2. $i = 0, 1, \ldots, a-2$ について, サイズ L_i の $A_{\vec{s},\delta,i}$ からのサンプルを用いて, $O(L_i)$ 時間でサイズ $L_{i+1} = L_i - 2^b$ の $A_{\vec{s},\delta^2,i+1}$ からのサンプルを構成する.
   - サンプル $(\vec{a}, b) \in L_i$ について, $\vec{a} = (a_1, a_2, \ldots, a_{n-ib}, 0, \ldots, 0) \in \mathbb{F}_2^n$ の $(a_{n-(i+1)b+1}, a_{n-(i+1)b+2}, \ldots, a_{n-ib}) \in \mathbb{F}_2^b$ に従って分類を行う.
   - 各組で代表を一つとり, それを $(\vec{a}^*, b^*)$ とする.
   - 各組の代表以外の要素 $(\vec{a}, b)$ を $(\vec{a} \oplus \vec{a}^*, b \oplus b^*)$ で置き換える.

- 全組をまとめてサイズ $L_i - 2^b$ の $A_{\vec{s},\delta^2,i+1}$ からのサンプルとする.

最終的に, サイズ $L_{a-1} = L - (a-1)2^b$ の $A_{\vec{s},\delta^{2^{a-1}},a-1}$ からのサンプルが得られる.

3. 得られた L_{a-1} 個の $A_{\vec{s},\delta^{2^{a-1}},a-1}$ からのサンプルを用いて, s_j を投票で決める.
   - $j = 1, 2, \ldots, n-(a-1)b$ について, $\vec{u}_j$ を $\mathbb{F}_2^n$ の標準基底 j 番目の単位ベクトルとする. サンプル $\{(\vec{a}_i, b_i)\}_{i=1,2,\ldots,m}$ から ℓ 個のベクトルを $\vec{a}_{i_1} + \vec{a}_{i_2} + \cdots + \vec{a}_{i_\ell} = \vec{u}_j$ となるようにうまく選ぶ. このとき, $b_{i_1} + b_{i_2} + \cdots + b_{i_\ell} = s_j + e_{i_1} + e_{i_2} + \cdots + e_{i_\ell}$ となり, ノイズが 0 になる確率は $\Pr[e_{i_1} + e_{i_2} + \cdots + e_{i_\ell} = 0] > 1/2 + (1-2\delta^{2^{a-1}})^\ell/2$ で与えられる. 適当な回数この試行を行い, s_j を多数決投票で決めれば良い.

Blum らの見積もりでは, サンプル数および計算ステップ数は $\delta = 1-2\tau$ として, $\mathrm{poly}\left(\delta^{-2^a}, 2^b\right)$ であった. $\tau < 1/2$ を定数とし, $a = \frac{1}{2}\log n$, $b = 2n/\log n$ とすれば, $2^{O(n/\log n)}$ を得る.

■LF アルゴリズム: Levieil と Fouque [LF06] は BKW アルゴリズムの一部アルゴリズムを改良し LF アルゴリズムを提案した.

簡単のために $n = ab$ を仮定する. BKW アルゴリズムでは基本アルゴリズムのステップ 3 において $\vec{s}$ の各要素を 1 ビットずつ決定している. ステップ 3 において得られたサンプルは, $A_{\vec{s},\delta^{2^{a-1}},a-1}$ からのサンプルであるため, $((a_1, a_2, \ldots, a_b, 0, \ldots, 0), b)$ という形をしている. このとき, $b = \sum_{i=1}^{b} a_i s_i + e$ となり, サンプルに影響を与えるのは, $\vec{s}$ の b ビット分である. LF アルゴリズムでは, $s_1, s_2, \ldots, s_b$ を総当りで計算する.

Levieil と Fouque は BKW アルゴリズムおよび LF アルゴリズムが必要とするサンプル数および計算ステップ数を, 以下のように詳細に解析した.

定理 4.7 *$n = ab$ とし, $\delta = 1-2\tau$ とする.*

- *BKW アルゴリズムはクエリ数 $m = 20\ln(4n)2^b\delta^{-2^a}$, ステップ数 $t = O(nam)$, メモリ量 $M = nm$, 成功確率 $\theta = 1/2$ で $\mathsf{LPN}_{n,m,\tau}$ 問題を解く.*
- *LF アルゴリズムはクエリ数 $m = (8b+200)\delta^{-2^a} + (a-1)2^b$, ステップ数 $t = O(nam)$, メモリ量 $M = nm + b2^b$, 成功確率 $\theta = 1/2$ で $\mathsf{LPN}_{n,m,\tau}$ 問題を解く.*

彼らの報告によれば, LF アルゴリズムと一部のヒューリスティクな手法を用いて $n = 99$, $\tau = 1/4$, $m = 10000$ の LPN 問題を CPU: Pentium 4 (3GHz), RAM: 1GB のマシンで解くことが可能である.

■Kirchner の指摘: Kirchner [Kir11] はランダムに選ばれた $\vec{s}$ よりは Ber_τ に従って選ばれるノイズベクトル $\vec{e}$ の方が, ハミング重みが小さくバリエーションが少ないことに着目した. LPN 問題を Sparse-LPN 問題に置き換えた上で問題を解くことを提案している.

Kirchner の手法は以下のようにまとめられる.

1. Applebaum ら [ACPS09] と同様の手法を用いて, $\mathcal{O}_{\vec{s},\chi}$ というオラクルを $\vec{e}' \leftarrow \mathsf{Ber}_\tau^n$ とランダムに選んだ場合の $\mathcal{O}_{\vec{e}',\chi}$ というオラクルに変換する.
2. BKW アルゴリズムや LF アルゴリズムと同様に基本アルゴリズムのステップ 1, 2 を行う.
3. ステップ 3 で, b ビットを決定する際に, $\vec{e}'$ の該当部分の重みが少ないことを考慮して総当りを行う.

一般の $\vec{s}$ であれば, 総当りに必要な回数は 2^b となる. 一方, $\vec{e}'$ はスパースであることが期待される. $d \geq 1$ を固定し b が十分に大きいとする. このとき, 圧倒的な確率の下で, ハミング重みは $(1+1/d)\tau b$ 以下である. よって, $\vec{e}'$ の候補数は $\binom{b}{(1+1/d)\tau b}$ 以下となり, 総当りに必要な回数が削減される.

表 4.1　Becker らによる確率 1/2 以上で SD 問題を解く場合のパラメータ例 [BJMM12]

	log(時間計算量)/m	log(空間計算量)/m	備考
Lee-Brickel	0.05752	–	[LB88]
Stern	0.05564	0.0135	[Ste88]
BLP	0.05549	0.0148	[BLP11b]
MMT	0.05364	0.0216	[MMT11]
BJMM	0.04934	0.0286	[BJMM12]

■Ring-LPN 問題への応用: Bernstein と Lange [BL12] は Levieil と Fouque の高速化手法および Kirchner のアイデアを用いることにより, Ring-LPN 問題の解法が高速化できることを示している.

4.2.2 Arora-Ge アルゴリズム

Arora と Ge [AG11] は多変数多項式問題で古くから用いられている再線形化と呼ばれる手法を用いて, LPN 問題を解くことを考えた. このアルゴリズムを $\mathsf{LPN}_{n,m,\tau}$ に用いた場合, $w = \tau m$ として, $\mathrm{poly}(n^w)$ 時間で解くことができる. $\mathrm{poly}(n^w) = 2^{O(\tau m \log n)}$ であるから, $\tau = o(n/m \log n^2)$ であれば, BKW アルゴリズムよりも効率が良い.

4.2.3 SD 問題を経由するアルゴリズム

$\mathsf{LPN}_{n,m,\tau}$ に対応するシンドローム復号問題を考える. 対応するシンドローム復号問題での重みを w とする.

この問題を総当りで解く場合には, 重みが w の m 次元ベクトル $\vec{e}$ を列挙すればよい. そのため, 時間計算量は $O(\binom{m}{w})$ となる.

より効率的な手法として, “Information set decoding” と呼ばれる手法が McEliece [McE78] によって提案されている. 近年その高速化が進んでおり, 時間計算量は $2^{m/20}$ にまで引き下げられている. Becker, Joux, May, Meurer [BJMM12] らによる評価例を表 4.1 に示す. この表は, 時間計算量を最小化した場合の $R = n/m$ の最悪時についてまとめられている. 問題のパラメータによっては, 表の数値よりも速く解くことが可能となる.

パラメータ設定によっては, $\mathsf{LPN}_{n,m,\tau}$ 問題を $\mathrm{SD}_{m-n,m,w}$ 問題に置き換えることで, これらの SD 問題用アルゴリズムも検討する必要がある.

4.2.4 量子アルゴリズムへの耐性

現在のところ多項式時間で LPN 問題を解く量子アルゴリズムは提案されていない. [BJLM13] などで一定の高速化は行われているため, 今後も継続して注視する必要がある.

4.3 LPN 問題のアプリケーション

90 年代から様々な応用が提案されている.

擬似乱数生成器　Blum, Furst, Kearns, Lipton [BFKL93] による擬似乱数生成器が有名である. Fischer, Stern [FS96] の構成や Appelbaum, Cash, Peikert, Sahai [ACPS09] による構成も知られている

共通鍵による両側認証　Hopper と Blum によって, 後に HB プロトコルと呼ばれる認証プロトコルが提案され

た [HB01]. 多くの変種が提案されており, 現在も研究が続けられている.

共通鍵暗号 Gilbert, Robshaw, Seurin [GRS08] による LPN-C と呼ばれる IND-CPA 安全な共通鍵暗号方式がある. Applebaum, Cash, Peikert, Sahai [ACPS09] は, LPN-C の変種が KDM-CPA 安全であることを示した. また Applebaum, Harnik, Ishai [AHI11] は ACPS09 の共通鍵方式が RKA-CPA 安全であることを示し, OT への応用を考察している. Applebaum [App13] は ACPS09 の共通鍵方式が RKA-KDM-CPA 安全であることを示し, このような方式を用いれば, Free-XOR 構成を用いた Yao's GC が標準モデルで安全であることを示した.

署名 大別して二つのタイプがある.

- Fiat-Shamir 変換: Stern の認証方式や Veron の認証方式に Fiat-Shamir 変換を施すことによって得られる署名である. 署名長の観点から効率が悪く実用には向いていない.
- FDH 系 CFS 署名が知られている.

標準モデルでの安全性証明は行われていない.

公開鍵暗号 大きく分けて二つの系統がある.

- Alekhnovich 暗号: Alekhnovich [Ale11] 暗号は LPN 仮定のみから IND-CPA 安全性を証明可能な方式である. IND-CCA2 版は Döttling, Müller-Quade, Nasciment [DMQN12] によって構成されている.
- McEliece 暗号または Niederreiter 暗号: McEliece [McE78] および Niederreiter [Nie86] によって提案された暗号である. Li, Deng, Wang [LDW94] が「Niederreiter 暗号の OW-CPA 性は McEliece 暗号の OW-CPA 性と等価である」ことを示している.
  - McEliece 系 Kobara, Imai [KI01] は McEliece 暗号用のパディング方法を提案し, その方式がランダムオラクルモデルで ND-CCA2 安全であることを示した. Nojima, Imai, Kobara, Morozov [NIKM08] は McEliece 暗号の変種が標準モデルで IND-CPA 安全でああることを示した. McEliece 暗号を基にした IND-CCA2 暗号については [DDMQN12] や Persichetti [Per13] に構成が見られる.
  - Niederreiter 系 StdM での IND-CCA2 安全な Niederreiter ベースの暗号としては, Freeman, Goldreich, Kiltz, Rosen, Segev の構成 [FGK+13] や, Mathew, Vasant, Venkatesan, Rangan の構成 [MVVR12] が知られている.

紛失転送 McEliece 暗号を用いた紛失転送プロトコルが提案されている [DvdGMQN12, DNdS12, DNMQ12].

4.4 追加の問題・制約

McEliece 暗号や Niederreiter 暗号の安全性証明では, McEliece 仮定と呼ばれる仮定が必要となる. 以下では, S_m で m 次対称群をあらわす.

定義 4.8 (McEliece 仮定) $[m(n), n, d(n)]_{q(n)}$-符号のクラス $\mathcal{C}$ を固定する. 敵 $\mathcal{A}$ の優位性を

$$\mathsf{Adv}_{\mathcal{A}}(n) = \left| \Pr_{\boldsymbol{S}\leftarrow \mathrm{GL}_n(\mathbb{F}_q), \boldsymbol{G'}\leftarrow\mathcal{C}, \boldsymbol{P}\leftarrow S_m}[\mathcal{A}(1^n, \boldsymbol{G} = \boldsymbol{SG'P}) = 1] - \Pr_{\boldsymbol{G}\leftarrow\mathbb{F}_q^{n\times m}}[\mathcal{A}(1^n, \boldsymbol{G}) = 1] \right|$$

で定義する. 任意の多項式時間の敵 $\mathcal{A}$ について, その優位性が無視できる関数であるとき, McEliece 仮定が成立するという.

左側の敵は McEliece 暗号の公開鍵（または Niederreiter 暗号の公開鍵の双対）を受け取っている. そのため, この仮定は, McEliece 暗号の公開鍵はランダムな同サイズの行列と見分けが付かないということを意味する.

表 4.2　Damgård と Park によるパラメータ設定の例 ([DP12] より)

セキュリティレベル	n	τ
80-bit	9000	0.0044
112-bit	21000	0.0029
128-bit	29000	0.0024
196-bit	80000	0.0015
256-bit	145000	0.0011

Faugère, Gauthier-Umaña, Otmani, Perret, Tillich [FGOPT13] は元となる Goppa 符号 (または Alternant 符号) のレートが高い場合には, McEliece 仮定を破るアルゴリズムを提案している.

また, McEliece 符号や Niederreiter 暗号で用いる符号が特殊な場合には, 多くの方式が破られている. そのため, 符号の選択には注意が必要である.

4.5　まとめ

これまでのところ, τ や n が十分大きい場合には, 現実的な時間で解を求めることは不可能である.

LPN 問題をベースとした暗号方式を実際に構成する際には, 4.2 節で挙げた各種のアルゴリズムに耐性を持つよう, パラメータ設定を行う必要がある. たとえば, Damgård と Park [DP12] は Alekhnovich 暗号の変種として公開鍵暗号を提案し, Bernstein と Lange の攻撃 [BL12] を元にしたパラメータ設定 (表 4.2) を行っている.

また McEliece 暗号やその変種を用いる場合には, 4.4 節で挙げたように, 符号の選定やパラメータの設定おいて, より一層の注意が必要である. Bernstein, Lange, Peters が [BLP10] および [BLP11a] で q 進-Goppa 符号を用いた q 進-McEliece 暗号についてパラメータの提案を行っている.　具体的なチャレンジ問題も `http://pqcrypto.org/wild-challenges.html` から入手可能である.　たとえば 128-bit 安全性を考える際には, $(q, n, m, \tau m) = (2, 2325, 3009, 57)$ といったパラメータを提案している.

LPN 問題の安全性評価については理論的なものが多く, 攻撃実験報告は小さいパラメータに対して行ったものが多い. そのため, 攻撃実験に関する研究もこれから非常に重要である.

第 4 章の参照文献

[Ale11] Michael Alekhnovich, “More on average case vs approximation complexity,” Computational Complexity 20(4): 755-786 (2011).

[App13] Benny Applebaum, “Garbling XOR gates “For Free” in the standard model,” TCC 2013: 162-181.

[ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai, “Fast cryptographic primitives and circular-secure encryption based on hard learning problems,” CRYPTO 2009: 595-618.

[AHI11] Benny Applebaum, Danny Harnik, and Yuval Ishai, “Semantic security under related-key attacks and applications,” ICS 2011: 45-60.

[AG11] Sanjeev Arora and Rong Ge, “New algorithms for learning in presence of errors,” ICALP (1) 2011: 403-415.

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer, “Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding,” EUROCRYPT 2012: 520-536.

[BMvT78] Elwyn R. Berlekamp, Robert J. McEliece, and Henk C. A. van Tilborg, “On the inherent intractability of certain coding problems,” IEEE Transactions on Information Theory 24(3): 384-386 (1978).

[BJLM13] Daniel J. Bernstein, Stacey Jeffery, Tanja Lange, and Alexander Meurer, “Quantum algorithms for the subset-sum problem,” PQCrypto 2013: 16-33.

[BLP10] Daniel J. Bernstein, Tanja Lange, and Christiane Peters, “Wild McEliece,” SAC 2010: 143-158.

[BLP11a] Daniel J. Bernstein, Tanja Lange, and Christiane Peters, “Wild McEliece incognito,” PQCrypto 2011: 244-254.

[BLP11b] Daniel J. Bernstein, Tanja Lange, and Christiane Peters, “Smaller decoding exponents: Ball-collision decoding,” CRYPTO 2011: 743-760.

[BL12] Daniel J. Bernstein and Tanja Lange, “Never trust a bunny,” RFIDSec 2012: 137-148.

[BFKL93] Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton, “Cryptographic primitives based on hard learning problems,” CRYPTO 1993: 278-291.

[BKW03] Avrim Blum, Adam Kalai, and Hal Wasserman, “Noise-tolerant learning, the parity problem, and the statistical query model,” J. ACM 50(4): 506-519 (2003).

[DP12] Ivan Damgård and Sunoo Park, “Is public-key encryption based on LPN practical?” IACR Cryptology ePrint Archive 2012: 699 (2012). 20140126:205953 版.

[DvdGMQN12] Rafael Dowsley, Jeroen van de Graaf, Jorn Muller-Quade, and Anderson C. A. Nascimento, “Oblivious Transfer Based on the McEliece Assumptions,” IEICE Transactions 95-A(2): 567-575 (2012).

[DNdS12] Bernardo Machado David, Anderson C. A. Nascimento, and Rafael T. de Sousa Jr., “Efficient Fully Simulatable Oblivious Transfer from the McEliece Assumptions,” IEICE Transactions 95-A(11): 2059-2066

(2012).

[DNMQ12] Bernardo Machado David, Anderson C. A. Nascimento, and Jorn Müller-Quade, "Universally Composable Oblivious Transfer from Lossy Encryption and the McEliece Assumptions," ICITS 2012: 80-99.

[DMQN12] Nico Döttling, Jorn Müller-Quade, and Anderson C. A. Nasciment, "IND-CCA secure cryptography based on a variant of the LPN problem," ASIACRYPT 2012: 485-503.

[DDMQN12] Nico Döttling, Rafael Dowsley, Jorn Müller-Quade, and Anderson C. A. Nasciment, "A CCA2 secure variant of the McEliece cryptosystem," IEEE Transactions on Information Theory 58(10): 6672-6680 (2012).

[FGOPT13] Jean-Charles Faugère, Valérie Gauthier-Umaña, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich, "A distinguisher for high-rate McEliece cryptosystems," IEEE Transactions on Information Theory 59(10): 6830-6844 (2013).

[FS96] Jean-Bernard Fischer and Jacques Stern, "An efficient pseudo-random generator provably as secure as syndrome decoding," EUROCRYPT 1996: 245-255.

[FGK+13] David Mandell Freeman, Oded Goldreich, Eike Kiltz, Alon Rosen, and Gil Segev, "More constructions of lossy and correlation-secure trapdoor functions," J. Cryptology 26(1): 39-74 (2013).

[GRS08] Henri Gilbert, Matthew J.B. Robshaw, and Yannick Seurin, "HB$^{\#}$: Increasing the security and efficiency of HB+," EUROCRYPT 2008: 361-378.

[GRS08] Henri Gilbert, Matthew J.B. Robshaw, and Yannick Seurin, "How to encrypt with the LPN problem," ICALP (2) 2008: 679-690.

[Hås01] Johan Håstad, "Some optimal inapproximability results," J. ACM 48(4): 798-859 (2001).

[HKL+12] Stefan Heyse, Eike Kiltz, Vadim Lyubashevsky, Christof Paar, and Krzysztof Pietrzak, "Lapin: An efficient authentication protocol based on ring-LPN," FSE 2012: 346-365.

[HB01] Nicholas J. Hopper and Manuel Blum, "Secure human identification protocols," ASIACRYPT 2001: 52-66.

[JKPT12] Abhishek Jain, Stephan Krenn, Krzysztof Pietrzak, and Aris Tentes, "Commitments and efficient zero-knowledge proofs from learning parity with noise," ASIACRYPT 2012: 663-680.

[KSS10] Jonathan Katz, Ji Sun Shin, and Adam Smith, "Parallel and concurrent security of the HB and HB+ protocols," J. Cryptology 23(3): 402-421 (2010).

[KPC+11] Eike Kiltz, Krzysztof Pietrzak, David Cash, Abhishek Jain, and Daniele Venturi. "Efficient authentication from hard learning problems," EUROCRYPT 2011: 7-26.

[Kir11] Paul Kirchner, "Improved generalized birthday attack," IACR Cryptology ePrint Archive 2011: 377 (2011).

[KI01] Kazukuni Kobara and Hideki Imai, "Semantically secure McEliece public-key cryptosystems – conversions for McEliece PKC," PKC 2001: 19-35.

[LB88] Pil Joong Lee and Ernest F. Brickell, "An observation on the security of McEliece's public-key cryptosystem," EUROCRYPT 1988: 275-280.

[LF06] Éric Levieil and Pierre-Alain Fouque, "An improved LPN algorithm," SCN 2006: 348-359.

[LDW94] Yuan Xing Li, Robert H. Deng, and Xin Mei Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," IEEE Transactions on Information Theory 40(1): 271-273 (1994).

[MVVR12] K. Preetha Mathew, Sachin Vasant, Sridhar Venkatesan, and C. Pandu Rangan, "An efficient IND-

CCA2 secure variant of the Niederreiter encryption scheme in the standard model," ACIPS 2012: 166-179.

[MMT11] Alexander May, Alexander Meurer, and Enrico Thomae, "Decoding random linear codes in $\tilde{\mathcal{O}}(2^{0.054n})$," ASIACRYPT 2011: 107-124.

[McE78] Robert J. McEliece, "A public-key cryptosystem based on algebraic coding theory," Jet Propulsion Laboratory DSN Progress Report 42-44: 114-116 (1978).

[Nie86] Harald Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," Problems of Control and Information Theory 15: 19-34. Problemy Upravleniĭa i Teorii Informat͡sii 15: 159-166 (1986).

[NIKM08] Ryo Nojima, Hideki Imai, Kazukuni Kobara, and Kirill Morozov, "Semantic security for the McEliece cryptosystem without random oracles," Designs, Codes and Cryptography 49: 289-305 (2008).

[Per13] Edoardo Persichetti, "Improving the Efficiency of Code-Based Cryptography," University of Auckland, 2013.

[Pie12a] Krzysztof Pietrzak, "Subspace LWE," TCC 2012: 548-563.

[Pie12b] Krzysztof Pietrzak, "Cryptography from learning parity with noise," SOFSEM 2012: 99-114.

[Reg09] Oded Regev, "On lattices, learning with errors, random linear codes, and cryptography," J. ACM, 56(6): 1–40 (2009).

[Ste88] Jacques Stern, "A method for finding codewords of small weight," Coding Theory and Applications 1988: 106-113.

第 5 章

Approximate Common Divisor 問題

5.1 Approximate Common Divisor 問題の概説

5.1.1 Approximate Common Divisor 問題とは

Approximate Common Divosr 問題 (ACDP) は，CaLC2011 において，Howgrave-Graham により，導入された問題である [HG01]．いくつかの暗号方式の安全性評価が，この問題を経由することにより行われている．Approximate Common Divisor (ACD) 問題は，次のように定式化される．

定義 5.1 (ACD 問題（その 1）) p を未知の素数とし，p の倍数 N は，既知であるとする．r を，その絶対値が N^{α} 以下の整数とする．q を N/p 程度の乱数として，

$$x = pq + r$$

とする．x が与えられた時に，r を求める問題である．

この問題に対して，法を p として簡約したものを考えることが多い．すなわち，次の問題を ACD 問題とみなすことも多い．

定義 5.2 (ACD 問題（その 2）) N を合成数として，p は，N の未知の素因数とする．ただし，$p \approx N^{\beta}$ とする．a を与えられた整数として，

$$a + x \equiv 0 \pmod{p}$$

をみたす x を求める問題である．ただし，$\alpha \leq \beta$ に対して，解 x は，$|x| < N^{\alpha}$ を満たしているとする．

5.1.2 Approximate Common Divisor 問題の拡張

ACD 問題は，いくつかの拡張問題を持つ．ここでは，以下の問題を考える．

定義 5.3 (複数 ACD 問題（その 1）[CMNT11]) p を未知の素数とする．q を十分大きい自然数として,，$N = pq$

とする．この N は既知であるとする．r_i を絶対値が N^α 以下の整数とする．q_i を q 程度の乱数として，

$$\begin{cases} x_1 &= pq_1 + r_1 \\ x_2 &= pq_2 + r_2 \\ &\vdots \\ x_n &= pq_n + r_n \end{cases}$$

とする．$x_1, x_2, \ldots, x_n$ が与えられた時に，$r_1, r_2, \ldots, r_n$ を求める問題である．

同様に，以下のようにも定式化される．

定義 5.4 (複数 ACD 問題（その２）) N を合成数として，p は，N の未知の素因数とする．ただし，$p \approx N^\beta$ とする．$a_1, \ldots, a_n$ を与えられた整数として，

$$\begin{cases} a_1 + x_1 &\equiv 0 \pmod{p} \\ a_2 + x_2 &\equiv 0 \pmod{p} \\ &\vdots \\ a_n + x_n &\equiv 0 \pmod{p} \end{cases}$$

をみたす $x_1, x_2, \ldots, x_n$ を求める問題である．ただし $\alpha_1, \alpha_2, \ldots, \alpha_n \leq \beta$ となる α_i に対して，解 $x_1, x_2, \ldots, x_n$ は，$|x_i| < N^{\alpha_i}$ を満たしているとする．簡単のため，$\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n$ であるとする．

N が与えられない問題を，General ACD 問題 (GACD 問題) と呼ぶ．この問題と区別するため，N が与えられる問題を Partial ACD 問題 (PACD 問題) と呼ぶこともある．明らかに，同一の n に対して，GACD 問題の方が，PACD 問題よりも困難である．複数 GACD 問題は，以下のように定義される，

定義 5.5 (複数 GACD 問題) p を未知の素数，N を γ ビットの自然数として，$p \approx N^\beta$ とする．q_i を 0 から N/p の間の乱数とし，r_i を絶対値が N^α 以下の整数とする．$x_1, x_2, \ldots, x_n$ を

$$\begin{cases} x_1 &= pq_1 + r_1 \\ x_2 &= pq_2 + r_2 \\ &\vdots \\ x_n &= pq_n + r_n \end{cases}$$

とする．$x_1, x_2, \ldots, x_n$ が与えられた時に，$r_1, r_2, \ldots, r_n$ を求める問題である．

5.1.3 Approximate Common Divisor 問題のアプリケーション

van Dijk ら [DGHV10] は，複数 GACD 問題の困難さを安全性の根拠としてもつ，整数上での完全準同型暗号を提案している．さらに，仮定を複数 PACD 問題の困難さに強めることにより，効率的になることを述べている．ついで，Coron ら [CMNT11] は，公開鍵サイズを削減する方式を提案している．彼らの方式も，複数 PACD 問題の困難さを安全性の根拠としている．

[DGHV10] および [CMNT11] では，以下のように述べられている．

[DGHV10] では，Approximate GCD 問題を次のように定義している．正の奇数 p に対して，γ ビットの整数上の分布 $\mathcal{D}_{\gamma,\rho}(p)$ を考える．$\mathcal{D}_{\gamma,\rho}(p)$ は，p を受け取り，0 から $2^\gamma/p$ の間の整数 q をランダムに選び，-2^ρ から 2^ρ の間の整数 r をランダムに選び，$x = pq + r$ を出力する．

(ρ, η, γ)-approximate GCD 問題とは，ランダムに選ばれた η ビットの奇数 p に対して，$\mathcal{D}_{\gamma,\rho}(p)$ からの多項式的に多くのサンプルが与えられた時に，p を求める問題である．

[DGHV10] で提案された somewhat 準同型暗号方式の安全性は，以下のように示されている．ここで，用いるパラメタを $(\rho, \rho', \eta, \gamma, \tau)$ とする．このとき，advantage ϵ で方式を破る攻撃者 A は，(ρ, η, γ)-approximate GCD 問題を，確率 $\epsilon/2$ 以上で，解くアルゴリズム B に変換することができる．アルゴリズム B の動作時間は，A の動作時間，$\lambda, 1/\epsilon$ の多項式である．

[CMNT11] では，Error-free Approximate GCD 問題を次のように定義している．正の奇数 p, q_0 に対して，整数上の分布 $\mathcal{D}'_\rho(p, q_0)$ を考える．$\mathcal{D}'_\rho(p, q_0)$ は，p と q_0 を受け取り，0 から q_0 の間の整数 q をランダムに選び，-2^ρ から 2^ρ の間の整数 r をランダムに選び，$x = pq + r$ を出力する．

(ρ, η, γ)-error-free approximate GCD 問題とは，ランダムに選ばれた η ビットの奇数 p とランダムに選ばれた square-free かつ 2^λ-rough で，0 から $2^\gamma/p$ の間の整数 q_0 に対して，$x_0 = q_0 p$ と $\mathcal{D}'_\rho(p、q_0)$ からの多項式的に多くのサンプルが与えられた時に，p を求める問題である．

[DGHV10] で提案された somewhat 準同型暗号方式の安全性は，以下のように示されている．ここで，用いるパラメタを $(\rho, \rho', \eta, \gamma, \tau)$ とする．このとき，advantage ϵ で方式を破る攻撃者 A は，(ρ, η, γ)-error-free approximate GCD 問題を，確率 $\epsilon/2$ 以上で，解くアルゴリズム B に変換することができる．アルゴリズム B の動作時間は，A の動作時間，$\lambda, 1/\epsilon$ の多項式である．

さらに，[CCK+13] では，中国人の剰余定理を用いる事により，バッチ処理が可能な方式を提案している．この論文中では，新たに，判定 Approximate GCD 問題を導入し，この問題の困難さを安全性の根拠とした方式を提案している．さらに，提案方式をベースに，128 ビット AES 回路の実装を行っている．72 ビットセキュリティを担保した上で，13 分以内で，暗号化の処理が終了すると報告している．この論文では，後に述べる [CN11] による攻撃を考慮した上で，パラメタ設定を行っている．

以上の記述では，原論文での記述を採用している．そのため，用いるパラメタが異なっているが，$\eta = \beta \log N, \rho = \alpha \log N, \gamma = \log N$ という関係にあることに注意されたい．

5.2 ACD 問題に対する評価

PACD 問題は，N の素因数分解を経由することにより，容易に解くことができる．具体的には，以下の手順による．まず，N を素因数分解をすることにより，p を求める．求めた p を用いることにより，x を求めることができる．法が既知の一次方程式 $a + x \equiv 0 \pmod{p}$ を解くことは，容易であるためである．これ以降，N の素因数分解を，直接的には，経由しないアルゴリズムを考察する．

N の素因数分解を直接的には経由しないアルゴリズムを，以下の二つに大別して説明をする．

1. 組み合わせ論に基づくアルゴリズム
2. 格子理論に基づくアルゴリズム

前者のアルゴリズムは，指数関数時間アルゴリズムではあるが，解に制約は存在しない．すなわち，どのような α に対しても，解を求めることが可能である．しかし，計算量は，α に依存する．その一方で，後者のアルゴリズムは，解くことができる解に制約が存在するものの，解がその制約をみたせば，多項式時間で求解が可能である．すなわち，任意の α に対して，解を求めることができる訳ではなく，制限が存在するが，十分高速に解を求めることができる．そのため，求める問題に応じて，適切なアルゴリズムの選択が重要である．

5.2.1 組み合わせ論に基づくアルゴリズム

PACD 問題を解く最も素朴なアルゴリズムは，全数探索アルゴリズムである．解 x の可能な値は，$2N^{\alpha}$ 個であるので，全数探索により，$\tilde{O}(N^{\alpha})$ の計算量で解の探索が可能である．これは，ビット長 $\log N$ に対して，指数関数時間必要である．

Chen と Nguyen は，全数探索よりも効率的に，解を求めるアルゴリズムを提案している [CN11]．彼らは，multipoint evaluation of univariate polynomials というテクニックを導入することにより，効率化に成功している．まず，このテクニックについて説明する．整数係数でモニックな 1 変数 n 次多項式 $f(x)$ を考える．$a_1, a_2, \ldots, a_n$ を整数として，$f(a_1), f(a_2), \ldots, f(a_n)$ の値全てを計算したい状況を考える．素朴なアルゴリズムでは，この計算には，$O(n^2)$ の計算量が必要である．これに対して，彼らは，$\tilde{O}(n)$ の計算量で，$f(a_1), f(a_2), \ldots, f(a_n)$ の全てを計算するアルゴリズムを提案している．すなわち，平方根の高速化が実現している．彼らは，PACD 問題を，multipoint evaluation of univariate polynomials に帰着した上で，このアルゴリズムを適用することにより，PACD 問題を解くアルゴリズムを構成している．実際の計算量は，

$$\tilde{O}(N^{\alpha/2})$$

で与えられる．

Chen と Nguyen[CN11] は，提案アルゴリズムを実装することにより，Coron らの論文 [CMNT11] 中で提示された推奨パラメタに対して，安全性の再評価を行っている．再評価結果を表 5.1 に記す．表中，「Secrutiy Level」の欄は，総当たりの攻撃により，見積もられた Security Level である．その一方で，「新しい Security Level」の欄は，Chen-Nguyen の攻撃により見積もられた Security Level である．従来の見積もりよりも，安全性が低下していることが確認できる．

表 5.1　Chen–Nguyen アルゴリズムによる評価（[CN11] より）

Name	Toy	Small	Medium		Large	
Security Level	52	61	72		100	
計算時間の見積もり	1.6 分	7.1 時間	190 日	76 日	2153 年	9 年
使用メモリ量	$\leq$ 130 Mb	$\leq$ 15 Gb	$\leq$ 72 Gb	$\approx$ 240 Gb	$\leq$ 72 Gb	$\approx$ 25 Tb
新しい Security Level	$\leq$ 37.7	$\leq$ 45.7	$\leq$ 55	$\leq$ 54	$\leq$ 67	$\leq$ 59

5.2.2 格子理論に基づくアルゴリズム

一般に，暗号の安全性解析において，格子理論にもとづくアルゴリズム [Cop95, Cop96, Cop97, HG97] は，重要なツールである．ここでは，格子理論を用いた ACD 問題を解くアルゴリズムについて説明する．Partial ACD 問題を解く格子理論に基づくアルゴリズムの中で，現状で最も優れたアルゴリズムは，Howgrave-Graham によるアルゴリズムである [HG01]．このアルゴリズムでは，α と β が，

$$\alpha < \beta^2 \tag{5.1}$$

を満たすときに，多項式時間で解を求めることが可能である．

この結果を用いると，よく知られた以下の結果を，容易に導くことができる [Cop96:A].

RSA タイプの合成数 $N = pq$ に対して，p の上位半分のビットがわかった時に，素因数分解が可能である．

RSA 型の合成数 $N = pq$ に対して，p の近似値 $\tilde{p}$ がわかった場合を考える．$x = p - \tilde{p}$ とおくと，$\tilde{p} + x \equiv 0 \pmod{p}$ が成り立つ．このため，PACD 問題が解ければ，素因数分解が可能となる．$p \approx N^{1/2}$ の時，すなわち，$|p - \tilde{p}| < N^{1/4}$ の時には，素因数分解が可能となる．具体的には，p の上位半分がわかれば，素因数分解が可能である．

5.2.3 量子アルゴリズムへの耐性

前述のように，Partial ACD 問題は，N の素因数分解ができれば，簡単に解くことができる．量子計算機を用いることができれば，Shor のアルゴリズム [Shor94] により，多項式時間で素因数分解を行うことができるため，PACD 問題を解くことは容易である．

5.2.4 ACD 問題に対する評価のまとめ

以上の議論をまとめる．Partial ACD 問題は，

1. 解の大きさに $\alpha < \beta^2$ という制限がある場合には，多項式時間で解くことができる．
2. その一方で， 解の大きさに制限がない場合には，$\tilde{O}(N^{\alpha/2})$ の計算量で解を求めることが可能である．

問題の設定により，最適なアルゴリズムが異なるため，適切な選択が必要である．

5.3 複数 ACD 問題に対する評価

5.3.1 組み合わせ論に基づくアルゴリズム

複数 ACD 問題に対しても，最も素朴なアルゴリズムは，全数探索アルゴリズムである．解 $x_1, x_2, \ldots, x_n$ のうち，一つでも値を求めることができれば，p を求めることができるため，$x_1, x_2, \ldots, x_n$ の全てを求めることが可能である．このため，x_1 をまず求めることにする．このとき，x_1 の取りうる値の可能な個数は，$2N^{\alpha_1}$ である．そのため，複数 ACD 問題を全数探索アルゴリズムにより解く計算量は，$\tilde{O}(N^{\alpha_1})$ で与えられる．

同様に，Chen-Nguyen のアルゴリズム [CN11] により，$\tilde{O}(N^{\alpha_1/2})$ の計算量で，この問題を解くことができる．このアルゴリズムでは，複数の方程式が与えられていることを有効に活用できていない．

5.3.2 格子理論に基づくアルゴリズム

5.3.2.1 Coppersmith 流のアルゴリズム

格子理論に基づくアルゴリズムにより，複数 ACD 問題を多項式時間で解くことができる条件を示す．前述の Howgrave-Graham アルゴリズム [HG01] を用いることにより，$\alpha_1 < \beta^2$ であれば，解を求めることができる．このアルゴリズムでも，方程式が複数個得られていることを活用していない．

ANTS2012 において，Cohn と Heninger は，$\beta \gg \frac{1}{\sqrt{\log N}}$ という条件下で，

$$\frac{\alpha_1 + \alpha_2 + \cdots + \alpha_n}{n} < \beta^{(n+1)/n}$$

の時に，多項式時間で解を求めるこができることを示している [CH11]．各 α_i が，全て等しく α であるとする．このとき，$\alpha < \beta^{(n+1)/n}$ の時に，解を求めることができる．

その一方で，Cohn と Heninger の結果は，α_i が等しく無い場合には，必ずしも最適ではない．これに対して，Takayasu と Kunihiro は，解くことができる条件の改良を行っている [TK13]．彼らは，

$$\sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n} < \beta^{(n+1)/n}$$

の時に多項式時間で解を全て求めることができることを示している．常に，

$$\frac{\alpha_1+\alpha_2+\cdots+\alpha_n}{n} \geq \sqrt[n]{\alpha_1\alpha_2\cdots\alpha_n}$$

が成り立つため，彼らの条件は，Cohn–Heninger の条件の改良となっている．ただし，各 α_i が，全て等しく α であるときには，この条件は，$\alpha < \beta^{(n+1)/n}$ となり，Cohn-Heninger の結果と一致する．

この結果の妥当性を検証する．$\alpha_1 = \beta^2$ であれば，$2 \leq i \leq n$ となる i に対して，$\alpha_i = \beta$ と取ることができるため，Takayasu–Kunihiro の結果は，Howgrave-Graham の結果の自然な拡張となっている．

5.4 GACD 問題の格子理論を用いたアルゴリズム

GACD 問題を解くアルゴリズムに関して，議論する．

5.4.1 組み合わせ論に基づくアルゴリズム

Chen と Nguyen は，PACD 問題を解くアルゴリズムを拡張により，General ACD 問題を，$\tilde{O}(N^{3\alpha/2})$ で解くことができることを示している [CN11]．総当たりのアルゴリズムでは，$\tilde{O}(N^{2\alpha})$ の計算量が必要であるため，指数関数の高速化を実現している．このとき，必要となるメモリ量は，$\tilde{O}(N^{\alpha/2})$ である．

Chen と Nguyen のアルゴリズムは，GACD の 2 個のサンプルしか用いていないが，積極的に複数個のサンプルを用いることにより計算量の削減が可能である．Coron らは，[CNT12] において，計算量 $\tilde{O}(N^{\alpha})$，メモリ量 $\tilde{O}(N^{\alpha})$ のアルゴリズムを提案している．

5.4.2 格子理論に基づくアルゴリズム

次に，格子理論に基づくアルゴリズムを述べる，Coppersmith の手法に基づくように，十分大きい法に対して成り立つ関係式を用いて，法を外し，整数上の方程式に変換してから解く方法と，解を最短ベクトルに埋め込むことにより解く方法を紹介する．この二つの方法の一般論に関しては，[K11] に詳しい．

5.4.2.1 Coppersmith の手法に基づく解析

Howgrave-Graham は，$n = 2$ の時の解析を行っている [HG01]．$n = 2, \alpha_1 = \alpha_2 := \alpha$ の時は，

$$\alpha < 1 - \frac{1}{2}\beta - \sqrt{1 - \beta - \frac{1}{2}\beta^2}$$

であれば，解を求めることができることを示している．一般の n の状況に関しては，Cohn と Heninger は，

$$\alpha < \frac{1 - 1/n^2}{n^{1/(n-1)}}\beta^{n/(n-1)}$$

のときに，多項式時間で解を求めることができることを示している [CH11].

5.4.2.2 最短ベクトルに埋め込む解法

次に，解きたい解を短いベクトルに埋め込む手法を用いた場合の解析について説明する．[DGHV10] では，Lagarias の同時 Diophantine 近似 (SDA) 問題を解くアルゴリズムを利用することにより，複数 ACD 問題が難しくなるかを評価している．今，サンプルは，$t+1$ 個用いるとする．$t+1 < \gamma/\eta$ の時には，解を埋め込んだベクトルが最短ベクトルにならないことを指摘している．そのため，LLL アルゴリズムなど格子簡約アルゴリズムなどを用いても，解を見つけることができない．その一方で，t が大きいときには，埋め込んだベクトルが最短になりやすくなる．しかし，この場合，用いる格子の次元が大きくなりすぎるため，効率的に解を求めることができない．経験的に，最短ベクトルの 2^k の近似精度でベクトルを求めるためには，$2^{t/k}$ の計算時間が必要である．そのため，$t \geq \gamma/\eta$ の時には，2^{η} の近似精度を実現するためには，およそ $2^{\gamma/\eta^2}$ の計算時間が必要である．そのため，γ/η^2 を $\log \lambda$ 程度に設定をすれば，全体の計算時間は指数関数時間になる．

さらに，[DGHV10] では，Nguyen と Stern による orthogonal 格子を用いた場合の解析も行っている．SDA 問題を経由するときと同様に，解を求めるためには，$2^{\gamma/\eta^2}$ 程度の計算量が必要であることを述べている．

5.4.3 完全準同型暗号の安全性への影響

いずれの攻撃においても，適切にパラメタが設定された状況では，攻撃に成功するのに，指数関数時間が必要であり，脆弱性は発見されていない．しかし，いずれも，理論上の解析であるため，数値実験により安全性の検証をする必要がある．

5.5 まとめ

この節の議論をまとめる．現状において，ACD 問題は，パラメタを適切に選ぶ事により，現実的な時間で解を求めることは不可能である．つまり，法に対して，解が，ある制限よりも小さいときには，多項式時間で解くことができるものの，その一方で，解が十分大きいときには，解を求めることができない．組み合わせ論に基づくアルゴリズムを用いた場合では，依然，指数関数時間の計算量が必要であるが，全数探索アルゴリズムの平方根の計算量で解を求めることができる．Chen–Nguyen のアルゴリズムは，暗号の提案時には，考慮されていなかった攻撃であり，実際に，提案論文で書かれた推奨パラメタのいくつかは，解読されることが示されている．この結果は，ごく最近に示されたものであり，今後の研究の動向に注視する必要がある．

第 5 章の参照文献

[CN11] Y. Chen and P. Q.Nguyen, “Faster Algorithms for Approximate Common Divisors: Breaking Fully-Homomorphic-Encryption Challenges over the Integers,” EUROCRYPT 2012, LNCS 7237, pp 502–519, 2012.

[CCK+13] J. H. Cheon, J.-S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi and A. Yun, “Batch Fully Homomorphic Encryption over Integers,” EUROCRYPT 2013, LNCS 7881, pp 315–335, 2013.

[CH11] H. Cohn, N. Heninger, “Approximate common divisors via lattices,” Proc. of ANTS 2012.

[Cop95] D. Coppersmith, “Factoring with a hint,” IBM Research Report RC 19905, 1995.

[Cop96] D. Coppersmith, “Finding a Small Root of a Univariate Modular Equation,” Advances in Cryptology – Eurocrypt ’96, LNCS 1070, Springer-Verlag, pp. 155–165, 1996.

[Cop96:A] D. Coppersmith, “Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known,” Advances in Cryptology – Eurocrypt ’96, LNCS 1070, Springer-Verlag, pp. 178–189, 1996.

[Cop97] D. Coppersmith, “Small solutions to polynomial equations, and low exponent RSA vulnerabilities,” Journal of Cryptology 10: 233, 260, 1997.

[CMNT11] J. -S. Coron, A. Mandal, D. Naccache, M. Tibouchi, “Fully homomorphic encryption over the integers with shorter public keys,” CRYPTO 2011, LNCS 6841, pp. 487–504, Springer-Verlag, 2011.

[CNT12] J. -S. Coron, D. Naccache, M. Tibouchi, “Public key compression and modulus switching for fully homomorphic encryption over the integers,” EUROCRYPT 2012, LNCS 7237, pp. 446–464, Springer-Verlag, 2012.

[DGHV10] M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, “Fully homomorphic encryption over the integers,” Proc. of Eurocrypt 2004, pp. 14–27. LNCS 6110. Springer-Verlag, Berlin, Heideberg , 2010. Longer version available as Report 2009/616 in the Cryptology ePrint Archive(http://eprint.iacr.org/2009/616).

[HG97] N. Howgrave-Graham, “Finding small roots of univariate modular equations revisited,” Proc. of Cryptography and Coding, LNCS 1355, pp. 1331–142, 1997.

[HG01] N. Howgrave-Graham, “Approximate integer common divisors,” Proceedings of CALC 2001, LNCS 2146, pp. 51–66, Springer, 2001.

[K11] 國廣 昇，“格子理論を用いた暗号解読の最近の研究動向,” 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review，Vol. 5, no. 1, pp. 42-55, 2011.

[Shor94] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in Proc. of 35nd Annual Symposium on Foundations of Computer Science, pp. 124–134, 1994.

[TK13] A. Takayasu and N. Kunihiro, “Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors,” in Proc. of ACISP2013, LNCS 7959, pp. 118–135, 2013.

離散対数問題の困難性に関する調査
関数体篩法の近年の改良とその影響について

2014 年 3 月

1 概説

有限体上の離散対数問題を解くことの計算の困難性はペアリング暗号の安全性の基盤となっており, 有限体はペアリング暗号の安全性を決定する重要な暗号パラメータとみなされる. さらに, 有限体はペアリング暗号の暗号処理速度にも影響を及ぼすため, 安全性と実用性の双方を考慮して有限体の設定を行う必要がある.

標数が大きい有限体上の離散対数問題を解くことに適したアルゴリズムとして数体篩法が知られており, 同様に標数が小さい場合については関数体篩法が適していることが知られている. 特に標数が小さい場合については下記の三種の有限体に関連付けられるペアリング暗号の研究が盛んに行われている: (i) 標数が 3 で拡大次数が 6ℓ (ℓ は素数, 以下同様) の有限体 $GF(3^{6\ell})$, (ii) 標数が 2 で拡大次数が 4ℓ の有限体 $GF(2^{4\ell})$, (iii) 標数が 2 で拡大次数が 12ℓ の有限体 $GF(2^{12\ell})$. これらの有限体を使用するペアリング暗号の安全性を評価するために, 各々の有限体に適したタイプの関数体篩法の研究が様々な組織によって行われている.

関数体篩法では, sieving (篩) によって relation と呼ばれる, モニックで既約な次数の小さい多項式 (因子基底) の積で表される多項式を生成し収集する. この relation から各因子基底の離散対数を解とする線型方程式が得られ, この後の線型代数段階でその線型方程式を解く. この二つの段階の計算量が関数体篩法の計算量を決定する. Sieving の段階で新たな手法 pinpointing が 2012 年に Joux によって提案された [4]. 従来は篩区間に対応する relation の候補である各多項式で, ある因子基底を因子として持つものを, その因子基底による割り算をほとんどすることなく, マーキングのみで収集していた. 即ち, 多項式の割り算をマーキングで代用することにより候補となる各多項式に対する計算コストを削減している. しかし, 候補となる多項式の数は膨大である. Pinpointing では, 小さな次数の既約多項式の積で表される多項式を探し, その多項式から複数の同様な異なる多項式を大量に生成する. Pinpointing の狙いは, 一つの relation を得るために必要な候補の多項式の個数を従来の方法に比べて少なくすることである. 有限体 $GF(q^n)$ 上の離散対数問題を解く場合に, $Q := q^n$ と書くことにして, 関数体篩法の計算量を表すために次の関数を用意する:

$$L_Q(\alpha, c) := \exp((c + o(1))(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}),$$

但し $0 < \alpha < 1$ で $c > 0$ とする.

以下で, 関数体篩法の計算量が改善される, 近年までの経緯について簡単に紹介する. (この部分については Adj, Menezes, Oliveira, と Henríquez らの原稿に詳しく書かれている [1].) 2006 年に Joux と Lercier によって提案された関数体篩法の計算量は,

$$q = L_Q(1/3, 1/3),\ n = 3^{-1/3}(\log Q/\log\log Q)^{2/3}$$

の場合に $L_Q(1/3, 1.44)$ であったが, この関数体篩法に pinpointing を適用することにより,

$$q = L_Q(-2/3, 1/3),\ n = 3^{2/3}(\log Q/\log\log Q)^{2/3}$$

の場合に $L_Q(1/3, 0.96)$ になる. この手法により Joux は 1425-bit の有限体 $GF(p^{57})$ ($p = 33341353$ とする) 上の離散対数問題を解くことに成功した.

2013 年, Joux は pinpointing に似た手法を導入することによって,

$$q \approx n/2$$

の場合に $L_Q(1/4 + o(1), c)$ となるアルゴリズムを提案し, 6168-bit の有限体 $GF(2^{8\cdot 3\cdot 257})$ 上の離散対数問題を解いた [5]. さらに, 同年, Barbulescu, Gaudry, Joux と Thomé は [5] の最後の計算段階を改良することによって

$$q \approx n,\ n \leq q + 2$$

の場合に有限体 $GF(q^{2n}) = GF(Q^2)$ 上の離散対数問題を解く計算量を quasi-polynomial time

$$(\log Q)^{O(\log \log Q)}$$

に改良することに成功した [2]. 注意すべきはこの計算量が, 任意の $0 < \alpha < 1$ と $c > 0$ に対して, $L_Q(\alpha, c)$ より漸近的に小さいことである.

最後に, 上述のように関数体篩法の計算量は適用する有限体の大きさだけではなく, 部分体の大きさと拡大次数の大きさの比などの影響も受ける. 従って, ペアリング暗号の安全性は, 推奨された暗号パラメータごとに評価される必要がある.

2 小さい標数の有限体を使用するペアリング暗号への影響

Adj, Menezes, Oliveira, と Henríquez らは, 計算量が quasi-polynomial time の関数体篩法 [2] を用いた場合の, 前の節で紹介した代表的な三種類の有限体に関連付けられるペアリング暗号の安全性について議論している [1]. 特に 128-bit 安全性が見込まれていた有限体 $GF(2^{4\cdot 1223})$, $GF(3^{6\cdot 509})$, $GF(2^{12\cdot 367})$, $GF(2^{12\cdot 439})$ の場合についてその安全性を評価しており, $GF(3^{6\cdot 509})$ の場合は 73.7-bit 安全性と見積もっている. また, $GF(2^{4\cdot 1223})$ についてはこの新しい関数体篩法の適用は難しく [1], $GF(2^{12\cdot 367})$ と $GF(2^{12\cdot 439})$ の場合は約 2^{40} 個以上のプロセッサーが必要と見積もっている.

3 Pinpointing を用いた関数体篩法の概要

文献 [4] では標数が小さい場合に適した関数体篩法 JL06-FFS [6] の sieving step において, relation を求める新たな手法である pinpointing を導入して議論している. まず, 次の節で JL06-FFS [6] について簡単に説明する.

3.1 標数が小さい場合の関数体篩法の例

有限体 $\mathbb{F}_{q^n}$ 上の DLP を JL06-FFS で解く場合, 二つの多項式 $f_1(x, y) = x - g_1(y), f_2(x, y) = -g_2(x) + y \in \mathbb{F}_q[x, y]$ を用意する. 但し g_1 と g_2 の次数をそれぞれ d_1, d_2 とし, $-g_2(g_1(y)) + y$ は $\mathbb{F}_q$ 上で既約な n 次多項式 $f(y)$ を因子として持つとする. さらに次数 d_1, d_2 と因子基底の最大次数 D は, $d_1 \approx \sqrt{Dn}$ と $d_2 \approx \sqrt{n/D}$ が成り立つように設定される.

[1] Granger, Kleinjung, Zumbrägel らは体の表現を工夫することにより, $GF(2^{4\cdot 1223})$ を使用した場合は 59-bit 安全性と見積もっている [3]. この成果は CRYPTO 2014 に採録された.

このアルゴリズムの sieving step では,

$$\mathcal{A}(y)g_1(y) + \mathcal{B}(y) = \mathcal{A}(g_2(x))x + \mathcal{B}(g_2(x))$$

の両辺が D-smooth となる一変数の $\mathbb{F}_q$ 係数多項式の組 $(\mathcal{A}(z), \mathcal{B}(z))$ を集める. 但し, $\mathcal{A}(z), \mathcal{B}(z)$ の次数は D 以下とし, さらに $\mathcal{A}(z)$ はモニックとする.

JL06-FFS の計算量は, $q = L_{q^n}(1/3, \alpha D)$ のとき, sieving step は $L_{q^n}(1/3, c_1)$, linear algebra step は $L_{q^n}(1/3, c_2)$ となる. ただし, $Q = q^n$ として,

$$L_Q(\beta, c) = \exp((c + o(1))(\log Q)^{\beta}(\log\log Q)^{1-\beta})$$

で,

$$c_1 = \frac{2}{3\sqrt{\alpha D}} + \alpha D,\ c_2 = 2\alpha D$$

とする. さらに次の条件に注意：

$$(D+1)\alpha \geq \frac{2}{3\sqrt{\alpha D}}.$$

3.2 Pinpointing

簡単な例として, JL06-FFS において $D = 1$ とした場合で, Pinpointing について説明する. まず, $g_1(y) = y^{d_1}$ と設定し, $D = 1$ より $\mathcal{A}(z) = z + a$, $\mathcal{B}(z) = bz + c$ であることから, 次の形の relation の候補について考える:

$$y^{d_1+1} + ay^{d_1} + by + c = xg_2(x) + ax + bg_2(x) + c. \tag{1}$$

この両辺が 1 次多項式の積に分解できる場合に relation が得られる.

3.2.1 One-sided pinpointing

式 (1) の左辺が 1-smooth であることと, $y = au$ とした場合に, 多項式 $u^{d_1+1} + u^{d_1} + ba^{-d_1}u + ca^{-d_1-1}$ が 1-smooth であることは同値である. 従って, $u^{d_1+1} + u^{d_1} + Bu + C \in \mathbb{F}_q$ の形の多項式に注目して, これが 1-smooth となる (B, C) が得られれば, その一つの (B, C) から $q-1$ 個の 1-smooth な多項式 $y^{d_1+1} + ay^{d_1} + by + c$ が得られる. ($a \in \mathbb{F}_q^*$ に対して $b = Ba^{d_1}, c = Ca^{d_1+1}$ とする.)

一つの 1-smooth な $u^{d_1+1} + u^{d_1} + Bu + C$ を得るために, 漸近的に $(d_1+1)!$ 個の候補が必要である. 従って (1) の左辺については $(d_1+1)! + (q-1)$ 個の候補が存在する. またそのときの $q-1$ 個の $a\mathbb{F}_q^*$ に対して, (1) の右辺が 1-smooth になる個数の期待値は $(q-1)/(d_2+1)!$ であることから, 一つの relation を得るために必要な候補の期待値は

$$\frac{(d_1+1)! + (q-1)}{(q-1)/(d_2+1)!} = \frac{(d_1+1)!(d_2+1)!}{q-1} + (d_2+1)!$$

となり, sieving の場合の $(d_1+1)!(d_2+1)!$ 個に比べてずっと小さい.

3.2.2 Kummer extensions, Frobenius and advanced pinpointing

拡大次数 n が $d_1d_2 - 1$ である Kummer extension の場合に, 式 (1) の両辺に pinpointing を行うことができる. さらに linear system の変数を実質的に $1/n$ 倍に減らすことができる.

有限体 $\mathbb{F}_q$ は 1 の原始 n 乗根 μ を含むとする. このとき $\mathbb{F}_q$ 上の n 次の Kummer extension は $P(x) = x^n - K$ で定義される. (K の設定に注意.) K の n 乗根 κ で $\kappa^q = \mu\kappa$ となるものが存在し,

$$P(x) = \prod_{i=0}^{n-1}(x - \mu^i\kappa)$$

とかける. そのような Kummer extension において, $g_1(y), g_2(x)$ を次のように定義する:

$$g_1(y) = y^{d_1}/K,\ g_2(x) = x^{d_2}. \tag{2}$$

このとき $x = g_1(y)$, $y = g_2(x)$ であることから, $x^{d_1d_2} - Kx = 0$ となり両辺を x で割ることで $P(x)$ を得る.

$D = 1$ で考えていることから因子基底は, $w \in \mathbb{F}_q$ に対して $x + w$ や $y + w$ の形をしている. これらの多項式は Frobenius map によって,

$$\begin{aligned}(x+w)^q &= x^q + w = \mu x + w = \mu(x + w/\mu),\\ (y+w)^q &= y^q + w = \mu y + w = \mu(y + w/\mu)\end{aligned}$$

となる. 従って, $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$ において,

$$\log(x + w/\mu) = q\log(x + q),\ \log(y + w/\mu) = q\log(y + q)$$

が成り立ち, linear system の変数を減らすことができる.

One-side pinpointing のとき, 即ち式 (1) の場合と同様にして,

$$x^{d_2+1} + bx^{d_2} + ax + c = y^{d_1+1}/K + ay^{d_1}/K + by + c \tag{3}$$

について考える. 式 (3) の右辺が 1-smooth であることと, $u^{d_2+1} + u^{d_2} + ab^{-d_2}u + cb^{-d_2-1}$ が 1-smooth であることは同値であり, 同様に左辺については $v^{d_1+1}/K + v^{d_1}/K + ab^{-d_1}v + cb^{-d_1-1}$ が対応する. さらに $\lambda = c/(ab)$ とすることで, u, v を変数とするこれらの多項式はそれぞれ次のように書くことができる:

$$u^{d_2+1} + u^{d_2} + ab^{-d_2}(u + \lambda),\ (v^{d_1+1} + v^{d_1})/K + ab^{-d_1}(v + \lambda).$$

逆に (A, B, λ) を, $A \neq 0$, $B \neq 0$, AB^{d_2} が $\mathbb{F}_q$ において n 冪となり (Kummer extension を使用している), さらに

$$u^{d_2+1} + u^{d_2} + A(u + \lambda),\ (v^{d_1+1} + v^{d_1})/K + B(v + \lambda)$$

がそれぞれ 1-smooth となるように選ぶ. このとき, $A = ab^{-d_2}$, $B = ba^{-d_1}$ とすることで, $AB^{d_2} = a^{1-d_1d_2} = a^{-n}$ から a を定めることができ, さらにその選び方は n とおりである. 各 a に対して $b = Ba^{d_1}$, $c = \lambda ab$ と定める.

最終的に relation 一つ当たりのコストは

$$O(\frac{n(d_1+1)!(d_2+1)!}{q-1}) + 1$$

となるが, Frobenius map の効果で n を相殺できる.

3.3 計算量

$\mathbb{F}_{q^n}$ 上の離散対数問題を, pinpointing を導入した JL06-FFS で解くことを考える. ここで $Q = q^n$ とし, α は次を満たすとする:

$$\alpha = \frac{1}{n}\left(\frac{\log Q}{\log\log Q}\right)^{2/3}.$$

$D = 1$ とした場合に linear algebra step の計算量は $L_Q(1/3, 2\alpha)$ となる. $\alpha \geq 3^{-2/3}$ に対して, このコストは (双方の) pinpointing のコストより大きいため, 総計算量は $L_Q(1/3, 2\alpha)$ となる. $\alpha \in [3^{-2/3}, 2^{2/3})$ に対しては JL06-FFS よりも総計算量は小さくなり, とくに $\alpha = 3^{-2/3}$ のとき, 総計算量は $L_Q(1/3, 1.44)$ から $L_Q(1/3, 0.96)$ に減少する.

3.4 数値実験

まず, $p_1 = 33553771$, $p_2 = 33341353$ とする. このとき有限体 $\mathbb{F}_{p_1^{47}}$ と $\mathbb{F}_{p_2^{57}}$ の大きさはそれぞれ 1175-bit と 1425-bit となる. これらの有限体上の離散対数問題を Advanced pinpointing を使用して解く数値実験を行った場合, 双方とも 32000 CPU-hour を必要とした.

Bitsize	Total time (CPU.h)	Relation construction (CPU.h)	Linear algebra (CPU.h)	Indiv. Log. (CPU.h)	文献
1175	32000	3	32000	4	文献 [4]
1425	32000	6	32000	< 12	文献 [4]

参考文献

[1] G. Adj, A. Menezes, T. Oliveira, F. R. Henríquez, "Weakness of $\mathbb{F}_{3^{6\cdot 509}}$ for Discrete Logarithm Cryptography," Pairing 2013, LNCS 8365, pp. 20-44, (2013).

[2] R. Barbulescu, P. Gaudry, A. Joux, E. Thomé, "A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic," CoRR abs/1306, 4244, (2013).

[3] R. Granger, T. Kleinjung, J. Zumbrägel, "Breaking '128-bit Secure' Supersingular Binary Curves (or how to solve discrete logarithms in $\mathbb{F}_{2^{4\cdot 1223}}$ and $\mathbb{F}_{2^{12\cdot 367}}$)," IACR Cryptology ePrint Archive 2014, 119, (2014).

[4] A. Joux, "Faster index calculus for the medium prime case. Application to 1175-bit and 1425-bit finite fields," EUROCRYPT 2013, LNCS 7881, pp. 177-193, (2013).

[5] A. Joux, "A new index calculus algorithm with complexity $L(1/4 + o(1))$ in small characteristic," SAC 2013, LNCS 8282, pp. 355-379, (2013).

[6] A. Joux and R. Lercier, "The function field sieve in the medium prime case," EUROCRYPT 2006, LNCS 4004, pp. 254-270, (2006).

発行日　2014年 7月14日　第1版
発行者
・〒184-8795
東京都小金井市貫井北町四丁目2番1号
独立行政法人 情報通信研究機構
（ネットワークセキュリティ研究所 セキュリティ基盤研究室、
セキュリティアーキテクチャ研究室）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN

・〒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