CRYPTREC Report 2014

平成 27 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 2014 年度活動報告である。

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、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について、検討を実施している。2014 年度は、暗号技術の安全性及び実装に係る監視及び評価として、ハッシュ関数 SHA-2,SHA-3 に関する外部評価を実施し、現時点では現実的な脅威につながる問題はないという評価結果を得ている。また、新世代暗号に係る調査としては、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、検討を実施した。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、軽量暗号技術に関する調査及び検討、アプリケーションに関する調査を実施し、今後の活動方針に関する提言を報告書としてとりまとめた。暗号技術の安全な利用方法に関しては、「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)」に POODLE 攻撃に対する解説を追加した。また、RC4 の注釈は、暗号技術活用委員会とともに検討し、変更に至った。さらに、ECDSA 及び ECDH の仕様書の参照先の変更について検討を行っている。

CRYPTREC は 2000 年に発足して以来、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討することでセキュアな IT 社会の実現に貢献してきた。暗号技術評価委員会及びその前身である暗号技術監視委員会、暗号方式委員会では、2003 年に公開された電子政府推奨暗号リスト及び 2014 年 3 月に改定された CRYPTREC 暗号リストの暗号の安全性を、技術的な観点から監視・評価してきた。15 年にわたり、国内外の多くの暗号研究者の協力により、継続的に安全性を評価してきたことは、日本だけではなく世界にも通用する現在の CRYPTREC ブランドの信頼の醸成につながっている。このような CRYPTREC 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。CRYPTREC ブランドを大切にしつつ、社会のニーズに応えるため、今後は様々な応用分野も視野に入れて活動を続けてほしい。

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。

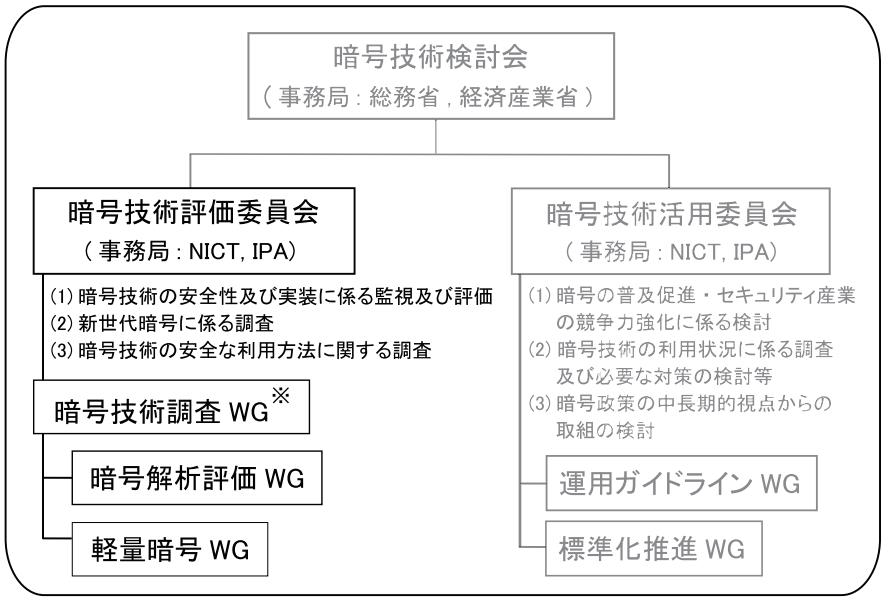
【問合せ先】　info@cryptrec.go.jp

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。2014 年度、評価委員会の指示に基づき実施される調査項目は、「暗号解析評価 WG」及び「軽量暗号 WG」にてそれぞれ検討される。

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 0.1：CRYPTREC 体制図

委員名簿

暗号技術評価委員会

委員長	今井 秀樹	東京大学 名誉教授
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　IS 研究所　ディビジョンマネージャー
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	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 上級研究員
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

石原 潤二　内閣官房内閣サイバーセキュリティセンター
高木 浩光　内閣官房内閣サイバーセキュリティセンター
大川 伸也　内閣官房内閣サイバーセキュリティセンター
森安 隆　内閣官房内閣サイバーセキュリティセンター
根本 農史　警察庁 情報通信局[2015 年 3 月まで]
中山 慎一　警察庁 情報通信局[2015 年 3 月から]
佐藤 健太　総務省 行政管理局[2015 年 1 月まで]
加藤 彰浩　総務省 行政管理局[2015 年 2 月から]
野村 知宏　総務省 自治行政局 住民制度課[2014 年 7 月まで]
内海 隆明　総務省 自治行政局 住民制度課[2014 年 8 月から]
筒井 邦弘　総務省 情報流通行政局
近藤 直光　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[2014 年 7 月まで]
中野 辰実　経済産業省 商務情報政策局[2014 年 8 月から]
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[2014 年 7 月まで]、中澤忠輝[2014 年 8 月から]、盛合志帆、野島良、大久保美也子、黒川貴司、金森祥子、笠井祥、大川晋司）

独立行政法人 情報処理推進機構（伊藤毅志、近澤武、小暮淳、大熊建司、神田雅透、稲垣詔喬、吉川法子[2015 年 1 月まで]、加藤久美[2015 年 2 月から]）

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、電子自治体及び重要インフラ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、暗号技術は情報システム及び情報通信ネットワーク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。現在、様々な暗号技術が開発され、それを組み込んだ多くの製品・ソフトウェアが市場に提供されているが、暗号技術を電子政府システム等で利用していくためには、暗号技術の適正な評価が行われ、その情報が容易に入手できることが極めて重要となる。

CRYPTREC (Cryptography Research and Evaluation Committees) では、2000年度から電子政府システム等での利用に資する暗号技術のリストアップを目的として暗号技術の評価プロジェクトを開始し、2000年度から2002年度までの3年間のプロジェクトの集大成として、2002年度に「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(電子政府推奨暗号リスト)」(平成15年2月20日公表)[1]を策定した (2012年度に「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)」[2]に改定)。引き続き、CRYPTRECでは、電子政府推奨暗号リスト等に記載された暗号アルゴリズムを対象とする調査・検討を行う活動を行ってきたが、2005年度に実施されたハッシュ関数の安全性評価に基づき、2006年6月にSHA-1の安全性に関する見解を、2006年度に実施された素因数分解問題の困難性に関する評価に基づき、RSA1024の安全性の評価結果をそれぞれ公表した。また、最近では、ストリーム暗号 128-bit RC4 をCRYPTREC 暗号リストの運用監視暗号リストに掲載し、推奨すべき状態ではなくなったものとして取り扱っている。

高度情報通信ネットワーク社会形成基本法(IT基本法)[3]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」[4]、

[1] http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_fy2005.pdf
[2] http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf
[3] http://www.kantei.go.jp/jp/singi/it2/hourei/honbun.html
[4] http://www.nisc.go.jp/active/kihon/pdf/bpc01_ts.pdf

「第2次情報セキュリティ基本計画」[5]、「国民を守る情報セキュリティ戦略」[6]及び「サイバーセキュリティ戦略」[7]により、電子政府システム等の情報セキュリティ水準の向上が図られてきた。

暗号技術に係る施策としては、例えば、上述の 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、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」[8]において「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、2008 年度には、「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」[9]が決定されるに至った。そして、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」[10]において、「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 年度に策定された「サイバーセキュリティ戦略」[11]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[12]の利用を推進する」ことや、「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[13]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。

今般、サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、2014 年 11 月に成立した「サイバーセキュリティ基本法」(平成 26 年法律第 104 号)[14]により、2015 年１月に、情報セキュリティ政策会議及び情報セキュリティセンターが改組され、それぞれ「サイバーセキュリティ戦略本部」及び「内閣サイバーセキュリティセンター(NISC)」が設置されている。

---

[5] http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf
[6] http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf
[7] http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf
[8] http://www.nisc.go.jp/active/kihon/pdf/sjf_2007.pdf
[9] 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）
[10] 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）
[11] http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf （2013 年 6 月 25 日情報セキュリティ政策会議決定）
[12] 「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。但し、運用監視暗号リストのものの利用は推奨していない。
[13] CRYPTREC の活動を指す。
[14] http://law.e-gov.go.jp/htmldata/H26/H26HO104.html、http://www.nisc.go.jp/law/pdf/basicact.pdf

今後とも、CRYPTREC によって発信される情報を踏まえて、関係各機関が連携して情報システム及び情報通信ネットワークをより安全なものにしていくための取り組みを実施していくことが非常に重要である。また、過去 15 年間に渡って実施してきた暗号技術の安全性及び信頼性確保のための活動は、最新の暗号研究に関する情報収集・分析に基づいており、引き続き、暗号技術に係る研究者等の多くの関係者の協力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[15]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)」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)」[16](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。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 年度以降は、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。

[15] http://www.cryptrec.go.jp/list_2003.html
[16] http://www.cryptrec.go.jp/list.html

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年度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[17]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。

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) 暗号技術の安全性及び実装に係る監視及び評価
(b) 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)
(c) 暗号技術の安全な利用方法に関する調査(暗号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な考え方は、CRYPTREC Report 2012 までに記載されていた電子政府推奨暗号リスト[18]掲載の暗号技術に対する考え方[19]と基本的に同じである。つまり、暗号技術の安全性及び実装に係る監視及び評価とは、研究集会、国際会議、研究論文誌、インターネット上の情報等を監視すること（情報収集）、CRYPTREC 暗号リストに掲載されている

[17] http://www.cryptrec.go.jp/topics/cryptrec_201212_listpc.html
[18] 2003 年 2 月 20 日に策定されたものを指す。
[19] たとえば、暗号技術検討会 2008 年度報告書を参照のこと。
http://www.cryptrec.go.jp/report/c08_kentou_final.pdf

暗号技術の安全性に関する情報を分析し、それを暗号技術評価委員会に報告すること（情報分析)、安全性等において問題が認められた場合、暗号技術評価委員会において内容を審議し、評価結果を決定すること（審議及び決定)、の 3 つ段階からなる。また、仕様書の参照先の変更を検討する際にも、監視に関する基本的な考え方を参考にしている。図 1.1 に電子政府推奨暗号の削除等の手順を示す。

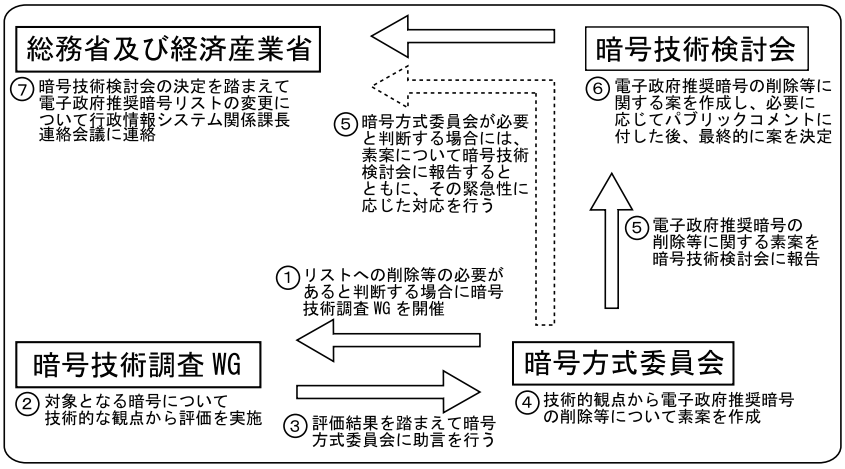


図1.1: 電子政府推奨暗号の削除等の手順[20]

(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。

[20] 表中の「暗号方式委員会」は適宜、暗号技術評価委員会と読み替える。

第２章 委員会の活動

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 2014 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

共通鍵暗号は大きくブロック暗号とストリーム暗号に分けられる。ブロック暗号に対する攻撃では、基本構造の一つである一般の Feistel 暗号に対する鍵回復攻撃で進展があった。

Asiacrypt 2015 において Peyrin らは、中間一致の手法による解析で、Feistel 構造に存在する trucated 差分を発見し、それを攻撃に利用した。ラウンド関数の種類により攻撃を分けており、Feistel-2 タイプ[1]および Feistel-3 タイプに対し各々従来を上回る結果を得ている。適用範囲は広く、既知の攻撃を上回る結果であるため、適用条件に当てはまる暗号に関しては注意が必要である。

ブロック暗号のもう一つの基本構造である SPN 型については目立った進展は少なく、代表的な AES の最も成功した攻撃は昨年度と変わっていない。また、ストリーム暗号に関しても目立った攻撃の進展は見られなかった。

2.1.2.公開鍵暗号に関する安全性評価について

公開鍵暗号の安全性の根拠とする数学的問題に関しては、離散対数問題(DLP: Discrete Logarithm Problem)の解読法において大きな進展があった。

Eurocrypt 2014 において、Barbulescu らは、DLP に対する新しい解読法を提示した。小標数の場合の計算量は準多項式時間[2]と評価されており、これまで最速であった関数体篩法の準指数時間より少ない。電子政府推奨暗号では、電子署名アルゴリズム DSA 及び鍵共有アルゴリズム DH が DLP ベースであるが、使用・推奨しているパラメータは素体(大標数)であり、今回の攻撃の対象外である。

Crypto 2014 において、Granger らは、これまでは 128 ビットの安全性[3]を持つと考えられていた標数 2 の体における DLP の解読成功を発表した。解読の対象になった問題は二つ

[1] Feistel 暗号のラウンド関数ではラウンド鍵に依存する F 関数が利用される。F 関数が一般的なものを Type-1、ラウンド鍵加算の後に仕様が公開された関数を通すのを Type-2、ラウンド鍵加算、S-box 層、線形拡散層の順に処理するのを Type-3 と呼ぶ。

[2] 多項式時間よりも遅く、指数時間ほどは遅くないアルゴリズムであり、ある固定の c に対して最悪でも $2^{O((\log n)^c)}$で抑えられるものを指す。

[3] 攻撃に必要な計算量が暗号化計算の2^n回分であるとき、nビット安全という。

あり、一つは GF(2^{1223})上で定義された種数 1 の曲線における DLP を GF(2^{4892})の DLP に埋め込んだ問題であり、もう一つは、GF(2^{367})上で定義された種数 2 の曲線における DLP を GF(2^{4404})の DLP に埋め込んだ問題である。これまでは、前者の安全性は 128 ビットであり、後者は 94.6 ビットであるとされていた。今回新たなテクニックを導入することにより、前者の安全性は 59 ビット程度と見積もられ、後者は計算機実験により完全解読された。

2.1.3. ハッシュ関数とメッセージ認証コードに関する安全性評価について

広く利用されているハッシュ関数 SHA-1、SHA-2 ファミリー[4]本体に対する攻撃には、目立った進展はなかった。一方、ハッシュ関数を利用したメッセージ認証コードについては、関数グラフが周期軌道に落ち込む性質に着目した攻撃に大きな進展があり、コード長 l に対して安全性が$O(2^l)$を下回る結果が得られている。

Crypto 2014 において、Peyrin らは、HMAC と類似の MAC に対する 4 種類の汎用攻撃を提案した。与えられたメッセージに対する署名を偽造する攻撃(universal forgery)で、計算量を従来の$O(2^{5l/6})$を $O(2^{3l/4})$に削減するなどの結果を示した。

同じ Crypto 2014 において、Dinur らは、最終処理にメッセージ長依存性がある HAIFA 型ハッシュ関数を使った HMAC に対する初の状態回復攻撃で計算量$O(2^{4l/5})$を達成したり、HMAC に対する状態回復攻撃におけるメッセージ長と計算複雑度のトレードオフを記述したりした他、SHA-1 と SHA-2 に適用可能な最初の偽造攻撃も示した。

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てきた。2013 年度においては、下記の表 2.1 の通り仕様書の参照先が変更されている。

2014 年度は、2013 年度に継続審議となった ECDSA/ECDH (SECG SEC 1 Version 1.0 から Version 2.0 へ)について検討を行った。評価の結果、SECG SEC 1 Ver 2.0[5]の「4.1.7 Self-Signing Operation」の部分に「軽微な修正」の範囲を超える部分があるとの指摘があり、また、実装の適合性評価についても配慮する必要があるとの意見があったため、同変更案は了承されなかった。今後の検討では、安全性以外の観点についても検討が必要である。

---

[4] NIST は FIPS 180-4 で次の 7 種類のハッシュ関数(SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256)を定めており、SHA-1 以外は SHA-2 ファミリーと呼ばれている。

[5] http://www.secg.org/sec1-v2.pdf

表 2.1: 仕様書の参照先の判定結果(2013 年度)

暗号技術の名称	判定結果	理由
RSA-PSS/RSASSA-PKCS1-v1_5/RSA-OAEP/RSAES-PKCS1-v1_5 (PKCS #1 v2.1 から PKCS #1 v2.2 へ)	仕様書の参照先の変更を認める。(2013 年度第 1 回暗号技術評価委員会了承)	アルゴリズムに変更がない
3-key Triple DES (NIST SP 800-67 から NIST SP 800-67 Revision 1 へ)		
SHA-256/SHA-384/SHA-512/SHA-1 (NIST FIPS 180-2 から NIST FIPS 180-4 へ)		
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。(2013 年度第 2 回暗号技術評価委員会了承)	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.暗号技術の安全な利用方法に関する調査

2.3.1.128-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、2013 年度から注釈の変更について検討を行い、継続審議となっていた。

2014 年度は、表 2.2 の通り、同注釈に関する変更案(以下、評価委案という。)を第 1 回暗号技術評価委員会にて作成した。その結果を、第 1 回暗号技術検討会に報告したところ、暗号技術活用委員会においても同案を審議すべきである旨、意見が出されたため、第 2 回暗号技術活用委員会においても同案について検討が行われ、「今後は極力利用すべきでない」という注釈変更の意図を明確化することとなり、同注釈に関する変更案(以下、活用委案という。)が決定された。再び、活用委案が第 3 回暗号技術評価委員会にて検討され、暗号技

術評価委員会においても活用委案が同意された。

表 2.2: 現行の注釈及び各委員会における変更案

現行の注釈	128-bit RC4 は、SSL(TLS1.0 以上)に限定して利用すること
暗号技術評価委員会における変更案	SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術を選択すること。 (2014 年度第 1 回暗号技術評価委員会採択　2014 年 8 月 4 日開催)
暗号技術活用委員会における案	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。 (2014 年度第 2 回暗号技術活用委員会採択　2015 年 1 月 26 日開催) (2014 年度第 3 回暗号技術評価委員会採択　2015 年 3 月 2 日開催)

2.3.2. 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）の更新

2014 年 10 月 14 日に SSL3.0 における CBC モードに対して新たに攻撃(以下、POODLE 攻撃という。)が公表された[6]。POODLE 攻撃とは、CBC モードの暗号化でのパディング処理においてパディングの内容の妥当性を検証しない SSL3.0 の仕様を利用する、中間者攻撃の一種である。攻撃者は、第一に、クライアントに悪意あるソフトウェアを読ませてサーバにデータを送信させ、第二に、送信されたデータの一部を細工してサーバに中継し、第三に、細工されたデータをサーバに受信させた時のエラーの有無を検知できる、という環境において、高い確率で送信データを解読できる。

この状況を鑑み、2013年度に発行した「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)」[7]を更新し、3.2節にPOODLE攻撃に関する記述を加えることとなった。詳しくは、付録4を参照のこと。

2.4. CRYPTREC シンポジウム 2015

【プログラムの概要】

日　時　：2015 年 3 月 20 日（金）10：00～15：50

場　所　：一橋大学一橋講堂

[6] Bodo Möller, Thai Duong, Krzysztof Kotowicz, “This POODLE Bites: Exploiting The SSL 3.0 Fallback,” https://www.openssl.org/~bodo/ssl-poodle.pdf

[7] http://www.cryptrec.go.jp/report/c13_tech_guideline_TLSSSL_web.pdf

主　催　：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

共　催　：総務省、経済産業省

参加人数：163 名

表 2.3　プログラム

時間	内容	
10:00	開会挨拶	情報処理推進機構　立石譲二　理事
	総務省挨拶・経済産業省挨拶	総務省・経済産業省
10:15	CRYPTREC 活動紹介	暗号技術検討会事務局
10:30	暗号技術評価委員会報告	今井秀樹　委員長　（東京大学　名誉教授）
10:45	暗号解析評価 WG 報告	高木剛　主査　（九州大学　教授）
11:05	軽量暗号 WG 報告	本間尚文　主査　（東北大学　准教授）
11:25	招待講演① “プロトコルの形式検証と脆弱性発見の現実 －Case of CCS Injection－”	林達也　様　（(株)レピダム　代表取締役）
12:10	昼休み	
13:40	暗号技術活用委員会報告	松本勉　委員長　（横浜国立大学　教授）
13:55	運用ガイドライン WG 報告	菊池浩明　主査　（明治大学　教授）
14:15	標準化推進 WG 報告	渡辺創　主査　（産業技術総合研究所　研究グループ長）
14:35	休憩	
15:00	招待講演② “ISP から見た「暗号技術に期待したいこと ・期待していないこと」”	須賀祐治　様　（(株)インターネットイニシアティブ　シニアエンジニア）
15:45	閉会挨拶	情報通信研究機構　今瀬真　理事

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2.4に示す通りである。

表 2.4 国際会議への参加状況

学会名・会議名		開催国・都市	期間
Eurocrypt 2014	International Conference on the Theory and Applications of Cryptographic Techniques	デンマーク・コペンハーゲン	2014 年 5 月 12 日～2014 年 5 月 30 日

SAC 2014	Conference on Selected Areas in Cryptography	カナダ・モントリオール	2014 年 8 月 14 日～8 月 15 日
Crypto 2014	International Cryptology Conference	米国・サンタバーバラ	2014 年 8 月 18 日～8 月 21 日
SHA-3	SHA-3 2014 Workshop	米国・サンタバーバラ	2014 年 8 月 22 日
FDTC 2014	Workshop on Fault Diagnosis and Tolerance in Cryptography	韓国・釜山	2014 年 9 月 23 日
CHES 2014	Workshop on Cryptographic Hardware and Embedded Systems	韓国・釜山	2014 年 9 月 24 日～9 月 26 日
PROOFS 2014	Security Proofs for Embedded Systems Workshop	韓国・釜山	2014 年 9 月 27 日
PQCrypto 2014	Theory of Cryptography Conference	カナダ・ウォータールー	2014 年 10 月 1 日～10 月 3 日
Asiacrypt 2014	International Conference on the Theory and Application of Cryptology and Information Security	台湾・高雄	2014 年 12 月 8 日～12 月 11 日
FSE 2015	International Workshop on Fast Software Encryption	トルコ・イスタンブール	2015 年 3 月 9 日～3 月 11 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

・Meet-in-the-Middle Attacks on Generic Feistel Constructions [Asiacrypt 2014]

一般的なバランス型 Feistel 暗号に対する鍵回復攻撃が発表された。中間一致の手法による解析で、Feistel 構造に存在する truncated 差分を発見し、攻撃に利用している。ラウンド関数の種類により攻撃を分けており、Feistel-2 タイプおよび Feistel-3 に対し各々結果を示している。Feistel-2 タイプでは、鍵長を k、ブロック長を n としたとき、k=n の場合 6 段を $2^{3n/4}$ の計算量で、k=2n の場合 10 段を $2^{11n/6}$ の計算量で攻撃可能である。Feistel-3 タイプでは、S-box 長を c としたとき、k=n の場合 10 段を $2^{n/2+4c}$ の計算量で、k=2n の場合

14 段を $2^{3n/2+4c}$ の計算量で攻撃可能である。適用範囲は広く、既知の攻撃より適用可能段数を伸ばしているため、適用条件に当てはまる暗号に関しては注意が必要である。

・Low Probability Differentials and the Cryptanalysis of Full-Round CLEFIA-128 [Asiacrypt 2014]

ブロック暗号の鍵スケジュールに対する差分確率は関連鍵差分解析に対する耐性の評価に使われ、k ビット鍵暗号に対する上限が 2^{-k} であれば十分であると考えられてきたが、CLEFIA-128 に対する関連鍵攻撃で反例が示された。ラウンド鍵を生成する鍵スケジュールの線型部分と Feistel 構造により、確率 2^{-128} の 2^{14} 個の特別に選択される差分を持ち、2^{14} ペアの弱鍵を持つ。ハッシュモードでは弱鍵ペアを 2^{122} 時間で発見することができ、一般の 2^{128} 時間よりも速く差分マルチ衝突を生成することができる。また、弱鍵クラスに属しているかどうかの判定を従来の 2^{14} に対し、2^{8} の時間・データ計算量で行うことができる。攻撃の計算量は実用レベルではないため、CLEFIA-128 に対する現実的な脅威にはなってない。

2.5.2. ハッシュ関数とメッセージ認証コードの解読技術

・Updates on Generic Attacks against HMAC and NMAC [Crypto 2014]

HMAC と類似の MAC に対する 4 種類の汎用攻撃を提案した。最初は、攻撃者が最初に攻撃するメッセージをコミットする攻撃(selective forgery)2 種で、一つは計算量$O(2^{l/2})$を要するタイトな攻撃、もう一つは計算量は$O(2^{2l/3})$と大きくなるもののコミットするメッセージの自由度がより大きい攻撃である。次に、与えられたメッセージに対する署名を偽造する攻撃(universal forgery)で、計算量を従来の$O(2^{5l/6})$を $O(2^{3l/4})$に削減した。最後に、HMAC に対する初の time-memory tradeoff 攻撃で、事前計算$O(2^{l})$で、最初の内部鍵K_{out}を計算量$O(2^{2l/3})$で復元、もう一つの内部鍵K_{in}を計算量$O(2^{3l/4})$で復元する。これらの攻撃では、拡張可能メッセージ型の第 2 原像攻撃や関数型グラフベース偽造攻撃など様々な技法を拡張することで実現した。

・Improved Generic Attacks Against Hash-based MACs and HAIFA [Crypto 2014]

近年、HMAC の安全性が$O(2^{l})$を大きく下回ることが、Leurent 他、及び、Peyrin 他によって示されている。ここでは、これらの研究を具体的なメッセージ長が限定されたり、特殊な繰り返しモードといった特徴を持つ具体的なハッシュ関数に焦点を当てたより拡張された結果を示す。最初は、HAIFA 型ハッシュ関数を使った HMAC に対する初の状態回復攻撃で、計算量は$O(2^{4l/5})$である。次に、HMAC に対する状態回復攻撃におけるメッセージ長と計算複雑度のトレードオフを記述する。これらの結果を利用して、最大メッセージ長が限定されている、いくつかの HMAC の設計に対する攻撃を構成。最後に、MAC オラクルに対して短いメッセージのクエリを送る初の汎用偽造攻撃を示す。特に、SHA-1 と SHA-2 に適用可能な最

初の偽造攻撃になっている。

2.5.3.暗号利用モードの解読技術

・GCM Security Bounds Reconsidered [FSE 2015]

GCM の衝突確率の上限は $2^{22}/2^{128}$ 以下であることは証明されているが、この上限に近い確率を実現する具体的な nonce の作り方は示されていなかった。本発表では、GCM の衝突確率を $2^{20.75}/2^{128}$ にする nonce の具体例を作成するとともに、nonce を適切に選ぶことにより、衝突確率は $32/2^{128}$ 以下になることを証明した。後者の結果は、GCM のオリジナルの主張に近いことを示す肯定的な結果である。

2.5.4.公開鍵暗号の解読技術

・A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic [Eurocrypt 2014]

離散対数問題(DLP: Discrete Logarithm Problem)に対する新しい解読法を提示した。計算量評価はヒューリスティックな仮定を用いているが、小標数の場合に計算量は準多項式時間となっており、これまで最速であった関数体篩法の準指数時間より小さくなっている。電子政府推奨暗号では、電子署名アルゴリズム DSA 及び鍵共有アルゴリズム DH が該当するが、使用・推奨しているパラメータは素体(大標数)であり、対象外となっている。ただし、小標数の DLP の困難性に基づいた暗号技術を使用する場合には、新解読アルゴリズムの影響を考慮する必要がある。

・Breaking ‘128-bit Secure’ Supersingular Binary Curves (or how to solve discrete logarithms in $F_2^{4\cdot 1223}$ and $F_2^{12\cdot 367}$) [Crypto 2014]

Granger らは、これまでは 128 ビットの安全性 を持つと考えられていた標数 2 の体における DLP の解読成功を発表した。解読の対象になった問題は二つあり、一つは GF(2^{1223})上で定義された種数 1 の曲線における DLP を GF(2^{4892})の DLP に埋め込んだ問題であり、もう一つは、GF(2^{367})上で定義された種数 2 の曲線における DLP を GF(2^{4404})の DLP に埋め込んだ問題である。これまでは、前者の安全性は 128 ビットであり、後者は 94.6 ビットであるとされていた。今回新たなテクニックを導入することにより、前者の安全性は 59 ビット程度と見積もられ、後者は計算機実験により完全解読された。

2.6. 委員会開催状況

2014 年度、暗号技術評価委員会は、表 2.5 の通り 3 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。

表 2.5　暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2014 年 8 月 4 日	委員会活動計画案、ワーキンググループ活動計画案、ハッシュ関数の評価、RC4 の注釈変更案、技術ガイドライン、仕様書の参照先変更、監視状況報告
第 2 回	2014 年 12 月 25 日	ワーキンググループ活動の中間報告、ハッシュ関数の評価の中間報告、仕様書の参照先変更、技術ガイドライン、監視状況報告
第 3 回	2015 年 3 月 2 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 の注釈変更案、CRYPTREC Report 2014 目次案、次年度活動計画案、監視状況報告

2.7. 暗号調査ワーキンググループ開催状況

2014 年度、各暗号調査ワーキンググループ（WG）が活動した主要活動項目は、表 2.6 の通りである。表 2.7 及び表 2.8 の通り、各 WG は計 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。

表 2.6　2014 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
暗号解析評価ワーキンググループ	高木 剛	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、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。
軽量暗号ワーキンググループ	本間 尚文	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適切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。昨年度は、これまでに提案されている軽量暗号の現状調査、アプリケーションに関する調査、実装評価等を行った。今年度はこれらをふまえてさらに検討を行い、CRYPTREC における今後の活動方針を検討し、暗号技術評価委員会に提言を行う。

表 2.7　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	2014 年 9 月 2 日	活動計画案、今年度の調査の進め方（昨年度作成した報告書の更新案、ID ベース暗号に関する調査報告書の更新案)
第 2 回	2015 年 2 月 17 日	報告書の更新内容についての審議と了承

表 2.8　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	2014 年 8 月 29 日	活動計画案、委員会への報告内容、今後の活動方針
第 2 回	2014 年 11 月 12 日	軽量暗号に関する論点の整理、報告書案の検討
第 3 回	2015 年 2 月 2 日	委員会への報告内容、報告書、及び、次年度活動計画についての了承

第3章 暗号技術調査ワーキンググループの活動

3.1.暗号解析評価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。本ワーキンググループでは、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。

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：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.活動方針

（1） 格子問題等の困難性に関する調査

2013 年度は、数学的問題の困難性のうち、

(i) Shortest Vector Problem (SVP)
(ii) Learning with Errors (LWE)
(iii) Learning Parity with Noise (LPN)
(iv) Approximate Common Divisor (ACD)

の 4 つを選んで調査を行った。2014 年度も引き続き、これらを利用した公開鍵暗号技術とパラメータ選択に関する調査を行う。

（2） 離散対数問題の困難性に関する調査

CRYPTREC において公表した「ID ベース暗号に関する調査報告書」(2008 年度)及び「2009 年度版リストガイト」において、近年の攻撃により脆弱となったパラメータを指摘し、報告書（の一部）を改訂する。

3.1.4.活動概要

2014 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　2014 年 9 月 22 日　　活動計画案や作業内容についての審議と了承
第 2 回　2015 年 2 月 17 日　　調査内容についての審議と了承

（1）格子問題等の困難性の調査について

主に、上述の数学的問題の困難性(i)～(iv)を利用した公開鍵暗号技術の例とパラメータ選択に関する記述を補った。

（2）離散対数問題の困難性の調査について

大きな標数の素体上構成される DSA 及び DH への安全性に影響はないことの再確認を行った。また、過去の ID ベース暗号に関する調査報告書における、小さな標数の離散対数問題の困難性を利用する際の注意喚起の方法について検討を行った。

（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、2014 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問題に関する 2 つの予測図を更新した。

3.1.5.成果概要

（1）格子問題等の困難性の調査について

2013 年度に作成した「格子問題等の困難性に関する調査」に関して、下記の(a)～(d)の更新部分について検討した。詳しくは、付録 5 を参照のこと。

(a)　第 2 章　一般的な攻撃に関する総論
　① 2.4 計算機実験
　　最新の実験結果を追加した。
(b)　第 3 章　Learning with error (LWE)
　① 3.1.3 節の追加
　　代表的な暗号方式として、Regev による方式および somewhat 準同型暗号方式の概略を記載した。
　② 3.2.2 節の最後に「■近年の攻撃研究の動向」を追加
　　2014 年に ACISP で発表された Binary-LWE 問題に対する攻撃手法の概略について記載した。

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

(c)　第 4 章　Learning parity with noise (LPN)

① 4.2 節に、代表的な暗号方式を追加（旧 4.3-4.5 節から移動した文書有り）

代表的な暗号方式として、Alekhnovich 暗号および McEliece 暗号の概略を記載した。

② 4.3 節(旧 4.2 節)に、いくつかコメントを追加

(d)　第 5 章　Approximate Common Divisor 問題

① 5.1.3 節において、5.1.3.1 節及び 5.1.3.2 節を追加

ACD 問題のアプリケーションとして、van Dijk らおよび Cheon らの somewhat 準同型暗号方式の概略を記載した。

② 5.1.4 節の追加

③ 5.5 節の追加

2014 年に、Cheon らが導入した co-ACD 問題についての概略を記載した。

表 3.1：2013-2014 年度の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(2013 年度)	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	

（2）離散対数問題の困難性の調査について

(a)　過去の ID ベース暗号に関する調査報告書(2008 年度及び 2009 年度)に、図 3.1 の通り、注意喚起のための文言を挿入する。

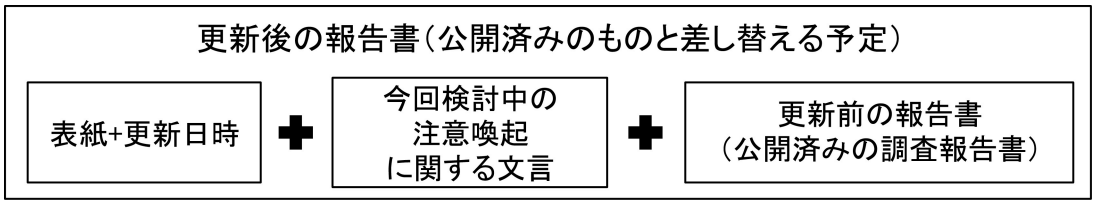


図 3.1: 更新のイメージ

(b)　注意喚起の文案(暗号解析評価 WG 了承)は下記の通りである。

ペアリング暗号の安全性は、楕円曲線上の離散対数問題と有限体上の離散対数問題を解く計算の困難性を基盤としている。有限体上の離散対数問題を効率よく解く手法には数体篩法と関数体篩法があり、前者は標数が大きな有限体に、後者は標数の小さな有限体の場合に利用できる。

標数の大きな有限体上の離散対数問題に適した数体篩法の改良も進んではいるものの、関数体篩法ほどの計算量の改善は現在まで報告されていない。従って、素体上構成されている DSA 及び DH への安全性に影響はない。

近年、関数体篩法において、ペアリング暗号に適した標数の小さいある種のタイプの有限体に対して有効な手法が提案され、計算量が大きく削減された。たとえば、「ID ベース暗号に関する調査報告書(平成 21 年 3 月)」の第 3 章の表内に掲載されているペアリング実装例のうち、表 3.2 の標数 2 において、埋め込み次数 4 で拡大次数 313 以下や、表 3.3 の標数 3 において、埋め込み次数 6 で拡大次数 127 以下は、現実的な時間内で解かれることが見込まれる。

関数体篩法や数体篩法の計算量は、有限体の位数以外に、拡大次数と部分体の位数の比などが関係するため、ペアリング暗号の安全性は利用する有限体ごとに評価する必要がある。詳しくは、「CRYPTREC Report 2014 暗号技術評価委員会報告 付録 6」を参照のこと。

（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 3.2 の通りとなる。

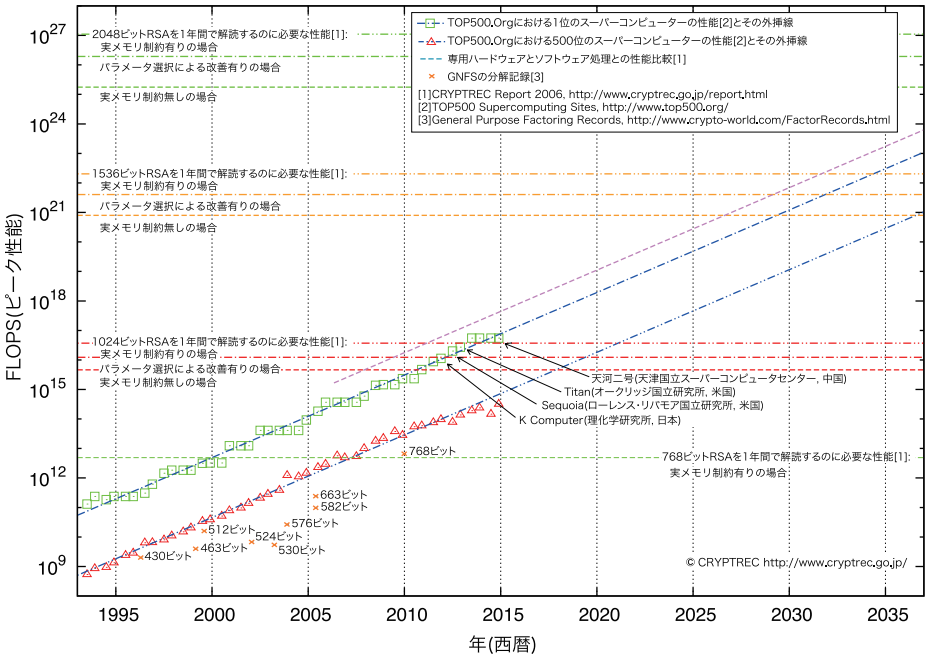


図 3.2：1 年間でふるい処理を完了するのに要求される処理能力の予測(2015 年 2 月更新)

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 3.3 の通りとなる。

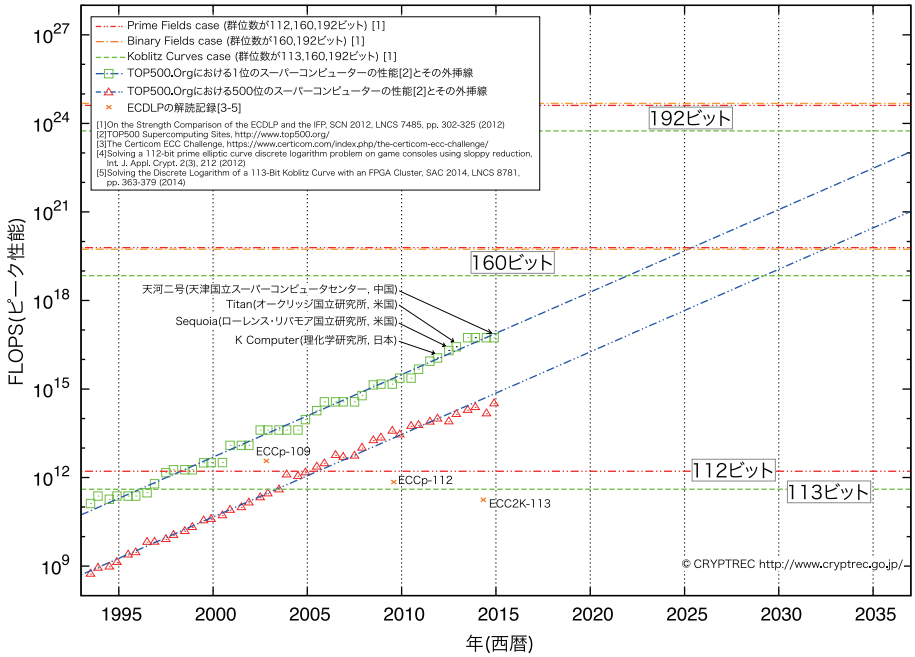


図 3.3： ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測(2015 年 2 月)

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適切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。昨年度は、これまでに提案されている軽量暗号の現状調査、アプリケーションに関する調査、実装評価等を行った。今年度はこれらをふまえてさらに検討を行い、CRYPTREC における今後の活動方針を検討し、暗号技術評価委員会に提言を行う[2]。

3.2.2.委員構成(敬称略、五十音順)

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

Ⅰ.　スケジュール及び審議概要

2014 年 8 月 29 日　　第 1 回軽量暗号 WG

- 本年度活動内容の審議・承認
- 軽量暗号に関する議論（既存暗号に対するアドバンテージ、CRYPTREC で扱う軽量暗号のスコープ、軽量暗号で達成すべき安全性）

  「暗号技術調査 WG(軽量暗号)報告書」の更新方法、執筆担当委員などについて合意した。
- 今後の活動方針に関する議論

[2] 2013 年度及び 2014 年度に調査・検討した内容(提言を含む)を「暗号技術調査 WG(軽量暗号)報告書」としてまとめた。詳しくは、付録 7 を参照のこと。

2014 年 11 月 12 日　第 2 回軽量暗号 WG

- 今年度調査に関する中間報告
- 今後の活動方針に関する議論

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

などの活動案が出されていたが、審議の結果、A）もしくは B）として暗号技術ガイドラインをまとめる方向で進めていくこととなった。

2015 年 2 月 2 日　第 3 回軽量暗号 WG

- 暗号技術評価委員会への報告内容の審議

暗号技術評価委員会への報告内容を合意した。

-「暗号技術調査 WG(軽量暗号)報告書」の内容確認・議論
- 次年度から開始する詳細評価の対象に関する議論

II. 「暗号技術調査 WG(軽量暗号)報告書」各技術分類の執筆担当委員

表 3.2:「暗号技術調査 WG(軽量暗号)報告書」各技術分類の執筆担当委員

<table>
<tr><td colspan="3">第 2 章 軽量暗号に関する現状調査：軽量暗号アルゴリズム</td></tr>
<tr><td rowspan="2">ブロック暗号</td><td>安全性</td><td>実装性能</td></tr>
<tr><td>青木 和麻呂 委員</td><td>渋谷 香士 委員</td></tr>
<tr><td>ストリーム暗号</td><td colspan="2">渡辺 大 委員</td></tr>
<tr><td>ハッシュ関数</td><td colspan="2">三宅 秀享 委員</td></tr>
<tr><td>メッセージ認証コード</td><td colspan="2">渡辺 大 委員</td></tr>
<tr><td rowspan="2">認証暗号</td><td>安全性</td><td>実装性能</td></tr>
<tr><td>峯松 一彦 委員</td><td>鈴木 大輔 委員</td></tr>
<tr><td colspan="3">第 3 章 軽量暗号に関する現状調査：軽量暗号に関わる新しい技術動向</td></tr>
<tr><td>低レイテンシ</td><td colspan="2">﨑山 一男 委員</td></tr>
<tr><td>サイドチャネル攻撃耐性</td><td colspan="2">成吉 雄一郎 委員</td></tr>
<tr><td>CAESAR プロジェクト</td><td colspan="2">岩田 哲 委員</td></tr>
<tr><td>軽量暗号の活用事例
および標準化動向</td><td colspan="2">小川 一人 委員</td></tr>
</table>

3.2.4.暗号技術評価委員会への報告

I. CRYPTREC で扱う軽量暗号のスコープ

- 軽量暗号 WG では、「実装性能と安全性のトレードオフを勘案した上で、従来の暗号技術に対して特定の性能指標で優位性（軽量性）を持つように設計された暗号技術」を軽量暗号のスコープとし、用途が想定される代表的な性能指標(表 3.3)に対して優位性を主張する暗号を主な対象とする。
- 本報告書では共通鍵暗号系の軽量暗号を対象としている。

表 3.3: 代表的な性能指標

性能指標		アプリケーションの例
ハードウェア実装	回路規模（消費電力、コスト）	RFID、低コストセンサー
	消費電力量	医療機器、バッテリ駆動デバイス
	レイテンシ（リアルタイム性能）	メモリ暗号化、車載機器、 産業向け I/O デバイス制御
ソフトウェア実装	メモリサイズ（ROM/RAM）	家電機器、センサー、車載機器

II. 既存の暗号に対して優位性を持つ分野

① 回路規模

- 回路規模の視点では、現在提案されている軽量暗号と AES の差は数 k gate 程度[3]である。
- ミューチップのようなダイサイズが 50μm 角クラスのチップでは数 k gate の差がクリティカルで、暗号機能の搭載可否に影響を与えうる。500μm 角クラスのチップでも 180nm など古いプロセスにおいては実装可否に影響を与える可能性がある。

② 消費電力量

- 一般に回路規模が小さいほど消費電力あるいは消費電力量は減る傾向にあり、軽量暗号を利用することで消費電力あるいは消費電力量に関する設計条件を緩和する効果が期待できる。

③ レイテンシ

- AES に対して 2 倍の応答速度をおよそ 1/10 の回路規模で実現できる軽量暗号が存在する。(20k gate で 10ns 以下での暗号演算が可能。AES では 200k gate で 15ns 要する)

[3] 現在、モバイル向け SoC や GPU で主流の 40nm 以下のプロセスでは、数 k gate 程度の回路規模は暗号の優劣の指標とはなりえない。

・ 産業向けI/Oデバイス制御に代表されるようなμs オーダーのリアルタイム性が求められる用途において、チップへのコストインパクトなしで暗号技術を利用できる。

④ メモリサイズ

・ 組込み機器向けソフトウェア実装のプログラムサイズにおいて、AES に対しておよそ1/4 のROMサイズで実装可能な軽量暗号が存在する。(産業分野や自動車などで利用されているマイコンRL78上で220バイトで実装可能)

・ レガシー製品に暗号機能を搭載する場合、残されたROM領域に実装する必要があり、軽量暗号でないと搭載できないケースが起こりうる。

・ 新規搭載の場合もROM領域が削減できれば、製品単価の安いチップを選定することができる。

[軽量暗号に見込める将来に向けた期待]

・ 2020年、センサー1兆個、IoT 機器500億個がつながる時代に、ローエンドマイコンを搭載する機器に暗号技術が必要になることが予想される。

・ 自動運転の実用化、工場やプラントがクラウドとシームレスにつながる時代に、現時点で暗号技術が利用されていない領域にも利用が広がることが予想される。

・ 現時点で暗号技術を搭載していない、想定すらしていない機器やシステムにおいて、将来的に実装面での制約を緩和する効果を期待できる。

III. 軽量暗号で達成可能な安全性

・ 電子政府推奨暗号リストおよび推奨候補暗号リストに掲載されている暗号技術は、安全性、実装性能が確認された方式であり、カテゴリ毎に想定されている利用の範囲で安全性の問題が生じない、実装性能では実装環境ごとの差が少ないバランスのとれた方式である。

・ 軽量暗号は特定の性能指標で優位性をもつように設計されており、提案されている軽量暗号は上記暗号技術よりも安全性が低くなる、もしくは条件付きの安全性になる傾向にある。

・ 例えば、64 ビットブロック暗号では同じ鍵で2^{32}ブロック(32GB)以上のデータを処理すると、高い確率で無作為に選んだビット列と区別できることが知られている。近年は平文ビット列を導出できることも明らかになってきた。

・ 上記への対策として、①一つの鍵で処理するデータ量を減らす、②CENCのようなモードの利用、③Abdalla-Bellare の方法を活用するなどリスクを回避する利用方法もある。

・ 提案されている軽量ブロック暗号の中には、関連鍵攻撃に対する耐性が保証されていない方式もあるが、関連鍵攻撃が起きないような鍵管理がされていれば許容できる。

・ ブロック長に関する安全性指標については研究が進んでいるが、それ以外の指標に

ついては明らかになっていないことがほとんどである。

・ 電子政府推奨暗号や推奨候補暗号でもリスクなしでの運用は困難であり、軽量暗号でも、利用に応じたリスクを考慮しながらの運用が必要である。

IV. 今後の活動方針に対する提言

軽量暗号WG では、2015 年度以降の CRYPTREC での活動方針として、以下の案 (A) (B) (C) を検討してきた。それぞれの概要と目的、期待される効果を表3.4に示す。

表 3.4: 各方針案の概要・目的と期待される効果

(A) 暗号技術ガイドライン (軽量暗号の最新動向)	(B) 暗号技術ガイドライン (軽量暗号の詳細評価)	(C) 軽量暗号に関する技術公募の実施
- 軽量暗号の最新技術動向をまとめた技術レポート - 軽量暗号の利用促進	- 軽量暗号の安全性と実装性能を統一的に評価した技術レポート - 軽量暗号を選択・利用する際の技術的判断材料として活用 - 軽量暗号の利用促進 - 第三者評価レポートとして活用	- 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・選定 - 電子政府システム等での最適な方式の選択と調達

軽量暗号 WG での議論の結果、今後の活動方針に対して以下のように提言する。

・ 軽量暗号は、特定の性能指標における優位性が認められ、次世代のネットワークサービスでの活用が期待される一方、電子政府推奨暗号リスト掲載の暗号技術ほど高い安全性を保証していない方式もあり、利用において留意すべき点がある。

・ 軽量暗号を選択・利用する際の技術的判断に資することや今後の利用促進をはかることを目的として暗号技術ガイドラインを発行することが有効と考えられる。

・ 暗号技術ガイドラインの発行 ((A)または(B)) について、軽量暗号全体となると膨大であり、また技術分類によって状況が異なる。詳細評価が望ましい分野と、現時点では既存文献のサーベイでよいと思われる分野がある。よって、(A)と(B)のハイブリッド案で軽量暗号に関する暗号技術ガイドラインを作成するのがよいと思われる。

・ 詳細評価を行う技術分類は、新規評価の必要性 (既存文献で十分な評価結果が得られるかどうか)、当該技術分野における我が国の技術の将来性、当該技術分野の現時点での注目度・重要度、評価結果から期待される学術的貢献等を鑑みて決定するのがよいと考えられる。

・ 軽量暗号は、現時点では直ちに電子政府システムで活用される段階ではないと考えるが、今後関連する次世代ネットワークサービスに搭載される可能性があることから、上記の活動は長期的には電子政府システムの安全性向上にも資すると期待される。

3.2.5. 今後の活動方針

軽量暗号 WG から提示された今後の活動方針に対する提言に沿い、A) 軽量暗号の最新動向 および、B) 軽量暗号の詳細評価 のハイブリッドの形で暗号技術ガイドラインの作成を行う。

2015 年度の活動内容(案)

(A) 軽量暗号の最新動向

必要に応じ、本年度作成した「暗号技術調査 WG(軽量暗号)報告書」の内容を更新する。

(B) 軽量暗号の詳細評価

(a) 詳細評価を行う対象技術分類の選定

軽量認証暗号、軽量 MAC、軽量ブロック暗号を検討の対象とする。

(b) 詳細評価対象技術分類に関する評価内容の策定

(c) 具体的な詳細評価の実施

詳細評価の対象技術分類の有力候補である軽量認証暗号について、関連する CAESAR プロジェクトの動向を鑑み、次年度は、第 1 回暗号技術評価委員会の開催に先んじて第 1 回軽量暗号 WG を開催する可能性もある。

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。

CRYPTREC 暗号リストの変更案

（2014 年度第 2 回暗号技術検討会了承）

（略）

運用監視暗号リスト

（略）

（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） 互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。

（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。

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成 27 年*月**日	（注10）	128-bit RC4 は 、SSL（TLS1.0 以上）に限定して利用すること。	互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLS での利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。

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 186-4 (July 2013), Digital Signature Standard (DSS) で規定されたもの。 ・ 参照 URL <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>

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 ・参照 URL ・SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) <http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/01_01sec1.pdf>
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/>

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.2.2) ・参照 URL <http://japan.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf> 和文：なし 英文：http://www.emc.com/security/rsa-bsafe.htm
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　ソリューション営業部　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.2.2) ・参照 URL <http://japan.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf> 和文：なし 英文：http://www.emc.com/security/rsa-bsafe.htm
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　ソリューション営業部　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.2.2) ・参照 URL <http://japan.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf> 和文：なし 英文：http://www.emc.com/security/rsa-bsafe.htm
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　ソリューション営業部　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/〉
関連情報 2	仕様 ・NIST Special Publication 800-56A Revision 1 (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/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf>

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 ・参照 URL ・SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) <http://www.cryptrec.go.jp/cryptrec_03_spec_cypherlist_files/PDF/01_01sec1.pdf>
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 Revision 1(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/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf>

2. 共通鍵暗号

暗号名	Triple DES
関連情報	仕様 ・NIST SP 800-67 Revision 1, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, January 2012. ・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:0422-59-4015 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 グループリーダー　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 180-4, Secure Hash Standard (SHS) ・参照 URL 〈http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf〉

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　スマートネットワーク事業部 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　スマートネットワーク事業部 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	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 プロダクト統括本部 開発基盤本部 ソフトウェア生産技術部　主任技師 栗田 博司 TEL：050-3154-4218, FAX ： 045-865-9065 E-MAIL：hiroshi.kurita.wp@hitachi.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　研究開発グループ　システムイノベーションセンタ セキュリティ研究部　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	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 プロダクト統括本部 開発基盤本部 ソフトウェア生産技術部　主任技師 栗田 博司 TEL：050-3154-4218, FAX ： 045-865-9065 E-MAIL：hiroshi.kurita.wp@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.2.2) ・参照 URL 〈http://japan.emc.com/emc-plus/rsa-labs/pkcs/files/h11300-wp-pkcs-1v2-2-rsa-cryptography-standard.pdf〉 和文：なし 英文：http://www.emc.com/security/rsa-bsafe.htm
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　ソリューション営業部　三田 晃 TEL：03-6830-3341，FAX：03-5308-8979，E-MAIL：akira.mita@rsa.com

2．共通鍵暗号

暗号名	RC4
関連情報	仕様 ・RC4 は EMC Corporation 社のトレードマークである。 ・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.cryptrec.go.jp/cryptrec_13_spec_cypherlist_files/PDF/cryptobytes_v5n2.pdf〉

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 186-4, Secure Hash Standard (SHS) ・参照 URL <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.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
★	A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic [Eurocrypt 2014, BEST PAPER]	56
★	Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus [Eurocrypt 2014]	56
★	Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster [SAC 2014]	58
☆	A Generic Algorithm for Small Weight Discrete Logarithms in Composite Groups [SAC 2014]	59
★	Partial Key Exposure Attacks on RSA: Achieving Boneh-Durfee's Bound [SAC 2014]	59
★	Batch NFS [SAC 2014]	59
☆	Security Analysis of Multilinear Maps over the Integers [Crypto 2014]	61
★	Breaking `128-bit Secure' Supersingular Binary Curves (or how to solve discrete logarithms in $F_{2^{4\cdot 1223}}$ and $F_{2^{12\cdot 367}}$) [Crypto 2014]	62
☆	Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms – Simplified Setting for Small Characteristic Finite Fields [Asiacrypt 2014]	68
ストリーム暗号		
☆	Big Bias Hunting in Amazonia: Large-scale Computation and Exploitation of RC4 Biases [Asiacrypt 2014]	68
ブロック暗号		
☆	Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities [Eurocrypt 2014]	57
★	Colliding Keys for SC2000-256 [SAC 2014]	60
☆	Improved Differential Cryptanalysis of Round-Reduced Speck [SAC 2014]	59
☆	An Improvement of Linear Cryptanalysis with Addition Operations with Applications to FEAL-8X [SAC 2014]	60
☆	Low Probability Differentials and the Cryptanalysis of Full-Round CLEFIA-128 [Asiacrypt 2014]	67
☆	Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon [Asiacrypt 2014]	67
☆	A Simplified Representation of AES [Asiacrypt 2014]	67
☆	Multi-user collisions: Applications to Discrete Logarithm, Even-Mansour and PRINCE [Asiacrypt 2014]	68
☆	Meet-in-the-Middle Attacks on Generic Feistel Constructions [Asiacrypt 2014]	69
☆	Differential Analysis and Meet-in-the-Middle Attack against Round-Reduced TWINE [FSE 2015]	69
★	Improved Higher-Order Differential Attacks on MISTY1 [FSE 2015]	70
★	Meet-in-the-Middle Technique for Truncated Differential and its Applications to CLEFIA and Camellia [FSE 2015]	70

☆	Side-Channel Analysis of Multiplications in GF(2^{128}): Application to AES-GCM [Asiacrypt 2014]	69
	故障利用攻撃	**頁**
☆	Tampering Attacks in Pairing-Based Cryptography [FDTC 2014]	62
	On the Effects of Clock and Power Supply Tampering on Two Microcontroller Platforms [FDTC 2014]	63
	Parametric Trojans for Fault-Injection Attacks on Cryptographic Hardware [FDTC 2014]	63
☆	Algebraic Fault Analysis on GOST for Key Recovery and Reverse Engineering [FDTC 2014]	63
☆	Differential Fault Analysis on the Families of SIMON and SPECK Ciphers [FDTC 2014]	63
	Differential Fault Intensity Analysis [FDTC 2014]	63
	Fault Sensitivity Analysis Meets Zero-Value Attack [FDTC 2014]	63
☆	On Fault Injections in Generalized Feistel Networks [FDTC 2014]	64
☆	Blind Fault Attack against SPN Ciphers [FDTC 2014]	64
☆	Clock Glitch Attacks in the Presence of Heating [FDTC 2014]	64
	Practical Validation of Several Fault Attacks against the Miller Algorithm [FDTC 2014]	64
☆	A Practical Second-Order Fault Attack against a Real-World Pairing Implementation [FDTC 2014]	64

1.2. Eurocrypt 2014 の発表

1.2.1. Eurocrypt 2014 の発表(1 日目)

A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic [Eurocrypt 2014, BEST PAPER]

Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, Emmanuel Thomé

離散対数問題(DLP: Discrete Logarithm Problem)に対する新しい解読法を提示した。計算量評価はヒューリスティックな仮定を用いているが、小標数の場合に計算量は準多項式時間となっており、これまで最速であった関数体篩法の準指数時間を上回る結果となっている。電子政府推奨暗号では、電子署名アルゴリズム DSA 及び鍵共有アルゴリズム DH が該当するが、参照先の仕様のパラメーターは素体(大標数)であり、対象外となっている。ただし、小標数の DLP の困難性に基づいた暗号技術を使用する場合には、新解読アルゴリズムによる評価結果を考慮する必要がある。

Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus [Eurocrypt 2014]

Jean-Charles Faugere, Louise Huot, Antoine Joux, Guenael Renault, Vanessa Vitse

楕円曲線上の離散対数問題(ECDLP: Elliptic Curve Discrete Logarithm Problem)に対する解読法の改良を提示した。電子政府推奨暗号では、鍵共有アルゴリズム ECDH が該当する。捩(ねじ)れ点写像の性質を用いる改良であり、例えば IPSEC(SECurity architecture for Internet Protocol)の鍵共有プロトコルに使われている曲線に適用可能であり、解読時間の短縮を図ることができる。

Generic Universal Forgery Attack on Iterative Hash-based MACs [Eurocrypt 2014]
Thomas Peyrin and Lei Wang
ハッシュベースのメッセージ認証コードに対する偽造攻撃の改良が提示された。電子政府推奨暗号では、メッセージ認証コード HMAC が該当する。例えば、任意のメッセージに対する偽造は、RIPEMD-160 を用いた HMAC では、これまで 2^{160} の計算量が必要と考えられていたが、$2^{133.3}$ に改良できるという結果である。

Links Between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities [Eurocrypt 2014]
Celine Blondeau and Kaisa Nyberg

ブロック暗号に対する様々な攻撃間の関係(同値性、時間メモリトレードオフによる変換等)をより明らかにする発表を行った。応用例として、26 段 PRESENT に対する既知の多次元線型識別(Multi-dimensional Linear Distinguisher)攻撃が、既知の既知平文(Known Plaintext)攻撃より少ないメモリにより選択平文(Chosen Plaintext)鍵回復攻撃に変換できることを示した。

1.3. SAC 2014 の発表

1.3.1. SAC 2014 の発表(1 日目)

Practical Cryptanalysis of PAES [SAC 2014]
Jeremy JEAN, Ivica Nikolić, Yu Sasaki, Lei Wang
CAESAR 候補 PAES に対する現実的な 2 種類の攻撃を示した。一つは 240 バイト以上の任意の平文に適用できる普遍的偽造(universal forgery)攻撃で繰り返し型の nonce を使用するときに適用でき、2^{11} の時間とデータしか必要としない。第 2 の攻撃は、2^{128} 個中 2^{64} 個の鍵に適用できるもので、既知の平文・暗号文組と無視できる程度の計算量で実行される。これらは PAES が目指す安全性が満たされないことを示しており、設計者は既に投稿を取り下げている。

Error-Tolerant Side-Channel Cube Attack Revisited [SAC 2014]
Jeremy JEAN, Ivica Nikolić, Yu Sasaki, Lei Wang
CHES 2013 で Dinur と Shamir は、Cube 攻撃を 2 元対称通信路の復号問題と見なすことで、エラー耐性を持たせた。本論文では、多項式近似等を用いてエラー耐性を大幅に改善した。PRESENT の実装に対する実験では、エラー確率が 40.5%の測定 $2^{21.2}$ 回で鍵回復成功率 50%を達成した。

Side-Channel Analysis of Montgomery's Representation Randomization [SAC 2014]
Eliane Jaulmes, Emmanuel Prouff, Justine Wild

CHES 2012 で、楕円曲線暗号のサイドチャネル攻撃対策として、Montgomery のスカラー倍算における中間計算結果をランダム化する方法が提案された。この提案ではハードウェア実装においてピアソンの相関を識別子とする一次のサイドチャネル攻撃に打ち勝つことを目的としていた。本論文では、この対策に欠陥があり、一次相関を利用した効果的な攻撃が示された。

Differential Cryptanalysis of SipHash [SAC 2014]

Eliane Jaulmes, Emmanuel Prouff, Justine Wild

SipHash は、INDOCRYPT 2012 で Aumasson と Bernstein によって提案した ARX (Addition-Rotation-XOR)型のメッセージ認証コードで、短いメッセージを高速に処理するように設計された。提案後、多くの実装性能が評価されたが、第 3 者による安全性評価はなかった。本論文では、SipHash の差分特性を既存の探索ツールを改良して探索した結果が報告された。SipHash-2-4 に対し、差分特性確率 $2^{-236.3}$ の経路を発見し、最終処理の識別子は現実的な計算量に収まるという結果を得ている。探索ツールの改良は、ARX 関数に対する確率計算における概念の拡張などによって実現した。

The Usage of Counter Revisited: Second-Preimage Attack on New Russian Standardized Hash Function [SAC 2014]

Jian Guo, Jeremy Jean, Gaëtan Leurent Leurent, Thomas Peyrin, Lei Wang

Streebog はロシアの標準規格 GOST R 34.11-2012 で規定されたハッシュ関数で、国際規格 ISO/IEC 10118-3(専用ハッシュ関数)への追加が検討されている。基本構造にはドメイン拡張にカウンターを利用する HAIFA 型を採用している。設計者は長いメッセージに対して、近年の第 2 原像攻撃への耐性があると主張しているが、本論文では、HAIFA 型の使い方が適切でないため、Streebog-512 の第 2 原像が計算量 2^{266} で求まるとの理論評価が示されている。

Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster [SAC 2014]

Erich Wenger, Paul Wolfger

楕円曲線上の離散対数問題を解くのに FPGA クラスタを使うことは広く知られているが、最近まで新規の楕円曲線を最初に解いた実績があるのは CPU クラスタだけだった。本論文では、113 ビットの Koblitz 曲線上の離散対数問題を高速 FPGA 実装で解いた結果が示された。使用したデザインでは、self-sufficient な Pollard の ρ 法を fully unrolled、高次のパイプライン化で実装。18 コアの Virtex-6 FPGA クラスタを使って、24 日間で解いた。著者によると、今までに、このように大きな Koblitz 曲線上に対する攻撃に小さなリソースで短時間に成功した例はない。

1.3.2. SAC 2014 の発表(2 日目)

A Generic Algorithm for Small Weight Discrete Logarithms in Composite Groups [SAC 2014]

Alexander May

合成位数 N の任意の巡回群を$(G, \cdot)$とする。ただし、$G \cong G_1 \times G_2$。本論文では、G 上の離散対数の汎用解法を示し、計算時間は$\tilde{O}\left(\sqrt{p} + \widetilde{\sqrt{|G_2|^{H(\delta)}}}\right)$ と評価された。ここで、ハミング重みを$\delta \log(N)$、p はG_1の最大素因数、$H(\cdot)$は 2 元エントロピー関数である。この結果は、$\delta = 1/2$以外では、Silver-Pohlig-Hellman の方法より計算時間が短い。

Partial Key Exposure Attacks on RSA: Achieving Boneh-Durfee's Bound [SAC 2014]

Atsushi Takayasu, Noboru Kunihiro

RSA の秘密鍵指数dが小さいとき($d < N^{\beta}$)、$(\beta - \delta)\log N$個の最下位ビット(LSBs)から d を求める方法がいくつか提案されていたが、Boneh と Durfee は、$\beta < 1 - \sqrt{2}$のとき、e が N と同じビット長なら常に攻撃が成功することを示した。しかし、それ以前に示された攻撃方式は常に成功するというわけではなかった。本論文は Boneh-Durfee の結果を$\delta = \beta$ まで拡張したもので、 $d \leq N^{9/16}$のときの MSBs、または、$d \leq N^{(9-\sqrt{21})/12}$のときの LSBs から$d$を特定する最良の方法を示した。

Batch NFS [SAC 2014]

Tanja Lange

個々の RSA 秘密鍵ではなく、多数の RSA 秘密鍵をターゲットにし、並列化を高めることによって、鍵 1 個あたりの攻撃コストを下げるバッチ型の攻撃を追求した。攻撃対象は、100 個以上の DNSSEC トップレベルドメインの 1024 ビット RSA 鍵など。標準的な発見的数体篩法(NFS)のバッチ型実装の領域と計算時間を評価したところ、RSA 鍵をBビット、$L = \exp\left((\log(2^B)^{1/3}(\log\log(2^B))^{2/3}\right)$とするとき、領域 $L^{1.181\cdots+o(1)}$で$L^{0.5\cdots+o(1)}$個の B ビット RSA 鍵を時間 $L^{1.022\cdots+o(1)}$ で抽出できるとの評価を得た。

Improved Differential Cryptanalysis of Round-Reduced Speck [SAC 2014]

Itai Dinur

NSA が設計したソフトウェア実装向け軽量暗号 Speck に対する差分解読法を改良し、従来より攻撃可能段数を伸ばした。結果は次表の通り。

パラメータ 2n/mn	攻撃可能 ／全段数	時間複雑度	データ複雑度(CP)	メモリ	論文
32/64	11/22	$2^{46.7}$	$2^{37.1}$	$2^{37.1}$	Abed et al. (FSE 2014)
32/64	11/22	2^{46}	2^{14}	2^{22}	本論文
32/64	12/22	2^{51}	2^{19}	2^{22}	本論文
32/64	13/22	2^{57}	2^{25}	2^{22}	本論文
32/64	14/22	2^{63}	2^{31}	2^{22}	本論文
…	…	…	…	…	…
128/128	16/32	2^{116}	2^{116}	2^{64}	Abed et al. (FSE 2014)
128/128	17/32	2^{113}	2^{113}	2^{22}	本論文
128/192	18/33	$2^{182.7}$	$2^{126.9}$	$2^{121.9}$	Abed et al. (FSE 2014)
128/192	18/33	2^{177}	2^{113}	2^{22}	本論文
128/256	18/34	$2^{182.7}$	$2^{126.9}$	$2^{121.9}$	Abed et al. (FSE 2014)
128/256	19/34	2^{241}	2^{113}	2^{22}	本論文

Colliding Keys for SC2000-256 [SAC 2014]

Alex Biryukov, Ivica Nikolić

推奨候補暗号リストに掲載されているブロック暗号 SC2000 の 256 ビット鍵版(SC2000-256)に対し、平文と暗号文の対応が同じになる等価鍵の組が約 2^{68} 組存在し、2^{58} 回の計算で全部を見出せるという理論評価結果が示された。実際の PC による実験で、2^{39} 回分の計算でこのような組が発見でき、これは効率なアルゴリズムを利用することで、通常の PC で数時間で実行できることが示された。さらに、SC2000-256 を利用した Davies-Meyer 型及び広瀬型のハッシュ関数の衝突発見がどれだけ現実的かが説明された。この結果の概要は、CRYPTREC Report 2012「暗号方式委員会報告書」で紹介されている。

An Improvement of Linear Cryptanalysis with Addition Operations with Applications to FEAL-8X [SAC 2014]

Eli Biham, Yaniv Carmeli

松井氏(三菱電機)が FEAL の発表 25 周年を記念して実施した解読チャレンジの優勝者による発表。FEAL-8X に対する線形解読法を改良して、2^{14} 個の既知平文を使い、14 時間の計算で鍵を復元した。攻撃の特徴は、加算ベースの S-box の近似を、偏差が拡大するようないくつかのセットに分類する点である。さらに、2～3 個の既知平文を使った鍵全数探索よりずっと速い鍵回復攻撃も示している。

1.4. Crypto 2014 の発表

1.4.1. Crypto 2014 の発表(1 日目)

Updates on Generic Attacks against HMAC and NMAC [Crypto 2014]

Jian Guo, Thomas Peyrin, Yu Sasaki, Lei Wang

HMAC と類似の MAC に対する汎用の偽造攻撃 4 種を提案した。攻撃者が最初に攻撃するメッセージをコミットする攻撃(selective forgery)2 種、計算量$O(2^{l/2})$を要するタイトな攻撃 1 種、計算量は$O(2^{3l/2})$と大きくなるもののコミットするメッセージの自由度がより大きい攻撃攻撃 1 種である。与えられたメッセージに対する署名を偽造する攻撃(universal forgery)では、計算量を従来の$O(2^{5l/6})$から $O(2^{3l/4})$ に削減した。最後に、HMAC に対する初の time-memory tradeoff 攻撃で、事前計算$O(2^{l})$で、最初の内部鍵K_{out}を計算量$O(2^{2l/3})$で復元、もう一つの内部鍵K_{in}を計算量$O(2^{3l/4})$で復元した。これらの攻撃では、拡張可能メッセージ型の第 2 原像攻撃や関数型グラフベース偽造攻撃など様々な技法が拡張されている。

Improved Generic Attacks Against Hash-based MACs and HAIFA [Crypto 2014]

Itai Dinur, Gaëtan Leurent

HMAC の安全性が$O(2^{l})$を大きく下回ることが、Leurent 他、及び、Peyrin 他によって明らかにされつつある。本論文では、具体的なメッセージ長が限定されたり、特殊な繰り返しモードといった特徴を持つ具体的なハッシュ関数に焦点を当て、より拡張された結果を示す。最初は、HAIFA 型ハッシュ関数を使った HMAC に対する初の状態回復攻撃で、計算量は$O(2^{4l/5})$である。次に HMAC に対する状態回復攻撃におけるメッセージ長と計算複雑度のトレードオフを記述する。これらの結果を利用して、最大メッセージ長が限定されている、いくつかの HMAC の設計に対する攻撃を構成。最後に、MAC オラクルに対して短いメッセージのクエリを送る初の汎用偽造攻撃を示す。特に、SHA-1 と SHA-2 に適用可能な最初の偽造攻撃になっている。

Security Analysis of Multilinear Maps over the Integers [Crypto 2014]

Hyung Tae Lee, Jae Hong Seo

Crypto 2013 で Coron, Lepoint, Tibouchi(CLT)が実用的な整数上の多線形写像として設計した Graded Encoding Scheme(GES)に対する攻撃を示した。攻撃の複雑度は Coron らによる従来の最小値$O(2^{\rho})$より小さい $O(2^{\rho/2})$である。ここで、ρ はセキュリティパラメータである。さらに、CLT GES のゼロ試験パラメータの生成における欠陥を利用することで、この攻撃法の実行時間が大幅に減らせることを示した。

1.4.2. Crypto 2014 の発表(2 日目)

RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis [Crypto 2014]

Daniel Genkin, Adi Shamir, Eran Tromer

PC の CPU が発生するノイズから、RSA の 4096 ビット鍵を回復するのに成功した。RSA 暗号のソフトウェアはポピュラーな GnuPG であり、いくつかの暗号文を復号する過程で生じる音を利用することによって、1 時間以内で全鍵ビットの回復に成功した。驚くべきことに、PC のクロックレートの GHz 域より何桁も低い 20kHz 以下(通常のマイク使用時)や数百 kHz

帯(超音波マイク使用時)の音声情報で攻撃できた。この攻撃は、PC に近くに携帯電話を置いたり、10m 離れたところにより高性能のマイクを置くことで攻撃が可能であることを意味している。発表では、壇上にノート PC と集音用パラボラ付きマイクを持込み、RSA の鍵ビットを読み取る様子をデモして見せた。

1.4.3. Crypto 2014 の発表(3 日目)

Breaking ‘128-bit Secure’ Supersingular Binary Curves (or how to solve discrete logarithms in $F^{24\cdot1223}$ and $F^{212\cdot367}$) [Crypto 2014]
Robert Granger, Thorsten Kleinjung, Jens Zumbragel
従来 128 ビットの安全性を有していると考えられていた散対数問題(DLP: Discrete Logarithm Problem)が、実際にははるかに低いことを示した。一つは genus 1 の超特異曲線が対象で、F_2^{4*1223} 上の離散対数問題が約 59 ビットの安全性しかないことを示した。もう一つは genus 2 の超特異曲線が対象で、F_2^{12*367} 上の離散対数問題を実際に解くことに成功した。これらの攻撃は、新しい体の表現法と実用的な降下原理を利用することによって効率を高めている。

1.5. SHA-3 2014 WORKSHOP の発表

1.5.1. SHA-3 2014 WORKSHOP の発表(1 日目)

Practical Complexity Cube Attacks on Round-Reduced Keccak Sponge Function [SHA-3]
Itai Dinur
Keccak は SHA-3 として採用されることが決まっているハッシュ関数であり、主要部は 1600 ビットの置換 f を使用したスポンジ構造で構成される。Keccak はわずかな変更で、MAC 及びストリーム暗号として利用できる。この発表では、PC で検証できる現実的な CUBE 攻撃を試み、MAC に対しては攻撃可能な(縮小)段数を従来の 4 段から 5 段に拡張した。また、ストリーム暗号モードに対する初の結果として、6 段縮小版が攻撃できることを示した。

1st and 2nd Preimage Attacks on 7, 8 and 9 Rounds of SHA3-224, 256, 384, 512 [SHA-3]
Donghoon Chang
SHA3-224/256/384/512 に対する原像攻撃及び第 2 原像攻撃を示した。先行する J.Bernstein の結果である Keccak-256 及び Keccak-512 に対する適用可能段数 2 段及び 8 段を、各々、8 段及び 9 段に拡張した。総当たり攻撃に対する計算時間の改善指数は、各々、1.29 及び 1.23 である。

1.6. FDTC 2014 の発表

1.6.1. FDTC 2014 の発表(2 日目)

Tampering Attacks in Pairing-Based Cryptography [FDTC 2014]
Johannes, Blomer, Peter Gunther, Gennadij Liske
ペアリング暗号に対する故障利用攻撃のサーベイ。Tate ペアリングを中心に、最終べき乗演算に対する攻撃とその対策に関する論文を紹介した。

On the Effects of Clock and Power Supply Tampering on Two Microcontroller Platforms [FDTC 2014]

Michael Hoefler, Thomas Korak

故障利用攻撃では、クロック信号と供給電位の２つが主に使われる。本論文では、AES を実装した２つのマイクロコントローラ ARM Cortex-M0 と ATxmega 256(XILINX Spartan-6 XC6SLX45 FPGA)に対し、短時間の供給電位低下とクロック信号へのグリッチの組み合わせで、誤動作を効率的に誘発できることを示した。

Parametric Trojans for Fault-Injection Attacks on Cryptographic Hardware [FDTC 2014]

Raghavan Kumar, Philipp Jovanovic, Wayne Burleson, Ilia Polian

故障利用攻撃がしやすいようにトロイを埋め込む方法を提案した。不純物をドープする濃度や範囲を注意深く操作することでトランジスタの電気特性を変更することで実現する。軽量暗号 PRINCE を実装した CMOS-ASIC に対し、20%の電位低下で 0.001 の確率でトロイが活性化することを確認した。

Algebraic Fault Analysis on GOST for Key Recovery and Reverse Engineering [FDTC 2014]

Xinjie Zhao, Shize Guo, Fan Zhang, Tao Wang, Zhijie Shi, Dawu Gu

ブロック暗号 GOST 28147-89 に対してる代数的故障攻撃を適用した結果を紹介した。8 個の S-box が既知のときの必要故障数を従来の 64 個から 8 個に減らし、未知のときの必要故障数を従来の 270 個から 64 個に減らした。この結果は理論上のものであり、実験での検証はされていない。

Differential Fault Analysis on the Families of SIMON and SPECK Ciphers [FDTC 2014]

Harshal Tupsamudre, Shikha Bisht, Debdeep Mukhopadhyay

米国 NSA が提案した軽量暗号 SIMON と SPECK に対する初の故障利用攻撃の報告。SIMON に対する攻撃は２種類で、一つはビット反転を利用するもので、最終段の n ビット鍵の復元に n/2 回の故障が必要。もう一つはバイトがランダムに変化するモデルで、平均 n/8 回の故障で最終段鍵 n ビットを復元する。SPECK に対する攻撃はビット反転を利用するものだけで、平均 n/3 回の故障で最終段鍵 n ビットを回復できた。

Differential Fault Intensity Analysis [FDTC 2014]

Nahid Farhady Ghalaty, Bilgiday Yuce, Mostafa Taha, Patrick Schaumont

本論文が提案する差分故障強度解析(DFIA)は、故障注入におけるビット反転に偏りがあることと、故障注入の強度に応じて、反転ビット数が 1 個、2 個、3 個と増えていくという仮定のもと構成された攻撃法である。この攻撃法の特長は、故障伝搬の解析が不要であること、正確な故障の中身は必要でなく偏りだけを仮定すること、故障感度解析のようにプロファイリングの段階を必要としないこと、の３つである。FPGA 上に実装された AES に対して DFIA を適用したところ、平均 7 回の誤動作注入で 128 ビット鍵の復元に成功した。

Fault Sensitivity Analysis Meets Zero-Value Attack [FDTC 2014]

Oliver Mischke, Amir Moradi, Tim Guneysu

AES の S-box の実装に含まれる逆元計算で、0 から 0 への写像が他と比べて非常に速いこと

を利用した攻撃法の提案。現状の対策法を利用した AES の実装にこの攻撃法を適用したところ、8 時間以内で全鍵ビットの復元に成功した。

On Fault Injections in Generalized Feistel Networks [FDTC 2014]
Helene Le Bouder, Gael Thomas, Yanis Linge, Assia Tria
一般化 Feistel 構造のブロック暗号に対する故障利用攻撃に関し、故障が影響を及ぼす S-box の個数に着目した解析を行い、必要な故障の回数を評価した。解析対象の暗号は、DES、MIBS、TWINE、CLEFIA の 4 種類。

Blind Fault Attack against SPN Ciphers [FDTC 2014]
Roman Korkikian, Sylvain Pelissier, David Naccache
SPN 構造のブロック暗号に対する Blind Fault Attack の提案と実験結果の報告。ここで、Blind というのは平文と暗号文の具体的な値は必要としない。鍵と平文を固定して故障を起こさせ、SPN 段の入出力のハミング重みを観測することで鍵を推定する。ここでは、3 種類のブロック暗号 LED、AES、SAFER++に対するシミュレーションで有効性を確認した。

Clock Glitch Attacks in the Presence of Heating [FDTC 2014]
Baris Ege, Thomas Korak, Michael Hutter, Lejla Batina
クロック信号にグリッチを入れる故障注入の効果には温度依存性が有り、室温のときより 100℃の方が故障が起きやすいことを確認した。さらに、グリッチによって命令を繰り返させることが可能であることが示された。

Practical Validation of Several Fault Attacks against the Miller Algorithm [FDTC 2014]
Nadia El Mrabet, Jacques Fournier, Louis Goubin, Ronan Lashermes, Marie Paindavoine
Miller アルゴリズムと最終指数計算を使った Tate ペアリングに対する既存のサイドチャネル攻撃対策実装に対して有効な 2 種類の攻撃法を開発した。一つは加算の際に最下位ワードに誤りを注入する方法、もう一つは Miller アルゴリズムのループをスキップさせる方法であり、実際にこれらが可能であることを実験で確認した。

A Practical Second-Order Fault Attack against a Real-World Pairing Implementation [FDTC 2014]
Johannes Blomer, Ricardo Gomes da Silva, Peter Gunther, Juliane Kramer, Jean-Pierre Seifert
Miller アルゴリズムを利用したペアリング暗号の実装に対する故障利用攻撃はいくつか提案されているが、有効性が理論的に評価されていなかったので、実際に評価した。その結果、ペアリング暗号に対する呼称利用攻撃は現実的脅威であることを証明した。実際に、AVR XMEGA A1 上に実装したオープンソースの ATE ペアリングに対して、二次故障利用攻撃を行い、成功した。

1.7. CHES 2014 の発表

1.7.1. CHES 2014 の発表(1 日目)

A New Framework for Constraint-Based Probabilistic Template Side Channel Attacks [CHES 2014]

Yossef Oren, Ofir Weisse, Avishai Wool

サイドチャネル攻撃に SAT-solver や Pseudo-Boolean-solvers を適用する研究はあるが、ビットレベルの記述が要求される。この論文では、バイトレベルの記述が利用でき、ノイズにも強い solver を提案する。この solver を DPA v4 contest のデータセットに適用したところ、1～2 波形で確率 79%の成功率で AES 鍵の導出に成功した。

How to Estimate the Success Rate of Higher-Order Side-Channel Attacks [CHES 2014]

Victor Lomne, Emmanuel Prouff, Matthieu Rivain, Thomas Roche, Adrian Thillard

実際に攻撃して鍵の回復を行うことをせずに、サイドチャネル攻撃の成功率を評価する方法を示した。この方法を 2 つの異なる CMOS マイクロコントローラ(130nm と 350nm)上にマスク実装された AES に適用し、シミュレーションと実験によってその有効性を確認した。

Good is Not Good Enough: Deriving Optimal Distinguishers from Communication Theory [CHES 2014]

Annelie Heuser, Olivier Rioul, Sylvain Guilley

サイドチャネル情報を通信チャネルと見なすことによって、数学的に最適なサイドチャネルの distinguisher を構成した。モデルが分かっていて、ノイズがガウシアンであるとき、この distinguishers は相関電力解析(CPA)を上回る性能を示す。ただし、モデルが比例スケールでしか分かってないときは、CPA が最適であることも示せる。また、ノイズがガウシアンでないときは、異なる最適な distiguisher が作れる。モデルが不完全にしか分かってないとき、鋭敏なビットの荷重和を使うことにより、古典的な線形回帰モデルを上回る性能を発揮する。

“Ooh Aah... Just a Little Bit”: A small amount of side channel can go a long way [CHES 2014]

Naomi Benger, Joop van de Pol, Nigel P. Smart, Yuval Yarom

X86 プロセッサに実装した OperSSL の ECDSA 署名を対象に、FLUSH+RELOAD サイドチャネル攻撃を利用して少量のデータを導出し、格子基底縮小(lattice reduction)を使って秘密鍵を導出することに成功した。FLUSH+RELOAD はキャッシュ攻撃の一種で、ECDSA の ephemeral 鍵を部分的に回復するのに利用した。Bitcoin プロトコルで使用されている secp256k1 曲線を使った実験で、署名生成 200 回で 256 ビット曲線の秘密鍵の導出に成功した。

1.7.2. CHES 2014 の発表(2 日目)

Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs [CHES 2014]

Daniel Genkin, Itamar Pipman, Eran Tromer

ノート PC の金属シャーシの電位変動を利用して、ポピュラーな RSA 暗号と ElGamal 暗号のソフトウェア実装に対するサイドチャネル攻撃が可能であることを示した。電位変動の取得は手で触れたり露出した金属を接触させることで可能で、イーサネット、VGA、USB ケー

ブルを通して測定する。実際にこの攻撃で、4096 ビットの RSA 鍵と 3072 ビットの ElGamal 鍵の回復に成功した。CPU のクロック周波数は GHz スケールだが、2MHz 付近の中周波数での数秒の測定、または、40kHz までの低周波数での 1 時間程度の測定で、攻撃が可能である。

Side-Channel Attack Against RSA Key Generation Algorithms [CHES 2014]
Aurelie Bauer, Eliane Jaulmes, Victor Lomne, Emmanuel Prouff, and Thomas Roche
RSA 暗号用の鍵生成で素数生成アルゴリズムが利用されるが、実装において、ANSI X9.31 と FIPS 186-4 でサイドチャネル攻撃対策の実装法が記されている。この報告では、通常攻撃対象とする証明可能素数試験ではなく、通常の対策で安全と考えられている素数篩の過程を対象にする。それにより、半分以上のビットを回復し、有名な Coppersmith による格子基底縮小法と組み合わせることで、1024 ビットの RSA のモジュラスを回復に成功した。

RSA meets DPA: Recovering RSA Secret Keys from Noisy Analog Data [CHES 2014]
Noboru Kunihiro and Junya Honda
RSA 暗号に対するコールドブート攻撃や差分電力解析では、秘密鍵の回復にノイズを含んだ二進データが利用されている。この報告では、二値化する前のノイズを含んだアナログのままのデータを利用した２種類の攻撃アルゴリズムを提案している。具体的には、平均値と分散を仮定して鍵ビットを推定するものであり、最尤推定法を使って、多項式時間のアルゴリズムを構成している。最初のアルゴリズムはノイズ分布が正確に分かっていることを仮定するもので、２番目のアルゴリズムは差分電力解析のアイデアを利用し、はっきりしたノイズの分布を必要としない。

Simple Power Analysis on AES Key Expansion Revisited [CHES 2014]
Christophe Clavier, Damien Marion, and Antoine Wurcker
AES の鍵拡大計算を 8 ビット環境で実装を対象に、ハミング重みが観察できる状況に対し、Mangard や VanLaven 他の先行研究があり、対策なし実装に対する鍵回復攻撃の方法が示されるている。この報告では、２種類のブーリアンマスクを用いた対策は攻撃できること、また、計算順序をシャッフルする対策は、サイドチャネル漏洩情報だけで攻撃できることを示した。最後の攻撃では大きな計算量を必要とするので、故障注入と組み合わせた受動・能動合併攻撃(PACA)を提案した。

1.7.3. CHES 2014 の発表(3 日目)

Efficient Power and Timing Side Channels for Physical Unclonable Functions [CHES 2014]
Ulrich Ruhrmair, Xiaolin Xu, Jan Solter, Ahmed Mahmoud, Mehrdad Majzoobi, Farinaz Koushanfar, Wayne Burleson
arbitar PUF に対して、初の電力とタイミングに着目した攻撃法を提案した。具体的な攻撃対象は、XOR Arbiter PUF と Lightweight PUF で、電力とタイミングによるサイドチャネル攻撃と機械学習を組み合わせることで、多項式時間の攻撃を実現した。

Side-Channel Leakage through Static Power ? Should We Care about in Practice? [CHES 2014]

Amir Moradi
FPGA 上の暗号実装に対し、暗号化の計算後の静的状態の電力消費から情報が漏洩していることを示す結果が報告された。実験は、レジスタのビットが全部 0 と全部 1 のときの漏洩電流を比較し、全部 1 のときの方が電流が大きくなることを示した。使用した FPGA はいずれも Xilix 製で、ボードと FPGA の組み合わせは次の通り。
- SASEBO-GII / FPGA as a Virtex-5 (65 nm)
- SAKURA-G / Target FPGA as a Spartan-6 (45 nm)
- SAKURA-X / Target FPGA as a Kintex-7 (28 nm)

1.8. Asiacrypt 2014 の発表

1.8.1. Asiacrypt 2014 の発表(1 日目)

Low Probability Differentials and the Cryptanalysis of Full-Round CLEFIA-128 [Asiacrypt 2014]
Sareh Emami, San Ling, Ivica Nikolić, Josef Pieprzyk, Huaxiong Wang
ブロック暗号の鍵スケジュールに対する差分確率は関連鍵差分解析に対する耐性の評価に使われ、k ビット鍵暗号に対する上限が 2^{-k} であれば十分であると考えられてきたが、CLEFIA-128 に対する関連鍵攻撃で反例が示された。ラウンド鍵を生成する鍵スケジュールの線型部分と Feistel 構造により、確率 2^{-128} の 2^{14} 個の特別に選択される差分を持ち、2^{14} ペアの弱鍵を持つ。ハッシュモードでは弱鍵ペアを 2^{122} 時間で発見することができ、一般の 2^{128} 時間よりも速く差分マルチ衝突を生成することができる。また、弱鍵クラスに属しているテストを従来の 2^{14} に対し、2^{8} の時間・データ計算量で行うことができる。攻撃の計算量は実用レベルではないため、CLEFIA-128 に対する現実的な脅威にはなってない。

Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon [Asiacrypt 2014]
Christina Boura, Maria Naya-Plasencia, Valentin Suder
不能差分攻撃を改良し、ブロック暗号 Camellia-128/192/256、CLEFIA-128、LBlock、SIMON 等に対し適用した結果が発表された。Camellia-128(11 段)の場合、時間計算量は $2^{118.43}$、データ計算量は $2^{118.4}$、メモリ計算量は $2^{92.4}$ と現実的な計算量ではない。CLEFIA-128(13 段)の場合は、使うテクニックにより各計算量は異なるが、やはり現実的な計算量ではない。ただし、いずれも従来の計算量よりも下がっている。

A Simplified Representation of AES [Asiacrypt 2014]
Henri Gilbert
ブロック暗号 AES のいわゆる超 S-box 表現を更に単純化し、安全性解析を行った結果が発表された。本手法により独立した属鍵を持つ 10 段 AES およびフル AES に対し、既知鍵識別者を構成すると、10 段 AES の場合、元の 8 段 AES と同じ時間計算量 2^{64} となるが、入力出力相関はより複雑になるため、ハッシュ関数構成に用いられた場合の安全性への影響は疑問の余地がある。また、暗号化やメッセージ認証に使われた場合の、安全性への影響はない。

GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA Signatures With Single-Bit Nonce Bias [Asiacrypt 2014]

Diego F. Aranha, Pierre-Alain Fouque, Benoit Gerard, Jean-Gabriel Kammerer, Mehdi Tibouchi, Jean-Christophe Zapalowicz

Gallant-Lambert-Vanstone(GLV)/Galbraith-Lin-Scott(GLS)らによるスカラー倍算高速化テクニックを用いた楕円曲線電子署名 ECDSA 実装に対する電力差分攻撃の発表。GLV/GLS は、k 倍を計算するときに、ほぼ半分のサイズの k_1、k_2 および高速な自己同型写像 ϕ により、$k=k_1+k_2\phi$ と分解することにより高速化を図る。ランダムスカラー倍を計算する際、k_1、k_2 を一様に取り、$k=k1+k_2\phi$ がほぼ一様であることを期待するか、k を一様にとった後、$k=k1+k_2\phi$ と分解するかの 2 つのアプローチがある。前者の場合、k の偏りを観測し、Bleichenbacher 攻撃と組み合わせることで ECDSA の完全鍵回復に成功した。後者の場合、統計的偏りは避けられるが、分解アルゴリズムがサイドチャネル情報を漏らす。電力解析により、テンプレート攻撃と格子縮小を組合せることにより、ECDSA の完全鍵回復が成功する。

1.8.2. Asiacrypt 2014 の発表(2 日目)

Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms - Simplified Setting for Small Characteristic Finite Fields [Asiacrypt 2014]

Antoine Joux, Cecile Pierrot

小標数の DLP 計算における事前計算の計算量を改良するアルゴリズムが発表された。q を基礎体の位数とすると、これまでは q^7 オーダーであった計算量が q^6 オーダーとなる。この改良により、事前計算の計算量は、一般の場合でも Kummer 拡大の場合と同程度の計算量となった。

Big Bias Hunting in Amazonia: Large-scale Computation and Exploitation of RC4 Biases [Asiacrypt 2014]

Kenneth G. Paterson

FSE2014 において Paterson らにより発表された、ストリーム暗号 RC4 の鍵ストリームに存在する偏りを利用した WPA/TKIP に対する平文解読攻撃を、Amazon EC2 を用いた大規模計算により精度を高め、改良した攻撃に適用した結果が発表された。63 仮想コア年の計算量を 4 万 3 千 US ドルで使用し、2 種類の計算を行ったが、RSA-768 の素因数分解篩処理の約 12 分の 1 の計算量に相当する。

Multi-user collisions: Applications to Discrete Logarithm, Even-Mansour and PRINCE [Asiacrypt 2014]

Pierre-Alain Fouque, Antoine Joux, Chrysanthi Mavromati

マルチユーザー環境における DLP の困難性は、シングルユーザー環境における困難性を単純にユーザー数倍したものになるとは限らないことを発表した。1 つ目のアイディアは、複数鍵の相関関係をグラフで表し、互いに連結された鍵の内一つが求まれば他のすべての鍵も求まる性質を利用するものであり、もう一つのアイディアは、van Oorschot-Wiener のアイディアを改良したものである。これらのテクニックを単独もしくは組み合わせて、DLP、Even-Mansour 関数、ブロック暗号 PRINCE の解析に適用した。一つめのアイディア DLP に適

用した場合、サイズ N の群、L ユーザーの DLP の鍵は、$\tilde{O}(\sqrt{NL})$オーダーで求まることが示された。鍵交換プロトコル Diffie-Hellmann や電子署名 DSA が関係するが、現状ではシングルユーザー環境でも十分な困難性を有するため、緊急の問題とはならない。

Meet-in-the-Middle Attacks on Generic Feistel Constructions [Asiacrypt 2014]
Jian Guo, Jeremy Jean, Ivica Nikolić, Yu Sasaki
一般的なバランス型 Feistel 暗号に対する鍵回復攻撃が発表された。中間一致の手法による解析で、Feistel 構造に存在する trucated 差分を発見し、攻撃に利用している。ラウンド関数の種類により攻撃を分けており、Feistel-2 タイプおよび Feistel-3 に対し各々結果を示している。Feistel-2 タイプでは、鍵長を k、ブロック長を n としたとき、k=n の場合 6 段を $2^{3n/4}$ の計算量で、k=2n の場合 10 段を $2^{11n/6}$ の計算量で攻撃可能である。Feistel-3 タイプでは、S-box 長を c としたとき、k=n の場合 10 段を $2^{n/2+4c}$ の計算量で、k=2n の場合 14 段を $2^{3n/2+4c}$ の計算量で攻撃可能である。

1.8.3. Asiacrypt 2014 の発表(4 日目)

Side-Channel Analysis of Multiplications in GF(2^{128}): Application to AES-GCM [Asiacrypt 2014]
Sonia Belaid, Pierre-Alain Fouque, Benoit Gerard
体 GF(2^n)の乗算に関するサイドチャネルセキュリティおよび AES-GCM への適用に関する結果が発表された。AES-GCM に適用するため、特に GF(2^{128})に焦点を当てているが、他の拡大次数の場合にもあてはまる。128 ビット乗算器を用いたハードウェア実装において、128 ビットの秘密は一度に扱われるため、分割統治戦略による従来の DPA 攻撃は適用できない。本研究では、乗算の代数的構造を利用し、鍵推測をすることなしに、秘密の被乗数のビットに関する情報を引き出す。乗算結果をレジスタに書き出すことに対応する漏洩を考慮し、ハミング重み/距離漏洩モデルに従うことを仮定する。鍵回復の問題と LPN(Learning Parities with Noise)問題とを関連づけ、特別な場合には、AES-GCM への攻撃は認証鍵の知識を与えることを示した。

1.9. FSE 2015 の発表

1.9.1. FSE 2015 の発表(1 日目)

Differential Analysis and Meet-in-the-Middle Attack against Round-Reduced TWINE [FSE 2015]
Alex Biryukov, Patrick Derbez, Leo Perrin
TWINE は SAC 2013 で発表された軽量の 64 ビット・ブロック暗号で、鍵長は 64 ビットと 128 ビットの２種類が利用でき、ともに 36 段である。本論文では、TWINE の一般化 Feistel 構造を等価変形することで、認証暗号の公募選考プロジェクト CAESAR の候補である LBlock と 4 段が同じ振る舞いをすることに着目し、中間一致攻撃、不能差分攻撃、truncated 差分攻撃を適用した。その結果、128 ビット鍵の 25 段縮小版に対し、従来より計算量は増えるものの、少ないデータ量で済む攻撃を示した。

攻撃法	データ量	時間	メモリ量
ゼロ相関線形解読法(Wang & Wu, ACISP 2014)	$2^{62.11}$	$2^{122.12}$	2^{60}
中間一致攻撃(本論文)	2^{48}	$2^{124.7}$	2^{109}
不能差分攻撃(本論文)	$2^{59.1}$	$2^{124.5}$	$2^{78.1}$

Improved Higher-Order Differential Attacks on MISTY1 [FSE 2015]

Achiya Bar-On

電子政府推奨暗号 MISTY1 は 64 ビット・ブロック暗号であり、8 段及び FL 関数 5 個で構成される。従来の最良の攻撃は、2012 年に角尾らが示した 7 段と FL 関数 4 個に対する高階差分攻撃だった。本論文では、角尾らと同じ縮小版に対して計算時間を 2^{-16} に短縮したものと、7 段と FL 関数 5 個に対する初の攻撃を示した。

攻撃法	段数	FL 関数	データ量	時間
高階差分攻撃(角尾ら, 2012)	7	4	$2^{49.7}$	$2^{116.4}$
高階差分攻撃(本論文)	7	4	$2^{50.1}$	$2^{100.4}$
高階差分攻撃(本論文)	7	5	$2^{51.45}$	2^{121}

Meet-in-the-Middle Technique for Truncated Differential and its Applications to CLEFIA and Camellia [FSE 2015]

Leibo Li, Keting Jia, Xiaoyun Wang, Xiaoyang Dong

中間一致攻撃に似た手法を使って、ブロック暗号の truncated 差分経路を構成する方法を開発し、CRYPTREC 暗号の CLEFIA と Camellia に適用した、その結果、CLEFIA-128 の攻撃可能段数を従来の 13 段から 14 段に拡張した他、攻撃可能段数は同じながら、必要データ量を削減するなどの改良を実現した。新規の結果を次表に示す。

暗号名	攻撃段数	仕様段数	データ量	時間	メモリ量
CLEFIA-128	13	18	2^{99}	2^{99}	2^{80}
CLEFIA-128	14	18	2^{100}	2^{108}	$2^{101.3}$
CLEFIA-192	14	22	2^{100}	2^{135}	2^{131}
CLEFIA-256	15	26	2^{100}	2^{203}	2^{139}
Camellia-128	11	18	2^{117}	$2^{119.3}$	2^{119}
Camellia-128	11	18	2^{117}	$2^{121.3}$	2^{119}
Camellia-192	11	24	2^{117}	$2^{183.3}$	2^{119}
Camellia-192	11	24	2^{117}	$2^{185.3}$	2^{119}

Relations between Impossible, Integral and Zero-Correlation Key-Recovery Attacks [FSE 2015]

Celine Blondeau, Marine Minier

Type-II Feistel 型暗号に、段関数の行列表現を適用することによって、不能差分攻撃とゼロ相関攻撃に対し、distiguisher 発見に利用できることを示した。また、鍵回復攻撃において、ゼロ相関攻撃のキーワードが、不能差分攻撃におけるキーワードの部分集合になることを示した。この議論を利用して、23 段縮小 LBlock に対して、時間複雑度が従来より小さい新規の攻撃を実現した。

Meet-in-the-Middle Attacks and Structural Analysis of Round-Reduced PRINCE [FSE 2015]

Patrick Derbez, Leo Perrin

ブロック暗号 PRINCE に対し、複雑度が次表となる中間一致攻撃を示した。

攻撃段数	データ量	時間	メモリ量
6	2^{16}	$2^{33.7}$	$2^{31.9}$
8	2^{16}	$2^{50.7}$	$2^{84.9}$
8	2^{16}	$2^{65.7}$	$2^{68.9}$
10	2^{57}	2^{68}	2^{41}

さらに、差分解読法を SAT Solver と組み合わせることにより、次表の攻撃が可能であることを示した。

攻撃段数	データ量	時間	メモリ量
4	2^{10}	5 sec	$<<2^{27}$
6	$2^{14.9}$	$2^{32.9}$	$<<2^{27}$

これらの研究成果は NXP Semiconductors 他によるチャレンジへ応募されたものであり、論文の著者らは 6 段及び 8 段の部門の優勝者となった。

1.9.2. FSE 2015 の発表(2 日目)

Differential-Linear Cryptanalysis of ICEPOLE [FSE 2015]

Tao Huang, Ivan Tjuawinata, Hongjun Wu

ICEPOLE は認証暗号の公募選考プロジェクト CAESAR の候補方式で、Keccak と類似の置換(permutation)を使用し、ハードウェア向けに設計されている。本論文では、nonce を誤使用したときに、ICEPOLE の状態復元に必要なデータ複雑度と時間複雑度が次表の通りとなる攻撃が可能であることを示した。

暗号名	データ量	時間
ICEPOLE-128	2^{46}	2^{46}
ICEPOLE-128a	2^{46}	2^{46}
ICEPOLE-256a	2^{60}	2^{60}

一旦、状態が復元できると、秘密鍵はそれから求めることが可能であり、ICEPOLE-128 と ICEPOLE-128a では、数値実験によって有効性を確認した。

Cryptanalysis of JAMBU [FSE 2015]

Thomas Peyrin, Siang Meng Sim, Lei Wang, Guoyan Zhang

ICEPOLE は認証暗号の公募選考プロジェクト CAESAR の候補方式である。本論文では、設計者が主張する nonce の誤使用時の安全性が満たされないことを示した。具体的には、与えられた平文に対する暗号文ブロックを予想するのに、2^{32} 回の暗号文呼び出しと 2^{32} 回分の計算で済むというものであり、この攻撃は実際に実装することで有効性が確認されている。

Related-Key Forgeries for Proest-OTR [FSE 2015]

Christoph Dobraunig, Maria Eichlseder, Florian Mendel

Proest は認証暗号の公募選考プロジェクト CAESAR の候補方式で、設計者によると高い安全性と実装性能を持つ置換である。具体的な認証暗号は、Proest と３種類の既存認証暗号モード COPA、OTR、APE との組み合わせで構成される。本論文では、Proest-OTR について、関連鍵攻撃が可能な条件下で、偽造攻撃が可能であることを示した。

Practical Cryptanalysis of the Open Smart Grid Protocol [FSE 2015]

Philipp Jovanovic, Samuel Neves

Open Smart Grid Protocol(OSGP)は、スマートグリッド用の通信プロトコルとして世界中で 400 万台の機器で利用されている。Energy Service Network Alliance (ESNA) が 2010 年頃開発し、ETSI(欧州電気通信標準化機構)が 2012 年に標準化している。この方式で利用されている認証暗号方式では、RC4 を利用した他の標準にない自製の OMA digest と呼ばれるものが、使用されている。

本論文では、13 回の OMA digest 呼び出しと無視できる程度の計算量、または、4 回の呼び出しと 2^{25} 回の簡単な計算で鍵を復元できることが示された。著者らは 2014 年 11 月に OSGP Alliance にこの安全性に関する欠陥を報告したところ、感謝の意を示されたものの、暗号文単独攻撃だけが現実的であり、OMA digest 呼び出しは非現実的とし、特に対応は取られていないということである。

1.9.3. FSE 2015 の発表(3 日目)

GCM Security Bounds Reconsidered [FSE 2015, BEST PAPER]

Yuichi Niwa, Keisuke Ohashi, Kazuhiko Minematsu, Tetsu Iwata

GCM の衝突確率の上限は $2^{22}/2^{128}$ 以下であることは証明されているが、この上限に近い確率を実現する具体的な nonce の作り方は示されていなかった。本発表では、GCM の衝突確率を $2^{20.75}/2^{128}$ にする nonce の具体例を作成するとともに、nonce を適切に選ぶことにより、衝突確率は $32/2^{128}$ 以下になることを証明した。後者の結果は、GCM のオリジナルな安全主張に近いことを示す肯定的な結果である。

付録 4

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 27 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

更新履歴

更新日時	主な更新内容
平成 26 年 3 月	初版.
平成 27 年 3 月	3.2 節に POODLE 攻撃に関する解説を挿入.

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、POODLE、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。

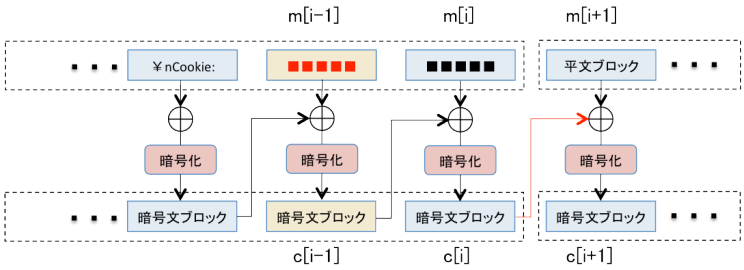


図 1　SSL3.0/TLS1.0 における CBC の概要

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]

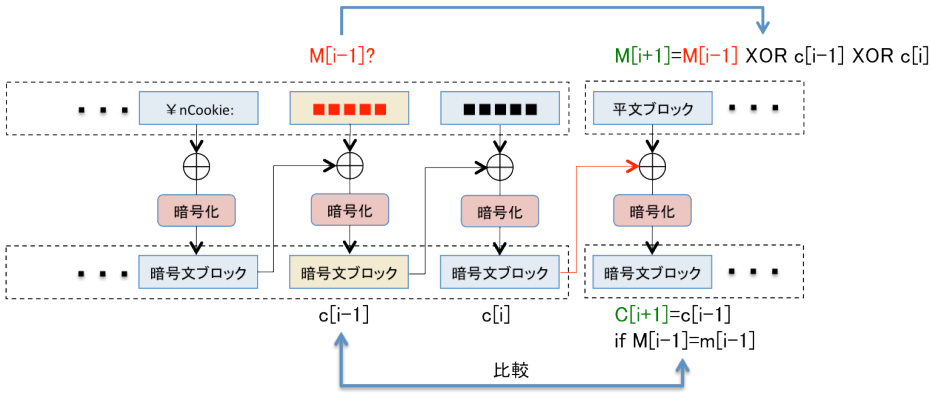


図 2　SSL3.0/TLS1.0 への平文選択攻撃

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。

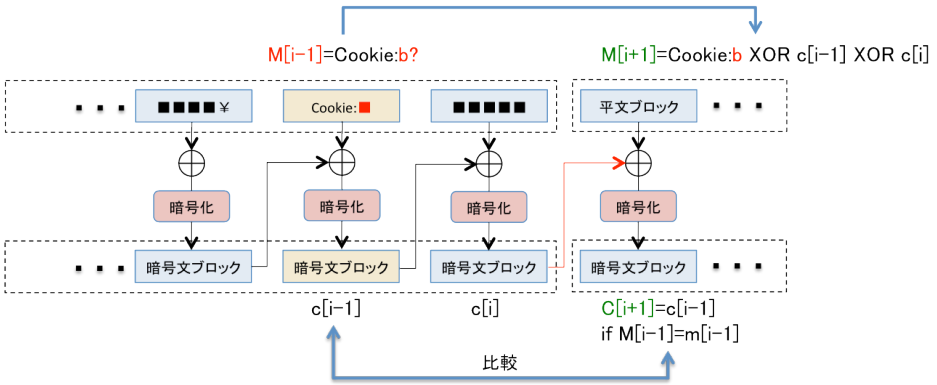


図 3　BEAST におけるバイト単位の平文選択攻撃

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。

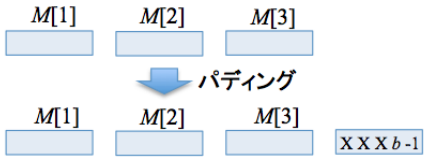
3.2 SSL3.0 における CBC モードの構成を利用した攻撃：POODLE

POODLE [6]は 2014 年に発見された比較的新しい、SSL3.0 における CBC モードに対する攻撃である。本攻撃は、Vaudenay により 2002 年に提案されたパディングオラクル攻撃の実装の一例と見なすことができる［7]。ここでは POODLE 攻撃の仕組みを概観する。

簡単のため、暗号化する平文 M の長さ n バイトがブロック長 b バイトで割り切れる場合を考える。また、平文 M の i ブロック目を $M[i]$ と記述する。すなわち、$M = M[1], M[2], \cdots, M[n/b]$ であり、各 i について $M[i]$ は b バイトである。AES の場合は、b は 16 バイト、Triple DES の場合は、8 バイトである。平文 M は、暗号化に先立ち、パディングとして $M[n/b+1]$ が最終ブロックに付与される。ここで b バイトである $M[n/b+1]$ の内訳は、下記の通りである。

- 1～b － 1 バイト目は任意の値
- b バイト目は b － 1

これを図示すると下のようになる。



従って、最終ブロックには、平文に関する情報が含まれない。

b バイトの文字列 X の最終バイト、すなわち b バイト目を LB(X) と記述する。従って、LB($M[n/b+1]$)= b － 1 である。パディングされた平文 $M = M[1], \cdots, M[n/b+1]$ に関す

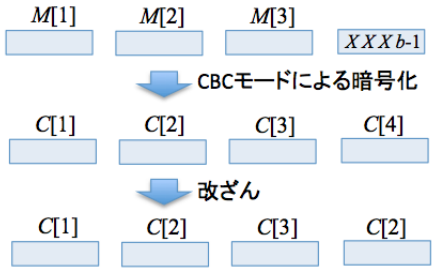
る暗号文 C [1], …, C [n/b+1]を受信する受信者は、CBC モードで復号した後に、下記のようにパディングの検査を行うものとする。

- LB(M [n/b+1]) = b − 1 の場合は、正常な暗号文、
- LB(M [n/b+1]) ≠ b − 1 の場合は、不正な暗号文とする。

攻撃者がこれら二つの検査結果の違いを観測でき、また、送信者と受信者の通信経路上に位置している場合、下記のような中間者攻撃を行うことにより、任意の i について LB(M[i])を復元可能である。

- 暗号文 C = C [1], …, C [n/b+1]を受信した攻撃者は、暗号文 C を C’ = C [1], …, C [n/b], C[i]に改ざんした上で、受信者に送信する。
- 受信者が正常な暗号文と判定した場合、LB(M [i]) として b − 1 + LB(C [i − 1] + C [n/b]) を出力する。 尚、+は排他的論理和である。

改ざん方法を図示すると下のようになる。



尚、この例では、攻撃者は LB(M[2])の復元を試みている。

受信者が改ざんされた C’ を正常な暗号文と判定した場合に、LB(M [i]) = b - 1 + LB(C [i − 1] + C [n/b]) となる理由は、CBC モードの構造にある。C[i]をブロック暗号の復号アルゴリズムに入力した場合、出力値は C [i − 1]+M [i]であるから、CBC モードにより復号したバイト列の最終ブロックは C [i − 1]+M [i] + C [n/b]である。受信者が正常であると判定した場合、

$$\mathrm{LB}(C\,[i-1]+M\,[i]+C\,[n/b]) = b-1$$

であるから、LB(M [i]) = b − 1 + LB(C [i − 1] + C [n/b])を満たすことになる。

上記の攻撃と JavaScript などのブラウザ上で動作する言語を組み合わせるにより、１バイトだけではなく複数バイトの復元も可能となる。尚、１バイトの復元に成功する確率は概ね 1/256 である。

3.3 圧縮処理部分の観測に基づく攻撃

3.3.1　CRIME

CRIME（Compression Ratio Info-Leak Mass Exploitation） [8] 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。

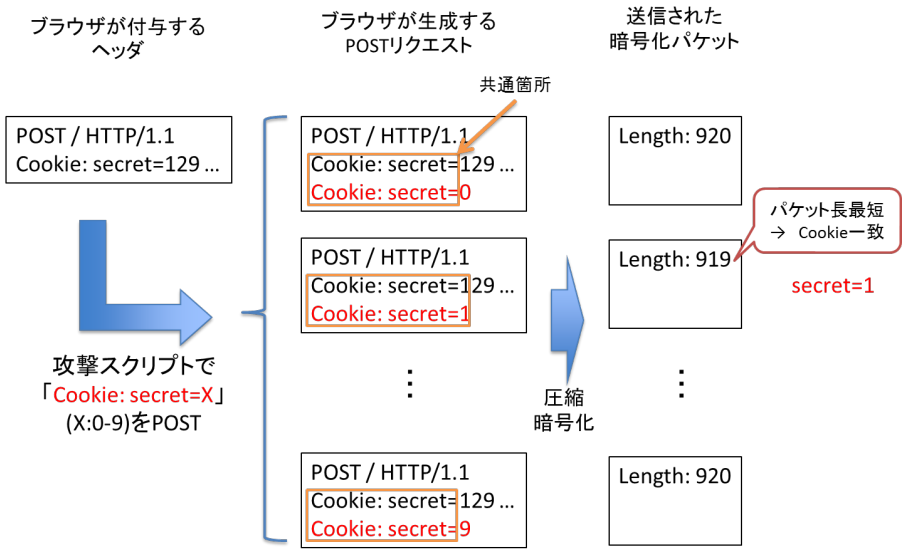


図 4 CRIME の攻撃の流れ

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。

3.3.2 TIME

TIME（Time Info-leak Made Easy） [9] 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。

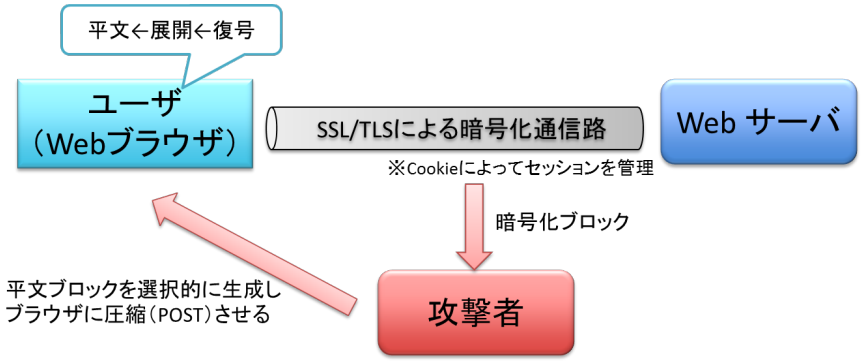


図 5 TIME の攻撃の流れ

3.3.3 BREACH

BREACH [10] 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。

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

Lucky Thirteen [11] 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。

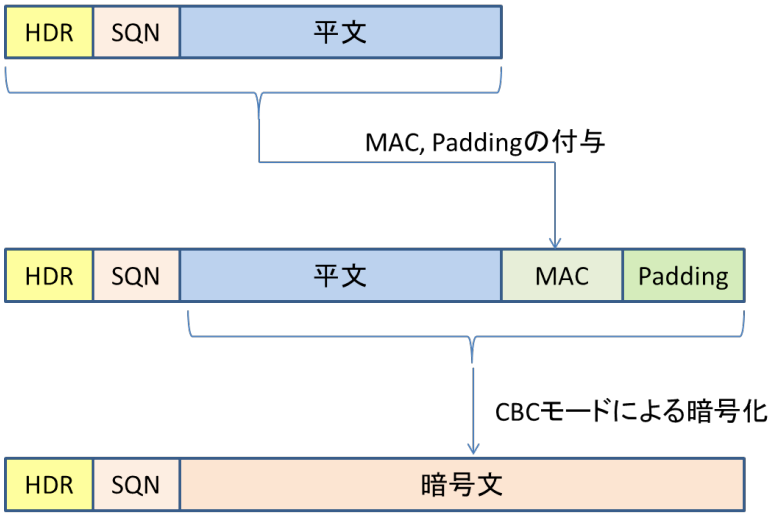


図 6　TLS における MEE-CBC-TLS の概要

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。

3.5 Renegotiation を利用した攻撃

3.5.1 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 [12]。

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。

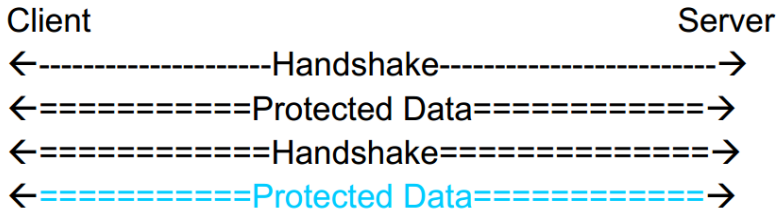


図 7 Renegotiation の概要（[13]より引用）

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

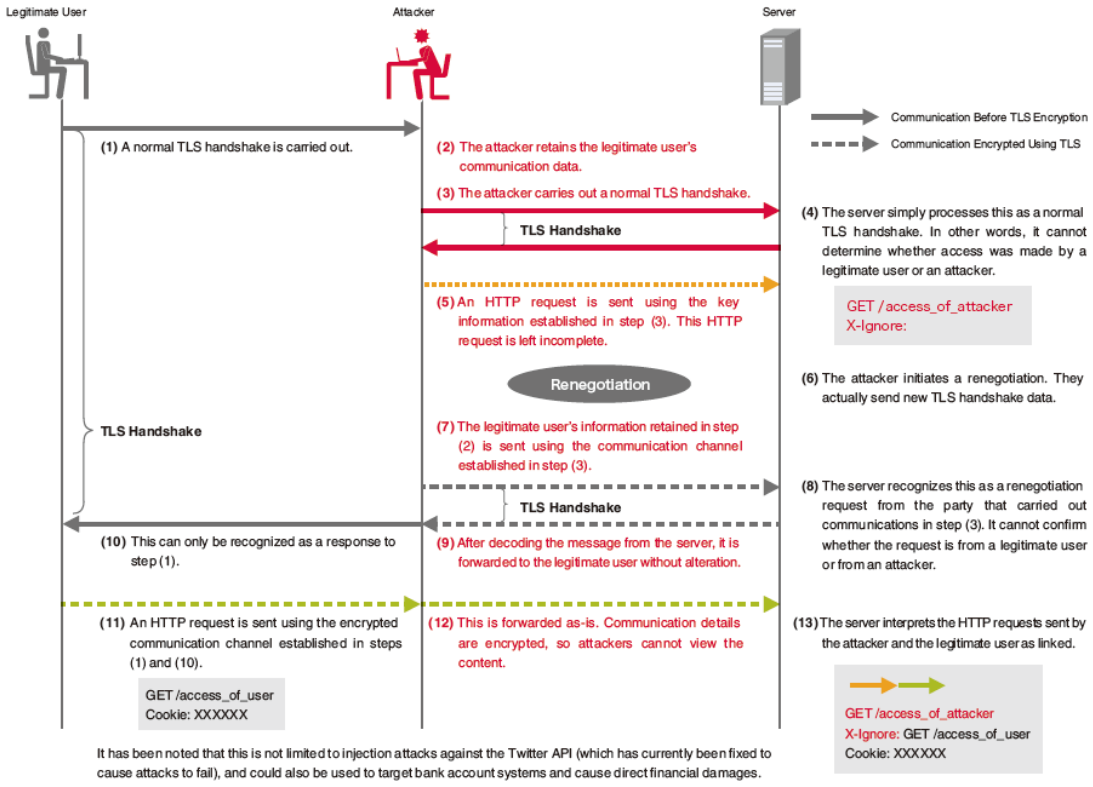


図 8 Renegotiation 攻撃の概要（[14]より引用）

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。

3.5.2 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 [15] [16] [17] 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。

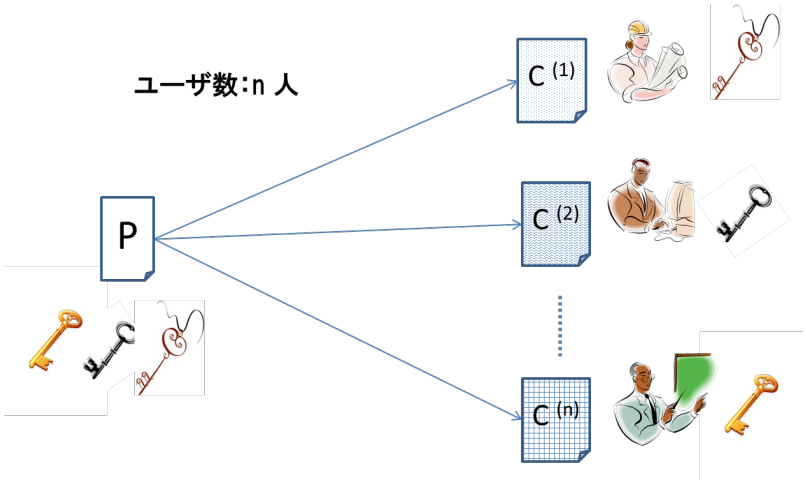


図 9 Broadcast Setting

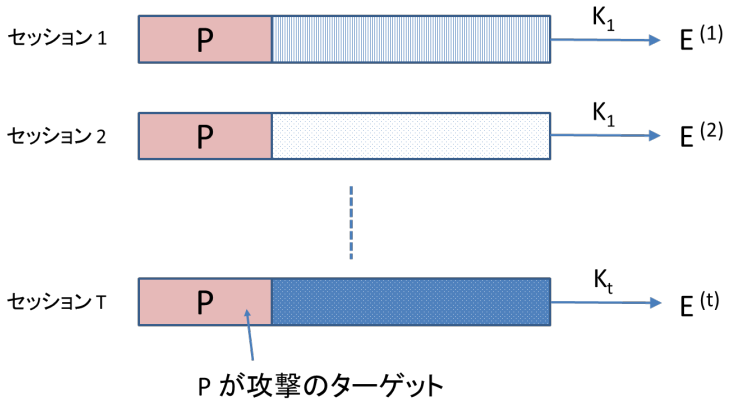


図 10 Multi-Session Setting

近年の結果として [1] [18] 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 [19]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、 [20] 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] [18]。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] [18] 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 [21] 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、 [22] 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。

(尚、ご所属は初版発行時のものになります。)

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] B. Möller, T. Duong , K. Kotowicz, “This POODLE Bites: Exploiting The SSL 3.0 Fallback,”: https://www.openssl.org/~bodo/ssl-poodle.pdf.

[7] S. Vaudenay, “Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS,” Eurocrypt 2002.

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

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

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

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

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

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

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

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

[16] 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.

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

[18] 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 (CCS2014)

[19] 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.

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

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

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

付録 5

格子問題等の困難性に関する調査

暗号技術調査 (暗号解析評価) ワーキンググループ

2015 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.「暗号技術調査ワーキンググループ (暗号解析評価)」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 委員構成

2013 年度及び 2014 年度における「暗号技術調査ワーキンググループ (暗号解析評価)」の委員構成は表 1.1 の通りである.

表 1.1 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 (2013–2014 年度)

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[*1]	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 ソーシャルイノベーション研究所 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 ソーシャルイノベーション研究所 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表 1.2 の通りである.

[*1] 2013 年度まで

表 1.2　章構成と執筆分担

章	担当	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[*1]	一般的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.

第 2 章　格子に関する研究は非常に多岐にわたるため, 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. SVP (Shortest Vector Problem) は, 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問題であり, パラメータを適切に取れば, 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. 実際の計算機環境における解析に関しては, 計算機実験 (SVP Challenge, Lattice Challenge, Ideal Lattice Challenge) が良く知られており, 日本の研究者らの実験結果も記録されてきている.

第 3 章　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 (the decision version of the shortest vector problem) 及び SIVP (the shortest independent vectors problem) 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, パラメータを適切に取れば, 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 4 章　LPN 問題は機械学習理論や符号理論から派生した問題であり, 誤り確率が十分大きい場合の LPN 問題を多項式時間で効率的に解くことは困難であると予想されている. 共通鍵や公開鍵の分野で多くの方式が LPN 問題に基づいて提案されている. LWE 問題と比較した場合, 利点としては, ハードウェア構成との相性が良い点や誤差のサンプリングが容易である点が挙げられる. 一方, 欠点として, 鍵や暗号文のサイズが大きくなりやすい点や発展的な応用が少ない点が挙げられる. 暗号方式のパラメータ設定の際には, 4.2 節で挙げたさまざまなアルゴリズムを考慮する必要がある. アルゴリズムの高速化について盛んに研究されており, 動向を注視する必要がある.

また, 攻撃に用いられるアルゴリズムの研究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 5 章 ACD 問題は, 2001 年に Howgrave-Graham により導入された問題であり, パラメータを適切に選ぶことにより, 効率的に解くことが困難であると予想されている. ACD 問題は, 複数 ACD 問題や GACD 問題など, いくつかの拡張問題をもつ. 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には, 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. 組み合わせ論に基づくアルゴリズムを用いた場合では, 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. 格子理論に基づくアルゴリズムを用いた場合では, 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, 十分大きいときには, 解くことができない. ACD 問題を安全性の根拠としてもつ, 完全準同型暗号方式が提案されている. 適切にパラメー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るが, 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.

1.3 更新履歴

表 1.3 更新履歴

更新日時	主な更新内容
2013 年度	•初版.
2014 年度	•2.1.3 節. 計算機実験に関する記録の更新. •3.1.3 節の追加. •3.2.2 節の最後.「■近年の攻撃研究の動向」の追加. •4.2 節. 代表的な暗号方式を追加 (旧 4.3-4.5 節から移動した文書有り). •4.3 節 (旧 4.2 節). いくつかコメントを追加. •5.1.3 節. 5.1.3.1 節及び 5.1.3.2 節の追加. •5.1.4 節の追加. •5.5 節の追加.

第 2 章

一般的な攻撃に関する総論

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.

2.1 準備

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 $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n), i \in \{1, 2, \ldots, n\}$ 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.

2.2 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.

2.3 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 [Ajt98]. 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[Micci98] 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 [Kho05, Kho10]. 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[LLL82], BKZ[Sch87] アルゴリズムがある. LLL アルゴリズムは, Lenstra, Lenstra, Lovász 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

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

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 $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ 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 $O(n^4 \log(\max_{1 \leq i \leq n} ||\boldsymbol{b}_i||^2))$ となる. また, 出力される基底の第一ベクトルのノルムは $||\boldsymbol{b}_1|| \leq (\frac{2}{\sqrt{3}})^n \lambda_1$ となることが証明されている [LLL82]. 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 Schnorr 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 $\mathrm{B} = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n)$ とし，$\beta \in [2, n]$ とする. 格子 B が LLL 簡約基底であり, かつ $1 \leq j \leq n$ 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 $\mathrm{B}' = (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_i, \boldsymbol{b}, \boldsymbol{b}_{i+1}, \ldots, \boldsymbol{b}_n)$ 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, AN12] 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 [Sch03, BL06].

■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 [LLL82], BKZ アルゴリズム [Sch87], L^2 アルゴリズム [NV05, NV06], BKZ2.0[GNR10, AN12] 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, $\boldsymbol{v} = \sum_{1 \leq i \leq n} u_i \boldsymbol{b}_i$ 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 [Sch94], 更に探索範囲を削減する枝刈り列挙 ([SH95, GNR10, MV09]) 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 [GNR10]. 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 [SchPD11].

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 [MV10]. ボロノイセルアルゴリズムは決定的アル

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 [Sch94]
Extream Pruning Enumeration	$2^{O(n)}$	$O(n)$	文献 [GNR10]

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 [AKS01]
AKS Sieve without perturbation	$O(2^{0.41n})$	$O(2^{0.21n})$	文献 [NS08]
List Sieve	$O(2^{3.199n})$	$O(2^{1.325n})$	文献 [MV10]
Gauss Sieve	$O(2^{0.52n})$	$O(2^{0.21n})$	文献 [MV10]
List Sieve Birthday	$O(2^{2.465n})$	$O(2^{1.233n})$	文献 [PS09]
NV Sieve	$O(2^{0.3836n})$	$O(2^{0.2557n})$	文献 [NS08, WLTB10]

ゴリズムであり, $2^{O(n)}$ 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を利用した実装例は知られていない.

篩アルゴリズムは SVP を解く確率的アルゴリズムである. 2001 年に Ajtai 等によって AKS Sieve[AKS01] 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 [NS08, BN07, AJ08, MV10, PS09, WLTB10]. 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, 理論上最も高速な篩アルゴリズムは 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.

2.4 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, ダルムシュタット工科大学によって 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[SVPC] 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[LC] 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[ILC] 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 [HPS98, GGH12, Gen09] 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 [Pla13] 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 [GNR10], あるいはその改良方式 [CN11, AN12] 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 2.4 に示す. SVP Challenge の結果として Kashiwabara らの RSR アルゴリズムの改良手法 [Kashi13], BKZ2.0[GNR10] 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などである [Kashi13]. 彼らの手法は,

表 2.3　q-ary lattice に対する Approx-SVP の求解 (Lattice Challenge[LC])

	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	
Aono, Naganuma	825	122.38	BKZ2.0 の改良	2012-10	文献 [AN12]
Chen, Nguyen	800	106.60	BKZ2.0	2013-3	文献 [CN11]
Aono, Naganuma	800	117.69	BKZ2.0 の改良	2012-10	文献 [AN12]
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 [AN12]
Chen, Nguyen	750	87.76	BKZ2.0	2013-3	文献 [CN11]
Chen, Nguyen	725	80.65	BKZ2.0	2013-3	文献 [CN11]
Aono, Naganuma	725	83.61	BKZ2.0 の改良	2012-9	文献 [AN12]
Chen, Nguyen	700	72.46	BKZ2.0	2013-3	文献 [CN11]
Aono, Naganuma	700	76.17	BKZ2.0 の改良	2012-9	文献 [AN12]

表 2.4　SVP の求解 (SVP Challenge[SVPC])

	次元	ノルム	アルゴリズム	時期	文献
Kashiwabara, Teruya	140	3025	RSR アルゴリズムの改良	2015-1	
Kashiwabara, Teruya	138	3077	RSR アルゴリズムの改良	2014-12	
Kashiwabara, Teruya	134	2976	RSR アルゴリズムの改良	2014-7	文献 [Kashi14]
Kashiwabara, Fukase	132	3012	RSR アルゴリズムの改良	2014-4	文献 [Kashi14]
Aono, Nguyen	130	2883	BKZ2.0 + Randomized ENUM	2014-10	
Kashiwabara, Fukase	130	3025	RSR アルゴリズムの改良	2013-11	文献 [Kashi13]
Kashiwabara, Fukase	128	2984	RSR アルゴリズムの改良	2013-9	文献 [Kashi13]
Aono, Nguyen	126	2855	BKZ2.0 + Extreme pruning	2014-9	
Kashiwabara, Teruya	126	2897	RSR アルゴリズムの改良	2014-8	
Aono	126	2906	BKZ2.0 + Extreme pruning	2014-7	
Kashiwabara, Fukase	126	2944	RSR アルゴリズムの改良	2013-9	文献 [Kashi13]
Chen, Nguyen	126	2969	BKZ2.0 + Randomized ENUM	2013-4	文献 [CN11]
Chen, Nguyen	124	2884	BKZ2.0 + Randomized ENUM	2013-3	文献 [CN11]
Chen, Nguyen	122	2913	BKZ2.0 + Randomized ENUM	2013-3	文献 [CN11]
Kashiwabara, Fukase	120	2756	BKZ2.0 の改良	2013-3	文献 [AN12]
Aono, Naganuma	120	2830	BKZ2.0 の改良	2013-9	文献 [Kashi13]

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.

Ideal Lattice に対する実験結果を表 2.5–2.6 に表す. Ideal Lattice Challenge においては 128 次元の SVP が解かれている [IKMT13]. 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

表 2.5 Ideal-SVP(< 1.05 Gaussian heuristic) の求解 (Ideal Lattice Challenge[ILC])

	次元	ノルム	アルゴリズム	時期	文献
Ishiguro, Kiyomoto, Miyake, Takagi	128	2959	Gauss Sieve の改良	2013-4	文献 [IKMT13]
Ishiguro, Kiyomoto, Miyake, Takagi	108	2669	Gauss Sieve の改良	2013-4	文献 [IKMT13]

表 2.6 Approx-SVP($n \det^{1/n}$) の求解 (Ideal Lattice Challenge[ILC])

	次元	ノルム	アルゴリズム	時期	文献
Wang, Aono, Hayashi, Takagi	500	507596	Progressive BKZ	2015-1	文献 [WAHT15]

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

[Ajt98] 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, pp. 10–19. ACM, 1998.

[AD97] 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, pp. 284–293. ACM, 1997.

[AKS01] M. Ajtai, R. Kumar and D. Sivakumar, “A Sieve Algorithm for the Shortest Lattice Vector Problem,” In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, STOC 2001, pp. 601–610. ACM, 2001.

[AN12] 青野 良範, 長沼 健 “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.

[AJ08] 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*, pp. 25–36. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2008.

[BN07] J. Blömer and S. Naewe, “Sampling Methods for Shortest Vectors, Closest Vectors and Successive Minima,” *Journal of Theoretical Computer Science*, volume 410, issue 18, pp. 1648–1665, 2009.

[CN11] 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, Springer LNCS 7073, pp. 1-20, 2011.

[FK15] M. Fukase and K. Kashiwabara, “An Accelerated Algorithm for Solving SVP Based on Statistical Analysis,” Journal of Information Processing Vol.23 No.1 pp. 67-80, 2015.

[GGH12] S. Garg, C. Gentry and S. Halevi, “Candidate Multilinear Maps from Ideal Lattices,” Cryptology ePrint Archive, Report 2012/610, 2012.

[GNR10] 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, Springer LNCS 6110, pp. 257–278, 2010.

[Gen09] C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices,” In *Proc of the 41st Annual ACM Symposium on Theory of Computing*, STOC 2009, pp. 169–178. ACM, 2009.

[HPS98] J. Hoffstein, J. Pipher and J. Silverman, “NTRU: A Ring-based Public Key Cryptosystem,” In *Algorithmic Number Theory*, Springer LNCS 1423, pp. 267–288, 1998.

[LLL82] A. Lenstra, H. Lenstra and L. Lovász, “Factoring Polynomials with Rational Coefficients,” *Mathema-*

tische Annalen, volume 261, issue 4, pp. 515–534, 1982.

[BL06] J. Buchmann and C. Ludwig, "Practical Lattice Basis Sampling Reduction," In *Proceedings of the 7th International Symposium*, ANTS-VII, Springer LNCS 4076, pp. 222–237, 2006.

[IKMT13] 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.

[Kashi13] 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`.

[Kashi14] K. Kashiwabara, "A fast algorithm for the shortest vector problem," Workshop "Post-Quantum Cryptography: Recent Results and Trends," November 2014. `http://www.isit.or.jp/lab2/2014/10/20/pqworkshop-2/`

[Kho05] S. Khot, "Hardness of Approximating the Shortest Vector Problem in Lattices," *Journal of the ACM*, Vol. 52, No. 5, pp. 789–808, Springer, 2005.

[Kho10] S. Khot, "Inapproximability Results for Computational Problems on Lattices," *The LLL Algorithm–Survey and Applications*, pp. 453–473, Springer, 2010.

[Micci98] 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, pp. 92–98. IEEE Computer Society, 1998.

[MV10] 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 2010, pp. 351–358. ACM, 2010.

[MV09] 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 2010, volume 65, pp. 1468–1480. SIAM, 2010.

[NV05] P. Q. Nguyen and T. Vidick, "Floating-point LLL Revisited," In *Proceedings of the 24th Annual Eurocrypt Conference*, Springer LNCS 3495, pp. 215–233, 2005.

[NV06] P. Q. Nguyen and T. Vidick, "LLL on the Average," In *Proceedings of the 7th International Symposium*, ANTS-VII, Springer LNCS 4076, pp. 238–256, 2006.

[NS08] P. Q. Nguyen and D. Stehlé, "Sieve Algorithms for the Shortest Vector Problem Are Practical," *Journal of Mathematical Cryptology*, volume 2, pp. 181–207, 2008.

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

[Pla13] T. Plantard and M. Schneider, "Creating a Challenge for Ideal Lattices," Cryptology ePrint Archive, Report 2013/039, 2013.

[PS09] X. Pujol and D. Stehlé, "Solving the Shortest Lattice Vector Problem in Time $2^{2.465n}$," Cryptology ePrint Archive, Report 2009/605, 2009.

[SchPD11] M. Schneider, "Computing Shortest Lattice Vectors on Special Hardware," PhD thesis, Technische Universität Darmstadt, 2011.

[ScheP11] M. Schneider, "Sieving for Shortest Vectors in Ideal Lattices," Cryptology ePrint Archive, Report

2011/458, 2011.

[LC] R. Lindner, M. Rueckert, P. Baumann and L. Nobach, Lattice Challenge, `http://www.latticechallenge.org/`.

[SVPC] M. Schneider and N. Gama, The SVP Challenge, `http://www.latticechallenge.org/svp-challenge/`.

[Sch87] C.-P. Schnorr, "A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms," *Journal of Theoretical Computer Science*, volume 53, issue 2-3, pp. 201–224, 1987.

[Sch94] C.-P. Schnorr, "Lattice Basis Reduction: Improved Practical Algorithms and Solving Subset Sum Problems," *Journal of Mathematical programming*, pp. 181–191. Springer, 1993.

[SH95] C.-P. Schnorr and H. H. Horner, "Attacking the Chor-Rivest Cryptosystem by Improved Lattice Reduction," In *Proceedings of the 14th annual international conference on Theory and application of cryptographic techniques*, Eurocrypt'95, Springer LNCS 921, pp. 1–12, 1995.

[Sch03] 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 2003, Springer LNCS 2607, pp. 145–156. 2003.

[WLTB10] 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.

[WAHT15] Y. Wang, Y. Aono, T. Hayashi and T. Takagi, "A New Progressive BKZ Algorithm," SCIS2015, 3E3-5, 2015.

第 3 章

LWE

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. 本章では, 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の調査結果を述べる (本章をまとめるにあたり, 文献 [Reg] を主に参考にした).

3.1 LWE の概説

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

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

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 m 個の元が与えられた時に, 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.

3.1.3 代表的な LWE ベースの暗号方式

ここでは, LWE 問題をベースとした代表的な暗号方式をいくつか紹介する.

3.1.3.1 [Reg05] による公開鍵暗号方式

LWE 問題をベースとした公開鍵暗号として, [Reg05] で提案された方式が代表的である. [Reg05] の暗号方式の構成のためには, 以下の 4 つのパラメータが必要である:

- n: 安全性パラメータ
- m: LWE サンプルの個数 ($m = 1.1 \cdot n \log q$ となる整数を選ぶ)
- q: 剰余パラメータ (q として $n^2 \leq q \leq 2n^2$ を満たす素数を選ぶ)
- $\alpha > 0$:ノイズパラメータ ($\alpha = 1/\left(\sqrt{n}\log^2 n\right)$)

以下に具体的な暗号方式の構成を示す:

秘密鍵の生成 一様ランダムに $\vec{s} \leftarrow \mathbb{F}_q^n$ を選ぶ.

公開鍵の生成 秘密鍵 $\vec{s}$, 剰余パラメータ q, ノイズパラメータ α を持つ LWE 分布から生成した m 個のサンプル $(\vec{a}_i, b_i)_{i=1}^m \leftarrow A_{\vec{s},\chi}^m$ を公開鍵とする (つまり各 i に対し, $\vec{a} \leftarrow \mathbb{F}_q^n$ で $e_i \leftarrow \chi = D_{\mathbb{Z},\alpha q}$ と選び, $b_i = \langle \vec{a}_i, \vec{s} \rangle + e_i \in \mathbb{F}_q$ と構成する).

暗号化 集合 S を $\{1, 2, \ldots, m\}$ の中から一様ランダムに選んだ部分集合とする (例えば, $S = \{1, m\}$). このとき, 平文ビットが 0 の暗号文を $\left(\sum_{i\in S} \vec{a}_i, \sum_{i\in S} b_i\right)$ とし, 平文ビットが 1 の暗号文を $\left(\sum_{i\in S} \vec{a}_i, \lfloor \frac{q}{2} \rfloor + \sum_{i\in S} b_i\right)$ とする.

復号 暗号文 $(\vec{a}, b)$ に対し, $b - \langle \vec{a}, \vec{s} \rangle \in \mathbb{F}_q$ が $\lfloor \frac{q}{2} \rfloor$ より 0 に近い場合, 復号結果として 0 を出力し, それ以外の場合は 1 を出力する.

復号の正当性について, $(\vec{a}, b) = \left(\sum_{i\in S} \vec{a}_i, \sum_{i\in S} b_i\right)$ の場合 (つまり, 平文 0 に対応する暗号文の場合),

$$b - \langle \vec{a}, \vec{s} \rangle = \sum_{i\in S} (b_i - \langle \vec{a}_i, \vec{s} \rangle) = \sum_{i\in S} e_i$$

なので, $-\frac{q}{4} < \sum_{i\in S} e_i < \frac{q}{4}$ であれば復号に成功する (つまり, 復号として 0 が出力される). 各ノイズ e_i は標準偏差が αq のガウス分布 $\chi = D_{\mathbb{Z},\alpha q}$ から選ばれているので, $\sum_{i\in S} e_i$ の標準偏差は高々 $\sqrt{m}\alpha q$ となる. ここで, 各パラメータの選択方法から $\sqrt{m}\alpha q < q/\log n$ なので, 非常に高い確率で復号に成功することが分かる (平文ビットが 1 の暗号文に対しても同様の議論が成り立つ). また, 上記の暗号方式の安全性については, LWE 仮定の下で CPA 安全であることが証明されている [Reg09, Section 5].

ここで紹介した [Reg05] による暗号方式は, 公開鍵サイズが $(mn \log q) = \widetilde{O}(n^2)$ で, 暗号文サイズも平文サイズの $O(n \log q) = \widetilde{O}(n)$ 倍に増加するため, 決して効率的ではない (より効率的な方式としては [PVW08] などを参照).

■パラメータ設定について 上記で構成した [Reg05] による公開鍵暗号方式の具体的なパラメータ設定例が [MR09] で示されている. パラメータ設定例として, $(n, m, q, \alpha) = (136, 2008, 2003, 0.0065)$, $(192, 1500, 16381, 0.0009959)$, $(233, 1042, 32749, 0.000217)$ などが挙げられており, これらの各パラメータ設定は格子ベース暗号の安全性を測る root Hermite factor δ の値が 1.01 程度になるように設定されている (root Hermite factor δ については後述の 3.2.2 節を参照).

3.1.3.2 [BV11] による somewhat 準同型暗号方式 ([LNV11] で少し改良)

近年, 効率的な LWE ベースの暗号方式を得るために, [LPR10] で紹介されている ring-LWE 問題 (定義 3.5 を参照) の困難性に依存した方式がいくつか提案されている. 以下では, [BV11] で提案されている somewhat 準同型暗号方式を紹介する (somewhat 準同型暗号とは暗号化したまま限定回の加算と乗算が可能な暗号方式). [BV11] の somewhat

準同型暗号方式の構成のために, 以下の 4 つのパラメータが必要である:

- n: 2 べき整数で, 暗号方式を構成する基礎的な環 $R = \mathbb{Z}[x]/(x^n + 1)$ を定義する (n が 2 べき整数の場合のみ, 多項式 $x^n + 1$ は $\mathbb{Z}$ 上既約となることに注意).
- q: $q \equiv 1 \bmod 2n$ を満たす素数で, 暗号文空間の基礎環 $R_q = \mathbb{F}_q[x]/(x^n + 1)$ を定義する.
- t: 条件 $t < q$ を満たす整数で, 暗号方式の平文空間 $R_t = (\mathbb{Z}/t\mathbb{Z})[x]/(x^n + 1)$ を定義する.
- σ: ノイズを与えるためのガウス分布の標準偏差.

そこで, [BV11] の somewhat 準同型暗号方式は以下のように構成される (少しだけ改良された方式として [LNV11] も参照): また, 以下の構成では, 定義 3.5 と同じように $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \to (a_0, a_1, \ldots, a_{n-1})$ より環 R を $\mathbb{Z}^n$ と同一視する (同様に, $R_q \simeq \mathbb{F}_q^n$ と同一視することが可能).

鍵生成　まず, $R \ni s \leftarrow \chi = D_{\mathbb{Z}^n,\sigma}$ を選び, 一様ランダムに $p_1 \in R_q$ を取り, 小さなエラー $e \leftarrow \chi$ を固定する ([BV11] では $s \leftarrow \chi$ を一様ランダムに選択するのに対し, [LNV11] では一様ランダムには選択しない点だけが異なる). そこで, 公開鍵を $\mathsf{pk} = (p_0, p_1)$ とし (ただし, $p_0 = -(p_1 s + te)$ とする), 秘密鍵を $\mathsf{sk} = s$ とする.

暗号化　平文情報 $m \in R_t$ と公開鍵 $\mathsf{pk} = (p_0, p_1)$ に対し, まず $R \ni u, f, g \leftarrow \chi$ を選び, 暗号文を

$$\mathsf{Enc}(m, \mathsf{pk}) = (c_0, c_1) = (p_0 u + tg + m, p_1 u + tf),$$

と定義する. ただし, 条件 $t < q$ より, 上記の数式では元 $m \in R_t$ を環 R_q の元として見なして計算する. つまり, 上記の暗号文は $(R_q)^2$ の元として表現される.

準同型暗号演算 (暗号加算・暗号乗算)　上記の暗号アルゴリズムでは暗号文として $(R_q)^2$ の元を出力するが, 以下で定義する暗号乗算では暗号文の長さを長くする操作であるため, ここでは任意の長さの暗号文に対する暗号加算・乗算を定義する; 2 つの暗号文 $\mathsf{ct} = (c_0, c_1, \ldots, c_\xi)$ and $\mathsf{ct}' = (c'_0, c'_1, \ldots, c'_\eta)$ が与えられているとする.

- まず, 暗号加算 "$\dot{+}$" は, 以下のように各成分ごとの加算

$$\mathsf{ct} \dot{+} \mathsf{ct}' = (c_0 + c'_0, c_1 + c'_1, \ldots, c_{\max(\xi,\eta)} + c'_{\max(\xi,\eta)})$$

  で与えられる. 同様に, 暗号減算も各成分ごとの減算で与えられる.

- 次に, 暗号乗算 "$*$" は以下で与えられる:

$$\mathsf{ct} * \mathsf{ct}' = (\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_{\xi+\eta})$$

  ただし, z を変数としたとき, 各 $\hat{c}_i$ は以下の関係式から計算可能である:

$$\sum_{i=0}^{\xi+\eta} \hat{c}_i z^i = \left(\sum_{i=0}^{\xi} c_i z^i\right) \cdot \left(\sum_{j=0}^{\eta} c'_j z^j\right)$$

復号　任意の長さの暗号文 $\mathsf{ct} = (c_0, c_1, \ldots, c_\xi)$ に対して, 復号は

$$\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}) = [\tilde{m}]_q \bmod t \in R_t,$$

で計算できる. ただし, $\tilde{m} = \sum_{i=0}^{\xi} c_i s^i \in R_q$ であり, $[\tilde{m}]_q$ は元 $\tilde{m}$ の各係数の $[-q/2, q/2)$ への剰余とする. また, $\vec{s} = (1, s, s^2, \ldots)$ としたとき, この復号処理を $\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}) = [\langle \mathsf{ct}, \vec{s} \rangle]_q \bmod t$ と書き直すこともできる.

復号の正当性については, 上記の暗号アルゴリズムで得られる暗号文 $\mathsf{ct} = (c_0, c_1)$ に対し, 関係式 $p_0 + p_1 s = -te$ が成り立つので

$$\langle \mathsf{ct}, \vec{s} \rangle = (p_0 u + tg + m) + s \cdot (p_1 u + tf) = m + t \cdot (g + sf - ue)$$

が環 R_q 上で成り立つ. ここで, 元 $m+t\cdot(g+sf-ue)$ を環 R の元と見なしたとき, その各係数が $[-q/2,q/2)$ 内に収まっている限り, $[\langle \mathsf{ct},\vec{s}\rangle]_q = m+t\cdot(g+sf-ue)$ が環 R 上で成立する (元 $e,f,g,u\leftarrow\chi$ が十分小さなノイズとして選択されていることに注意). この場合, 剰余 mod$t$ の操作で正しい復号結果 $m\in R_t$ が得られる. また, 暗号加算・暗号乗算された暗号文について, 2 つの暗号文 $\mathsf{ct}_1,\mathsf{ct}_2$ に対し,

$$\begin{cases} \langle \mathsf{ct}_1 \dot{+} \mathsf{ct}_2,\vec{s}\rangle = \langle \mathsf{ct}_1,\vec{s}\rangle + \langle \mathsf{ct}_2,\vec{s}\rangle \\ \langle \mathsf{ct}_1 * \mathsf{ct}_2,\vec{s}\rangle = \langle \mathsf{ct}_1,\vec{s}\rangle \cdot \langle \mathsf{ct}_2,\vec{s}\rangle \end{cases}$$

が成り立つので, 暗号文のノイズが十分小さい限り, 準同型演算が可能な暗号方式となっている. 具体的には, 暗号文 $\mathsf{ct}_1,\mathsf{ct}_2$ が平文情報 $m_1,m_2\in R_t$ に対応しているとき, 各暗号文のノイズが小さい場合に限り

$$\begin{cases} \mathsf{Dec}(\mathsf{ct}_1 \dot{+} \mathsf{ct}_2,\mathsf{sk}) = m_1+m_2 \\ \mathsf{Dec}(\mathsf{ct}_1 * \mathsf{ct}_2,\mathsf{sk}) = m_1\times m_2 \end{cases}$$

が成立する.

また, この暗号方式の安全性については, 定義 3.5 で与えられた ring-LWE 問題を少し変形した以下の問題の計算量困難性に依存する (以下は [LNV11] を引用):

定義 3.3 (polynomial-LWE 問題 [BV11], [LNV11]) パラメータ (n,q,t,σ) が与えられた時, polynomial-LWE 問題 $\mathsf{PLWE}_{n,q,\chi}$ とは, 次の 2 つの分布を識別することである:

1. 一様ランダムに $(R_q)^2$ の元 (a_i,b_i) をサンプリングする.
2. 一様ランダムに $s\leftarrow\chi=D_{\mathbb{Z}^n,\sigma}$ を選び, 一様ランダムに $a_i\leftarrow R_q$ をサンプリングし, $e_i\leftarrow\chi$ を選び $b_i=a_is+e_i$ とする. このとき, $(a_i,b_i)\in(R_q)^2$ をサンプリングする.

上記で構成した somewhat 準同型暗号方式の安全性については, 具体的には上記の polynomial-LWE 問題の計算量困難性仮定の下で KDM 安全 (key dependent message security) であることが証明されている [BV11].

■パラメータ設定について 上記で構成される somewhat 準同型暗号方式に関して, [LNV11, Table 1] で具体的なパラメータ設定例が挙げられている. 表 3.1 で, [LNV11, Table 1] の中で代表的なパラメータ設定例を示すと共に, そのパラメータ設定に対する distinguishing attack による攻撃計算量の見積もりも示しておく. また, distinguishing attack による攻撃原理とその攻撃計算量評価については, 後述の 3.2.2 節で説明する (具体的には, 表 3.1 の distinguishing attack の攻撃計算量は式 (3.3) から算出した値である).

表 3.1 [BV11] による somewhat 準同型暗号方式のパラメータ設定例とその安全性レベル (詳細は [LNV11, Table 1] を参照, δ は各パラメータに対する root Hermite factor で詳細は 3.2.2 節を参照)

パラメータ (n,q,t,σ)	暗号乗算の深さ	distinguishing attack の攻撃計算量
$(2048, 52\text{-bit}, 128, 8)$	1	2^{198} $(\delta=1.0041)$
$(4096, 86\text{-bit}, 128, 8)$	2	2^{250} $(\delta=1.0035)$
$(4096, 118\text{-bit}, 128, 8)$	3	2^{149} $(\delta=1.0048)$
$(4096, 150\text{-bit}, 128, 8)$	4	2^{92} $(\delta=1.0062)$
$(16384, 338\text{-bit}, 128, 8)$	9	2^{243} $(\delta=1.0035)$

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 節で説明したように, 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 3.4 ([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 節の定義 3.5 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 3.5 (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 $\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_d\}$ 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である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 3.2[*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 3.2 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.

表 3.2 $\log_2(T_{\mathrm{BKZ}})$ 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

[*1] 表 3.2 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.

■近年の攻撃研究の動向 [BG14] では LWE 問題の特殊な場合に有効な攻撃手法を提案している. 具体的には, 定義 3.1 で紹介した LWE 問題において, 秘密情報 $\vec{s} \in \mathbb{F}_q^n$ と取り方として, $\vec{s} \leftarrow \{-1, 0, 1\}^n$ と限定する binary-LWE 問題について考察している. この binary-LWE 問題に対して, [BG14] では 3.2.2 節で少し紹介した decoding attack をベースとした攻撃手法を提案している. より具体的には, binary-LWE 問題を inhomogeneous short integer solution(ISIS) 問題に帰着させて解く手法を示しており (ISIS 問題: $(\mathbf{A}, \vec{v})$ が与えられた時, $\vec{v} \equiv \mathbf{A}\vec{y} \pmod q$ を満たす短い整数ベクトル $\vec{y}$ を見つける問題), 通常の攻撃よりも非常に効率的であることを理論的かつ実験的にも示している.

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] において [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, pp. 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, pp. 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, pp. 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, pp. 474–495, 2009.

[BG14] S. Bai and S. D. Galbraith, “Lattice Decoding Attacks on Binary LWE,” In *–Australasian Conference on Information Security and Privacy–ACISP 2014*, Springer LNCS 8544, pp. 322–337, 2014.

[BGV12] Z. Brakerski, C. Gentry and V. Vaikuntanathan, “(Leveled) fully homomorphic encryption without bootstrapping,” In *Innovations in Theoretical Computer Science–ITCS 2012*, ACM, pp. 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, pp. 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), pp. 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, pp. 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, pp. 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, pp. 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, pp. 18–34, 2013.

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

[Gen09] C. Gentry, "Fully homomorphic encryption using ideal lattices," In *Proc. 41st ACM Symp. on Theory of Computing–STOC 2009*, ACM, pp. 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, pp. 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, pp. 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, pp. 19–37, 2012.

[GKPV10] S. Goldwasser, Y. Kalai, C. Peikert and V. Vaikuntanathan, "Robustness of the Learning with Errors Assumption," In *Innovation in Computer Science–ICS 2010*, Tsinghua University, pp. 230–240, 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, pp. 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, pp. 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, pp. 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, pp. 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, pp. 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, pp. 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, pp. 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), pp. 267–302, 2007.

[MR09] D. Micciancio and O. Regev, "Lattice-based Cryptography," Post–Quantum Crytography, Springer, pp. 147–191, 2009.

[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: extended abstract," In *Proc. 41st ACM Symp. on Theory of Computing–STOC 2009*, ACM, pp. 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, pp. 554–571, 2008.

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

[Reg05] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," J. ACM, **56**(6) (2009), pp. 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, April 2014, Volume 71, Issue 1, pp. 57–81, 2014.

第 4 章

LPN

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

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

4.1.1 LPN 問題とは

LPN 問題とは誤差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. 特に q を素数とした場合には LWE 問題と非常によく似た問題・仮定となるが, 誤差分布 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, 誤差分布 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, 誤差分布 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,

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

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 $\mathsf{SD}_{k,m,w}$ とは,

$$\boldsymbol{H} = [\vec{h}_1^\top \vec{h}_2^\top \cdots \vec{h}_m^\top] \in \mathbb{F}_2^{k\times m},\ \vec{u} \in \mathbb{F}_2^k$$

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 $\mathsf{SD}_{m-n,m,O(\tau m)}$ に変換可能である.

4.1.2.3 Exact-LPN 問題

誤差分布として, $\vec{e}\leftarrow\mathsf{Ber}_\tau^m$ ではなく, ハミング重みが丁度 w のものだけを考える. このように誤差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, 疎 (sparse) であることを要求する. Applebaum ら [ACPS09] は $\vec{s}$ を誤差分布である 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.

Pietrzak 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,

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

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 上の誤差分布 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] による疑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 変換によるもの: 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.
- Full-Domain Hash によるもの: CFS 署名が知られている.

今までのところ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 暗号の派生: 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 暗号の派生: 標準モデルで IND-CCA2 安全な Niederreiter ベースの暗号として, 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].

以下では, LPN 仮定に基づく公開鍵暗号方式の例として Alekhnovich 暗号を取りあげる. また, 追加の仮定が必要であるが Alekhnovich 暗号よりも効率が良い公開鍵暗号方式の例として McEliece 暗号を取り上げる.

4.2.1 Alekhnovich 暗号 [Ale11]

Alekhnovich は [Ale11] で 2 つ公開鍵暗号方式を提案している. ここではシンプルな 1 つ目の暗号方式を取り上げる. パラメータを以下とする.

- n: 安全性パラメータ
- m: LPN サンプルの個数 (例: $m = 2n + 1$)
- $\tau > 0$: 誤差パラメータ (例: $\tau = n^{-1/2-\epsilon}$)

このとき Alekhnovich 暗号は以下で構成される:

秘密鍵の生成: ランダムに $\vec{e} \leftarrow \mathsf{Ber}_\tau^m$ を選ぶ.

公開鍵の生成 ランダムに $\boldsymbol{A} \leftarrow \mathbb{F}_2^{n\times m}$ を選ぶ. ランダムに $\vec{s} \leftarrow \mathbb{F}_2^n$ を選ぶ. $\vec{b} = \vec{s}\boldsymbol{A} + \vec{e} \in \mathbb{F}_2^m$ を計算し, $\boldsymbol{B} = \binom{\boldsymbol{A}}{\vec{b}}$ とする. $\boldsymbol{M} \in \mathbb{F}_2^{(m-n-1)\times m}$ を $\ker(\boldsymbol{B}^\top)$ の基底とし, 公開鍵を $\boldsymbol{M}$ とする.

暗号化 平文が 0 の場合, $\vec{t} \leftarrow \mathbb{F}_2^{m-n-1}$ と $\vec{f} \leftarrow \mathsf{Ber}_\tau^m$ をランダムに選び, $\vec{c} = \vec{t}\boldsymbol{M} + \vec{f} \in \mathbb{F}_2^m$ を出力する.
平文が 1 の場合, ランダムに $\vec{c} \leftarrow \mathbb{F}_2^m$ を選び出力する.

復号 暗号文 $\vec{c} \in \mathbb{F}_2^m$ について, $\delta = \langle \vec{c}, \vec{e} \rangle$ を計算する. δ を出力する.

復号の正当性について以下考察する. 平文が 1 の場合, 復号は確率 $1/2$ で成功する.
一方, 平文が 0 の場合, $\vec{e} \in \mathrm{Span}(\boldsymbol{B})$ および $\vec{t}\boldsymbol{M} \in \ker(\boldsymbol{B}^\top)$ より $\vec{t}\boldsymbol{M}\vec{e}^\top = 0$ であることに注意すると,

$$\langle \vec{c}, \vec{e} \rangle = \vec{t}\boldsymbol{M} \cdot \vec{e}^\top + \vec{f}\vec{e}^\top = \langle \vec{f}, \vec{e} \rangle$$

なので, $\langle \vec{f}, \vec{e} \rangle = 0$ であれば復号に成功する. 誤り確率を評価すると, $\Pr[\langle \vec{f}, \vec{e} \rangle = 1] \approx (1-\tau)^{\tau m} = o(1)$ となり, $1 - o(1)$ の確率で復号に成功する. また, 上記の暗号方式の安全性については, 判定版 LPN 仮定の下で CPA 安全であることが証明される.

ここで紹介した暗号方式は, 1 ビット暗号であり, 復号誤りの確率も高いため実用的ではない. 効率的な方式としては 2 つ目の Alekhnovich 暗号や次に挙げる McEliece 暗号を参考にされたい.

4.2.2 McEliece 暗号

以下では, S_m で m 次対称群を表し, $\mathrm{GL}_n(\mathbb{F}_q)$ で n 次の $\mathbb{F}_q$ 要素正則行列全体がなす群を表す.

- n: 安全性パラメータ
- m: サンプルの個数
- τ: 誤差パラメータ (例: $\tau = cn$)
- t: 誤り訂正符号の誤り訂正能力 ($t = \Omega(\tau m)$)

鍵生成: 誤り訂正能力が t である (m, n)-線形符号の生成行列 $\boldsymbol{G}$ を生成する. $\boldsymbol{S} \leftarrow \mathrm{GL}_n(\mathbb{F}_2)$ をランダムに選ぶ. $\boldsymbol{P} \leftarrow S_m$ をランダムに選ぶ. $\boldsymbol{M} = \boldsymbol{SGP}$ とする.
公開鍵を $\boldsymbol{M}$ とし, 秘密鍵を $(\boldsymbol{S}, \boldsymbol{G}, \boldsymbol{P})$ とする.

暗号化: 平文を $\vec{v} \in \mathbb{F}_2^n$ とする. 乱数 $\vec{e} \leftarrow \mathsf{Ber}_\tau^m$ を選び, 暗号文 $\vec{c} = \vec{v}\boldsymbol{M} + \vec{e}$ を計算する.

復号: $\hat{\vec{v}} = \vec{c}\boldsymbol{P}^{-1}$ を計算する. $\hat{\vec{v}}$ を誤り訂正符号で訂正し復号すると $\vec{v}' = \vec{v}\boldsymbol{S}$ を得る. $\vec{v} = \vec{v}'\boldsymbol{S}^{-1}$ を出力する.

復号の正当性は以下で確認される. $\vec{c} = \vec{v}\boldsymbol{M} + \vec{e}$ として, $\hat{\vec{v}} = \vec{c}\boldsymbol{P}^{-1}$ を計算すると,

$$\hat{\vec{v}} = \vec{v}\boldsymbol{M}\boldsymbol{P}^{-1} + \vec{e}\boldsymbol{P}^{-1} = \vec{v}\boldsymbol{S}\boldsymbol{G} + \vec{e}\boldsymbol{P}^{-1}$$

を得る. $\vec{v}\boldsymbol{S}\boldsymbol{G}$ は符号語であり, $\vec{e}\boldsymbol{P}^{-1}$ は誤りであり. $\vec{e}\boldsymbol{P}^{-1}$ の重みが t 以下であれば, 誤り訂正符号の復号により, $\vec{v}' = \vec{v}\boldsymbol{S}$ を得る. よって, 高い確率で復号に成功する.

平文 $\vec{v}$ および $\boldsymbol{M}$ がランダムであれば, 暗号文 $\vec{c}$ は LPN 仮定の下で疑似ランダムである. $\boldsymbol{M}$ が疑似ランダムであることを言うためには, McEliece 仮定と呼ばれる仮定が必要となる.

定義 4.7 (McEliece 仮定) $[m(n), n]_{q(n)}$-符号のクラス $\mathcal{C}$ を固定する. 敵 $\mathcal{A}$ の優位性を

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

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.

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. 暗号として用いる場合には, パラメータ設定によって彼らの攻撃を避けることが可能である.

■McEliece 暗号の変種の安全性について: 二元 Goppa 符号を用いた場合, 鍵サイズが大きくなることが知られている. そのため, 元となる符号を変更し, 鍵サイズや暗号文サイズを小さくする研究が進められてきた. しかし, 符号が特殊な場合には多くの方式が破られている. McEliece 暗号やその変種を用いる場合には, 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 元-Goppa 符号を用いた q 元-McEliece 暗号についてパラメータの提案を行っている.

■パラメータ設定について: Bernstein, Lange, Peters は [BLP10] および [BLP11a] で q 元-Goppa 符号を用いた q 元-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入手可能である. [*1] 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 問題をベースとした暗号方式を実際に構成する際には, 4.3 節で挙げる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 4.1) を行っている.

4.3 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.

[*1] http://pqcrypto.org/wild-challenges.html.

表 4.1 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

しかし平均時の困難性についてはよく分かっていない. そのため LPN 問題を解くための提案されたアルゴリズムについて調査を行った.

$\mathsf{LPN}_{n,m,\tau}$ 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, 時間 $O(2^n)$ で圧倒的な確率で $\mathsf{LPN}_{n,m,\tau}$ 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.

4.3.1 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 $\mathcal{O}_{\vec{s},\tau}$ 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: $(t-1)k < n \leq tk$ を満たす適当な自然数 t, k を固定する. 以下では,

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

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 ik 個の要素が必ず 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. $i = 0, 1, \ldots, t-2$ 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 $L_{i+1} = L_i - 2^k$ 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, $\vec{a} = (a_1, a_2, \ldots, a_{n-ik}, 0, \ldots, 0) \in \mathbb{F}_2^n$ の $(a_{n-(i+1)k+1}, a_{n-(i+1)k+2}, , \ldots, a_{n-ik}) \in$

$\mathbb{F}_2^k$ 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 $L_i - 2^k$ 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 $L_{t-1} = L - (t-1)2^k$ の $A_{\vec{s},\delta^{2^{t-1}},t-1}$ からのサンプルが得られる.

3. 得られた L_{t-1} 個の $A_{\vec{s},\delta^{2^{t-1}},t-1}$ からのサンプルを用いて, s_j を投票で決める.
   - $j = 1, 2, \ldots, n-(t-1)k$ 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, $b_{i_1} + b_{i_2} + \cdots + b_{i_\ell} = s_j + e_{i_1} + \cdots + e_{i_\ell}$ となり, 誤差が 0 になる確率は $\Pr[e_{i_1} + e_{i_2} + \cdots + e_{i_\ell} = 0] > 1/2 + (1-2\delta^{2^{t-1}})^\ell/2$ 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, $\mathrm{poly}\left(\delta^{-2^t}, 2^k\right)$ であった. $\tau < 1/2$ を定数とし, $t = \frac{1}{2}\log n$, $k = 2n/\log n$ 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 $n = tk$ 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, $A_{\vec{s},\delta^{2^{t-1}},t-1}$ からのサンプルであるため, $((a_1, a_2, \ldots, a_k, 0, \ldots, 0), b)$ という形をしている. このとき, $b = \sum_{i=1}^k a_i s_i + e$ となり, サンプルに影響を与えるのは, $\vec{s}$ の k ビット分である. LF アルゴリズムでは, $s_1, s_2, \ldots, s_k$ 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 4.8 $n = tk$ とし, $\delta = 1-2\tau$ とする.

- BKW アルゴリズムはクエリ数 $m = 20\ln(4n)2^k\delta^{-2^t}$, ステップ数 $t = O(ntm)$, 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 $m = (8k+200)\delta^{-2^t} + (t-1)2^k$, ステップ数 $t = O(ntm)$, メモリ量 $M = nm + k2^k$. 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 に従って選ばれる誤りベクトル $\vec{e}$ 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 を行い, $A_{\vec{e}',\delta^{2^{t-1}},t-1}$ からのサンプルを得る.
3. ステップ 3 で, k 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^k 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 k 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 $(1+1/d)\tau k$ 以下である. よって, $\vec{e}'$ の候補数は $\binom{k}{(1+1/d)\tau k}$ 以下となり, 総当りに必要な回数が削減される.

■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.

■GJL アルゴリズム: Guo, Johansson, Löndahl [GJL14] は, covering codes と呼ばれる符号を用いて Kirchner の手法の高速化を提案している. Kirchner の手法ではステップ 3 で, $A_{\vec{e}',\delta^{2^{t-1}},t-1}$ からのサンプル $\{(\vec{a}_i, b_i)\}$ が得られる. この $\vec{a}_i$ を covering code の受信語とみなすことで探索空間の圧縮を行い, 高速化に成功している.

■サンプル数が少ない場合: これまでに挙げてきた BKW アルゴリズムおよびその改良では, サンプルが $O(2^{n/\log n})$ 個必要であった. Lyubashevsky [Lyu05] はサンプル数が $n^{1+\epsilon}$ 個と少ない場合であっても, BKW アルゴリズムを適用できるような指数個のサンプルの構成法を示している. また, 上中谷と國廣 [KK15] は BKW アルゴリズムと Lyubashevsky の方法とを補間するようなアルゴリズムを提案している.

4.3.2 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.

4.3.3 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 4.2 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.

表 4.2 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]

パラメータ設定によっては, $\mathsf{LPN}_{n,m,\tau}$ 問題を $\mathsf{SD}_{m-n,m,w}$ 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.

4.3.4 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.

4.4 まとめ

LPN 問題は学習理論や符号理論から派生した問題である. 誤り確率 τ が十分大きい場合の LPN 問題を多項式時間で効率的に解くことは困難であると予想されている.

共通鍵や公開鍵の分野で多くの方式が LPN 問題に基づいて提案されている. LWE 問題と比較した場合, 利点としては,

- $\mathbb{F}_2$ およびその拡大体を基に構成するため, ハードウェア構成との相性が良い点
- 誤差分布としてベルヌーイ分布やその一般化した分布を用いるため, 誤差のサンプリングが容易である点

が挙げられる. 一方, 欠点として,

- 鍵や暗号文のサイズが大きくなりやすい点
- ID ベース暗号や完全準同型暗号といった発展的な応用が少ない点

が挙げられる.

暗号方式のパラメータ設定の際には, 4.2 節で挙げたさまざまなアルゴリズムを考慮する必要がある. アルゴリズムの高速化について盛んに研究されており, 動向を注視する必要がある. また, 攻撃に用いられるアルゴリズムの研究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] M. Alekhnovich, "More on average case vs approximation complexity," Computational Complexity 20(4): 755–786 (2011).

[App13] B. Applebaum, "Garbling XOR gates "For Free" in the standard model," In *Theory of Cryptography Conference–TCC 2013*, Springer, LNCS 7785, pp. 162–181, 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, pp. 595–618, 2009.

[AHI11] B. Applebaum, D. Harnik and Y. Ishai, "Semantic security under related-key attacks and applications," In *Innovations in Computer Science–ICS 2011*, Tsinghua University, pp.45-60, 2011.

[AG11] S. Arora and R. Ge, "New algorithms for learning in presence of errors," In *International Colloquium on Automata, Languages and Programming–ICALP 2011*, Part I, Springer LNCS 6755, pp. 403–415, 2011.

[BJMM12] A. Becker, A. Joux, A. May and A. Meurer, "Decoding random binary linear codes in $2^{n/20}$: How $1+1=0$ improves information set decoding," In *Advances in Cryptology–EUROCRYPT 2012*, Springer LNCS 7237, pp. 520–536, 2012.

[BMvT78] E. R. Berlekamp, R. J. McEliece and H. C. A. van Tilborg, "On the inherent intractability of certain coding problems," IEEE Transactions on Information Theory 24(3): 384–386 (1978).

[BJLM13] D. J. Bernstein, S. Jeffery, T. Lange, and A. Meurer, "Quantum algorithms for the subset-sum problem," In *Post-Quantum Cryptography–PQCrypto 2013*, Springer LNCS 7932, pp. 16–33, 2013.

[BLP10] D. J. Bernstein, T. Lange and C. Peters, "Wild McEliece," In *Selected Areas in Cryptography–SAC 2010*, Springer LNCS 6544, pp. 143–158, 2011.

[BLP11a] D. J. Bernstein, T. Lange and C. Peters, "Wild McEliece incognito," In *Post-Quantum Cryptography–PQCrypto 2011*, Springer LNCS 7071, pp. 244–254, 2011.

[BLP11b] D. J. Bernstein, T. Lange and C. Peters, "Smaller decoding exponents: Ball-collision decoding," In *Advances in Cryptology–CRYPTO 2011*, Springer LNCS 6841, pp. 743–760, 2011.

[BL12] D. J. Bernstein and T. Lange, "Never trust a bunny," In *Radio Frequency Identification. Security and Privacy Issues–RFIDSec 2012*, Springer LNCS 7739, pp. 137–148, 2013.

[BFKL93] A. Blum, M. L. Furst, M. J. Kearns and R. J. Lipton, "Cryptographic primitives based on hard learning problems," In *Advances in Cryptology–CRYPTO '93*, Springer LNCS 773, pp. 278–291, 1994.

[BKW03] A. Blum, A. Kalai and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," J. ACM 50(4): 506–519 (2003).

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

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

[DNdS12] B. M. David, A. C. A. Nascimento and R. T. de Sousa Jr., “Efficient Fully Simulatable Oblivious Transfer from the McEliece Assumptions,” IEICE Transactions 95-A(11): 2059–2066 (2012).

[DNMQ12] B. M. David, A. C. A. Nascimento and J. Müller-Quade, “Universally Composable Oblivious Transfer from Lossy Encryption and the McEliece Assumptions,” In *International Conference on Information Theoretic Security–ICITS 2012*, Springer LNCS 7412, pp. 80–99, 2012.

[DMQN12] N. Döttling, J. Müller-Quade and A. C. A. Nasciment, “IND-CCA secure cryptography based on a variant of the LPN problem,” In *Advances in Cryptology–ASIACRYPT 2012*, Springer LNCS 7658, pp. 485–503, 2012.

[DDMQN12] N. Döttling, R. Dowsley, J. Müller-Quade and A. C. A. Nasciment, “A CCA2 secure variant of the McEliece cryptosystem,” IEEE Transactions on Information Theory 58(10): 6672–6680 (2012).

[FGOPT13] J.-C. Faugère, V. Gauthier-Umaña, A. Otmani, L. Perret and J. P. Tillich, “A distinguisher for high-rate McEliece cryptosystems,” IEEE Transactions on Information Theory 59(10): 6830–6844 (2013).

[FS96] J. B. Fischer and J. Stern, “An Efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding,” In *Advances in Cryptology–EUROCRYPT ’96*, Springer LNCS 1070, pp. 245–255, 1996.

[FGK+13] D. M. Freeman, O. Goldreich, E. Kiltz, A. Rosen and G. Segev, “More constructions of lossy and correlation-secure trapdoor functions,” J. Cryptology 26(1): 39–74 (2013).

[GRS08] H. Gilbert, M. J. B. Robshaw and Y. Seurin, “HB$^{\#}$: Increasing the security and efficiency of HB+,” In *Advances in Cryptology–EUROCRYPT 2008*, Springer LNCS 4965, pp. 361–378, 2008.

[GRS08] H. Gilbert, M. J. B. Robshaw and Y. Seurin, “How to encrypt with the LPN problem,” In *International Colloquium on Automata, Languages and Programming–ICALP 2008*, Part II–Track B, Springer LNCS 5126, pp. 679–690, 2008.

[GJL14] Q. Guo, T. Johansson and C. Löndahl, “Solving LPN Using Covering Codes,” In *Advances in Cryptology–ASIACRYPT 2014*, Part I, Springer LNCS 8873, pp. 1–20, 2014.

[Hås01] J. Håstad, “Some optimal inapproximability results,” J. ACM 48(4): 798–859 (2001).

[HKL+12] S. Heyse, E. Kiltz, V. Lyubashevsky, C. Paar and K. Pietrzak, “Lapin: An efficient authentication protocol based on ring-LPN,” In *Fast Software Encryption–FSE 2012*, Springer LNCS 7549, pp. 346–365, 2012.

[HB01] N. J. Hopper and M. Blum, “Secure human identification protocols,” In *Advances in Cryptology–ASIACRYPT 2001*, Springer LNCS 2248, pp. 52–66, 2001.

[JKPT12] A. Jain, S. Krenn, K. Pietrzak and A. Tentes, “Commitments and efficient zero-knowledge proofs from learning parity with noise,” In *Advances in Cryptology - ASIACRYPT 2012*, Springer LNCS 7658, pp. 663–680, 2012.

[KK15] 上中谷 健, 國廣 昇, “LPN 問題に対する BKW アルゴリズムの拡張,” SCIS2015, 3E1-3, 2015.

[KSS10] J. Katz, J. S. Shin, and A. Smith, “Parallel and concurrent security of the HB and HB+ protocols,” J. Cryptology 23(3): 402–421 (2010).

[KPC+11] E. Kiltz, K. Pietrzak, D. Cash, A. Jain and D. Venturi. "Efficient Authentication from Hard Learning Problems," In *Advances in Cryptology–EUROCRYPT 2011*, Springer LNCS 6632, pp. 7–26, 2011.

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

[KI01] K. Kobara and H. Imai, "Semantically secure McEliece public-key cryptosystems – conversions for McEliece PKC," In *Public Key Cryptography–PKC 2001*, Springer LNCS 1992, pp. 19–35, 2001.

[LB88] P. J. Lee and E. F. Brickell, "An observation on the security of McEliece's public-key cryptosystem," In *Advances in Cryptology–EUROCRYPT '88*, Springer LNCS 330, pp. 275–280, 1988.

[LF06] É. Levieil and P.-A. Fouque, "An improved LPN algorithm," In *Security and Cryptography for Networks–SCN 2006*, Springer LNCS 4116, pp. 348–359, 2006.

[LDW94] Y. X. Li, R. H. Deng and X. M. Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," IEEE Transactions on Information Theory 40(1): 271–273 (1994).

[Lyu05] V. Lyubashevsky, "The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem," In *Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques–APPROX–RANDOM 2005*, Springer LNCS 3624, pp. 378–389, 2005.

[MVVR12] K. P. Mathew, S. Vasant, S. Venkatesan and C. P. Rangan, "An efficient IND-CCA2 secure variant of the Niederreiter encryption scheme in the standard model," In *Australasian Conference on Information Security and Privacy–ACISP 2012*, Springer LNCS 7372, pp. 166–179, 2012.

[MMT11] A. May, A. Meurer and E. Thomae, "Decoding random linear codes in $\tilde{\mathcal{O}}(2^{0.054n})$," In *Advances in Cryptology–ASIACRYPT 2011*, Springer LNCS 7073, pp. 107–124, 2011.

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

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

[NIKM08] R. Nojima, H. Imai, K. Kobara and K. Morozov, "Semantic security for the McEliece cryptosystem without random oracles," Designs, Codes and Cryptography 49: pp. 289–305 (2008).

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

[Pie12a] K. Pietrzak, "Subspace LWE," In *Theory of Cryptography Conference–TCC 2012*, Springer LNCS 7194, pp. 548–563, 2012.

[Pie12b] K. Pietrzak, "Cryptography from learning parity with noise," In *Conference on Current Trends in Theory and Practice of Computer Science–SOFSEM 2012*, Springer LNCS 7147, pp. 99–114, 2012.

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

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

第 5 章

Approximate Common Divisor 問題

本章では, Approximate Common Divisor (ACD) 問題及び関連する問題の困難性や暗号技術へのアプリケーションについての調査結果について述べる.

5.1 Approximate Common Divisor 問題の概説

5.1.1 Approximate Common Divisor 問題とは

Approximate Common Divisor 問題 (ACDP) は, CaLC2001 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. $a_1, a_2, \ldots, a_n$ 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持つ, 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 らは, 公開鍵サイズを削減する方式を提案している [CMNT11]. 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. 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, パラメータ設定を行っている.

以下, 順に, van Dijk らの方式 [DGHV10], Cheon らの方式 [CCK+13] を説明する. ただし, 記述を容易にするため, 完全準同型方式ではなく, somewhat 準同型方式を記載する.

5.1.3.1 van Dijk らの方式 [DGHV10]

正の奇数 p に対して, 以下のように, γ ビットの整数上の分布 $\mathcal{D}_{\gamma,\rho}(p)$ を導入する.

$$\mathcal{D}_{\gamma,\rho}(p) = \{ \text{ choose } q \leftarrow \mathbb{Z} \cap [0, 2^\gamma/p), r \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho) : \text{ output } x = pq + r\}$$

KeyGen(λ)

秘密鍵： η ビットの奇数 p

公開鍵： x_i を $D_{\gamma,\rho}(p)$ から $\tau + 1$ 個取り, それらを $x_0, x_1, \ldots, x_\tau$ とする. ただし, x_0 が最大とする. x_0 は奇数で, $x_0 \bmod p$ は偶数であるとし, そうでなければ, あらためて, x_i を取り直す. 公開鍵 pk は, $(x_0, x_1, \ldots, x_\tau)$ である.

Enc($pk, m \in \{0, 1\}$)

Step1 ランダムな部分集合 $S \subseteq \{1, 2, \ldots, \tau\}$ を選ぶ.

Step2 $r \leftarrow \mathbb{Z} \cap (-2^{\rho'}, 2^{\rho'})$ を選ぶ.

Step3 暗号文

$$c \leftarrow (m + 2r + 2\sum_{i \in S} x_i) \bmod x_0$$

とする.

Dec(sk, c)

$m' \leftarrow (c \bmod p) \bmod 2$ を計算し, m' を出力する.

5.1.3.2 CCK+13 方式 [CCK+13]

簡単のため, 論文中メッセージ空間は, 二進系列の場合のみを記述する. 一般の場合の記述は, [CCK+13] を参照されたい.

KeyGen(λ)

秘密鍵： η ビットの異なる奇数 $p_0, p_1, \ldots, p_{l-1}$

公開鍵： $\pi = \prod_{i=0}^{l-1} p_i$ とする. q_0 を, 0 から $2^\gamma/\pi$ の間の整数をランダムに選び, $x_0 = q_0\pi$ とする. ただし, q_0 は, 2^{λ^2}-rough であるとする.

$$x_i \bmod p_j = 2r_{i,j}, r_{i,j} \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho) \text{ for } 1 \le i \le \tau$$
$$x'_i \bmod p_j = 2r'_{i,j} + \delta_{i,j}, r'_{i,j} \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho) \text{ for } 0 \le i \le l-1$$

ここで, $\delta_{i,j}$ は, $i = j$ のときに, 1 であり, $i \neq j$ とき, 0 を取る. 公開鍵 pk は, $(x_0, x_1, \ldots, x_\tau, x'_0, x'_1, \ldots, x'_{l-1})$ である.

Enc($pk, \boldsymbol{m} = (m_0, m_1, \ldots, m_{l-1}) \in \{0, 1\}^l$)

Step1 $\boldsymbol{b} = (b_1, b_2, \ldots, b_\tau) \in \{0, 1\}^\tau$ をランダムに選ぶ.

Step2 暗号文

$$c \leftarrow (\sum_{i=0}^{l-1} m_i x'_i + \sum_{i=1}^{\tau} b_i x_i) \bmod x_0$$

とする.

Dec(sk, c)

$m_j \leftarrow (c \bmod p_j) \bmod 2$ を計算し, $\boldsymbol{m} = (m_0, m_1, \ldots, m_{l-1})$ を出力する.

5.1.4 安全性の根拠となる問題

[DGHV10] では, Approximate GCD 問題を次のように定義している. (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, $\mathcal{D}_{\gamma,\rho}(p)$ からの多項式個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, 用いるパラメータを $(\rho, \rho', \eta, \gamma, \tau)$ 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, 次のように定義する.

$$\mathcal{D}'_\rho(p, q_0) = \{ \text{ choose } q \leftarrow \mathbb{Z} \cap [0, q_0), r \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho) : \text{ output } x = pq + r \}$$

(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.

[CMNT11] 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, 用いるパラメータを $(\rho, \rho', \eta, \gamma, \tau)$ 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.

[CCK+13] で提案された somewhat 準同型暗号方式は, 判定 Approximate GCD 問題の困難さに安全性の根拠をおいている. この問題は, 以下のように定式化される.

1. $\mathcal{D}'_\rho(p, q_0)$ から多項式個のサンプルを受け取った上で,
2. $z = x + rb \bmod x_0$ を受け取った時に, $b \in \{0, 1\}$ を判定する問題である. ここで, $x \leftarrow \mathcal{D}'_\rho(p, q_0)$ と $r \leftarrow \mathbb{Z} \cap [0, x_0)$ である.

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, 用いるパラメー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ータに対して, 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, 「Securtiy 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, 適切にパラメー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 関連問題 co-ACD 問題の安全性評価

Cheon らは, ACM CCS2014 において, ACD 問題の関連問題として, co-ACD 問題を導入し, この問題の困難さに安全性の根拠をおく加法準同型暗号を提案している [CLS14]. この加法準同型暗号方式は, 同様の機能を持つ Paillier 暗号と比べて, 高速に演算が可能であるという性質を持つ. さらに, co-ACD 問題の安全性を議論し, ACD 問題に対するアルゴリズムを適用した場合には, 十分, 安全であることを示している.

以下に, co-ACD 問題の定義を記す. まず, 分布 $\hat{\mathcal{D}}_{\rho,Q}$ を, 以下のように定義する. 素数 $(p_1, p_2, \ldots, p_k)$ として, $e \leftarrow \mathbb{Z} \cap (-2^\rho, 2^\rho)$ とし,

$$(eQ \bmod p_1, eQ \bmod p_2, \ldots, eQ \bmod p_k)$$

を出力する. 計算 co-ACD 問題は, $\hat{\mathcal{D}}_{\rho,Q}$ からの多項式個のサンプルが与えられたときに, $\prod_{i=1}^{k} p_i$ の非自明な因数を求める問題である.

しかし, 最近になり, co-ACD 問題に特化した攻撃手法が提案されている [FLT15]. [FLT15] は, 短い平文に対する暗号文を複数得られた状況で, Nguyen-Stern の直交格子解読手法, グレブナー基底手法, Coppersmith アルゴリズムを用いることにより, 効率的に平文の復元が可能であると主張している.

5.6 まとめ

この節の議論をまとめる. 現状において, ACD 問題は, パラメー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ータのいくつかは, 解読されることが示されている. また, ACD 問題に関連した問題 co-ACD 問題は, 当初の想定よりも弱いことが明らかになっている. これらの結果は, 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,” In *Advances in Cryptology–EUROCRYPT 2012*, Springer 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,” In *Advances in Cryptology–EUROCRYPT 2013*, Springer LNCS 7237, LNCS 7881, pp. 315–335, 2013.

[CLS14] J. H. Cheon, H. T. Lee and J. H. Seo, “A New Additive Homomorphic Encryption based on the co-ACD Problem,” In *the 2014 ACM SIGSAC Conference on Computer and Communications Security–CCS2014*, ACM, pp. 287–298, 2014.

[CH11] H. Cohn and N. Heninger, “Approximate common divisors via lattices,” In *the 10th Algorithmic Number Theory Symposium–ANTS–X*, pp. 271–293, 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,” In *Advances in Cryptology–Eurocrypt ’96*, Springer LNCS 1070, pp. 155–165, 1996.

[Cop96:A] D. Coppersmith, “Finding a Small Root of a Bivariate Integer Equation; Factoring with High Bits Known,” In *Advances in Cryptology–Eurocrypt ’96*, Springer LNCS 1070, pp. 178–189, 1996.

[Cop97] D. Coppersmith, “Small solutions to polynomial equations, and low exponent RSA vulnerabilities,” Journal of Cryptology, Volume 10, Issue 4, pp. 233–260, 1997.

[CMNT11] J.-S. Coron, A. Mandal, D. Naccache and M. Tibouchi, “Fully homomorphic encryption over the integers with shorter public keys,” In *Advances in Cryptology–CRYPTO 2011*, Springer LNCS 6841, pp. 487–504, 2011.

[CNT12] J. -S. Coron, D. Naccache and M. Tibouchi, “Public key compression and modulus switching for fully homomorphic encryption over the integers,” In *Advances in Cryptology–EUROCRYPT 2012*, Springer LNCS 7237, pp. 446–464, 2012.

[DGHV10] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, “Fully homomorphic encryption over the integers,” In *Advances in Cryptology–EUROCRYPT 2004*, Springer LNCS 6110, pp. 14–27, 2010. Longer version available as Report 2009/616 in the Cryptology ePrint Archive (`http://eprint.iacr.org/2009/616/`).

[FLT15] ピエール=アラン・フーク, タンクレード・ルポワン , メディ・ティブシ, “Co-ACD 仮定とそれを基にした準同型暗号方式の安全性評価,” SCIS2015, 3E4-4, 2015.

[HG97] N. Howgrave-Graham, “Finding small roots of univariate modular equations revisited,” In *Cryptog-*

raphy and Coding–IMA 1997, Springer LNCS 1355, pp. 1331–142, 1997.

[HG01] N. Howgrave-Graham, “Approximate integer common divisors,” In *Cryptography and Lattices–CaLC 2001*, Springer LNCS 2146, pp. 51–66, 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 *Annual Symposium on Foundations of Computer Science–FOCS'94*, IEEE Computer Society, pp. 124–134, 1994.

[TK13] A. Takayasu and N. Kunihiro, “Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors,” In *Australasian Conference on Information Security and Privacy–ACISP2013*, Springer 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 2 月作成 (2015 年 2 月更新)

概 要

ペアリング暗号の安全性は, 楕円曲線上の離散対数問題と有限体上の離散対数問題を解く計算の困難性を基盤としている. 即ちそれらの離散対数問題の内で一つでも解くことができればペアリング暗号は解読されてしまう. 有限体上の離散対数問題を効率よく解く手法として数体篩法と関数体篩法が挙げられ, 前者は標数が大きい有限体に, 後者は標数の小さい有限体の場合に適している. 近年, 関数体篩法の改良で大きな進展があった. これまで関数体篩法の関係探索段階において, sieving (篩) と呼ばれる手法が採用されてきたが, 近年は pinpointing に代表される新たな手法 (Frobenius representation algorithm など) が提案され, さらに Kummer extension の性質などが利用できる有限体では計算量が大きく削減される. 一方で, 標数の大きい有限体上の離散対数問題に適した数体篩法の改良も進んではいるものの, 関数体篩法ほどの計算量の改善は現在まで報告されていない.

本稿では, ペアリング暗号に適した標数の小さい有限体上の離散対数問題において, 上記の新たな手法を導入した関数体篩法に関する近年の研究報告について簡単に説明する. 特に重要な事実として, Kummer extension などの性質の利用が有効でない, ペアリング暗号で利用される標数の小さな有限体上の離散対数問題に対しても, 新たな手法の有効性を示す研究報告を挙げる.

最後に, 関数体篩法や数体篩法を有効に適用するには, 拡大次数の大きさと部分体の大きさの比などが関係するため, ペアリング暗号の安全性は推奨された有限体ごとに評価される必要があることを注意として挙げる.

1 概説

有限体上の離散対数問題を解く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.

関数体篩法では関係探索段階において, 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. 後述の新しい手法である pinpointing の戦略に沿った手法が登場するまではこの二つの段階の計算量が関数体篩法の計算量を決定していた [1]. Pinpointing は sieving に代わる手法として Joux によって 2012 年に提案された [14].

[1]関数体篩法の一種で, 漸近的な計算量が quasi-polynomial である Frobenius Representation algorithm [5] の計算量は, 関係探索段階や線型代数段階ではなく, 与えられた離散対数問題を解く段階である個別離散対数計算段階 (Individual Logarithm Phase) の計算量で見積もられる. しかし, Joux と Pierrot らの ASIACRYPT 2014 のスライドに書かれているように, Frobenius Representation algorithm においても, 実際の計算では線型代数段階の計算コストが最も大きい場合が多い.

Sieving では, 篩区間に対応する relation の候補である各多項式に対して, 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, マーキングのみを行うことで収集していた. 即ち sieving の利点は, 多項式の割り算をマーキングで代用することで, relation の候補となる各多項式に対する計算コストを削減することである. 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, Henríquez らの原稿に詳しく書かれている [2].) 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,

$$q = L_Q(1/3, 3^{-2/3}),\ n = 3^{2/3}(\log Q/\log\log Q)^{2/3}$$

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, その計算量は $L_Q(1/3, 0.96)$ に削減された. その結果 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 の方針に沿って改良され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 [16]. さらに, 同年, Barbulescu, Gaudry, Joux と Thomé は [16] 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 $GF(q^{2n}) = GF(Q)$ 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 [5]. 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. これら [5, 16] の種の手法は Frobenius representation algorithm と呼ばれる [22].

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

この節では, 小さい標数の有限体を使用するペアリング暗号への Frobenius representation algorithm が与える影響に関する研究成果について紹介する. 結論としては, 数値実験の報告においても理論値によるその安全性評価の報告においても, 小さい標数の有限体を使用するペアリング暗号の安全性がそれ以前の見積もりより低くなることを意味する結果が報告されている.

表 1: 標数が 2 または 3 である有限体上の離散対数問題に関する記録. 表中の * は Kummer extension または twisted Kummer extension の性質を適用されたことを意味する.

Date	Field	Bitsize	CPU-hours	Algorithm	Authors	Reference
1992	$GF(2^{401})$	401	114000	[6]	Gordon, McCurley	[11]
2001.09	$GF(2^{521})$	521	2000	[19]	Joux, Lercier	[19]
2001	$GF(2^{607})$	607	> 200000	[6]	Thomé	[24]
2005.09	$GF(2^{613})$	613	26000	[19]	Joux, Lercier	[21]
2012.06	$GF(3^{6\cdot 97})$	923	895000	[20]	Hayashi et al.	[13]
2013.02	$GF(2^{2\cdot 7\cdot 127})$	1778*	220	[16]	Joux	[15]
2013.02	$GF(2^{3^3\cdot 73})$	1971*	3132	[7]	Göloğlu et al.	[7]
2013.03	$GF(2^{2^4\cdot 3\cdot 5\cdot 17})$	4080*	14100	[16]	Joux	[17]
2013.04	$GF(2^{809})$	809	19300	[1, 20]	The Caramel Group	[4]
2013.04	$GF(2^{2^3\cdot 3^2\cdot 5\cdot 17})$	6120*	750	[7, 16]	Göloğlu et al.	[8]
2013.05	$GF(2^{2^3\cdot 3\cdot 257})$	6168*	550	[16]	Joux	[18]
2014.01	$GF(3^{6\cdot 137})$	1303	888	[16]	Adj et al.	[3]
2014.01	$GF(2^{2\cdot 3^5\cdot 19})$	9234*	398000	[16]	Granger et al.	[9]
2014.01	$GF(2^{2^2\cdot 3\cdot 367})$	4404	52000	[16]	Granger et al.	[10]
2014.09	$GF(3^{5\cdot 479})$	3796	8600	[16]	Joux, Pierrot	[22]
2014	$GF(3^{6\cdot 163})$	1551	1201	[16]	Adj et al.	[3]
2014.10	$GF(2^{1279})$	1279	35040	[16]	Kleinjung	[23]

まず数値実験に関してであるが, 表 1 は標数が 2 または 3 である有限体上の離散対数問題に関する主な記録をまとめたものである [2]. 表 1 が示すように, Frobenius representation algorithm ([7, 16]) において Kummer extension または twisted Kummer extension の性質などを適用できる場合は, 9234-bit 長の離散対数問題の記録のように, 大きな bit 長の離散対数問題が解かれている. それに比べて素数次拡大の場合の最高記録は 1279-bit 長の離散対数問題となっている. ペアリング暗号で利用される (i) $GF(3^{6\ell})$ (ℓ は素数とする) に分類される有限体については, 素数次拡大の有限体に次いで計算コストの高い有限体に分類でき, $GF(3^{6\cdot 137})$ や $GF(3^{6\cdot 163})$ の場合が解かれている. 従って $\ell \leq 163$ である有限体 $GF(3^{6\ell})$ 上の離散対数問題が現実的な時間内で解かれることが見込まれる. また, (iii) $GF(2^{12\ell})$ (ℓ は素数とする) の場合については, 128-bit 安全性が見込まれていた有限体 $GF(2^{12\cdot 367})$ の場合が解かれている. 従って, その部分体である $GF(2^{4\cdot 367})$ 上の離散対数問題も解くことが可能であるため, $\ell \leq 367$ である有限体 $GF(2^{12\ell})$ と 有限体 $GF(2^{4\ell})$ 上の離散対数問題は現実的な時間内で解かれることが見込まれる.

理論的な安全性評価については, Adj, Menezes, Oliveira, Henríquez らは, Frobenius representation algorithm ([5]) を用いた場合, 特に 128-bit 安全性が見込まれていた有限体 $GF(3^{6\cdot 509})$ の場合は 73.7-bit 安全性と見積もっている [2]. また, Granger, Kleinjung, Zumbrägel らは体の表現を工夫することにより, 同じく 128-bit 安全性が見込まれていた有限体 $GF(2^{4\cdot 1223})$ を使用した場合は 59-bit 安全性と見積もっている [10].

[2] 表 1 は, Joux らがまとめた離散対数問題に関するサーベイ集 “The Past, evolving Present and Future of Discrete Logarithm” [21] の Table 1 を編集し 2014 年 1 月以降の結果などを追記したものである.

3 Pinpointing を用いた関数体篩法の概要

表 1 が示すように, Frobenius representation algorithm は, 標数が小さい有限体上の離散対数問題を現時点で最も効率よく解く手法である. Frobenius representation algorithm の新たな方針は, 関係探索段階において sieving とは異なる手法で relation を効率よく生成することである. この方針が最初に採用されたのは関数体篩法 JL06-FFS [20] の 関係探索段階において pinpointing を導入した手法である [14]. この節では pinpointing 用いた関数体篩法について簡単に説明する. Frobenius representation algorithm [16, 5] については Hayashi が参考文献 [12] で簡明に説明している.

3.1 標数が小さい場合の関数体篩法の例

まず, 関数体篩法 JL06-FFS [20] について簡単に説明する. 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.

この関数体篩法の関係探索段階では,

$$\mathcal{A}(y)g_1(y) + \mathcal{B}(y) = \mathcal{A}(g_2(x))x + \mathcal{B}(g_2(x))$$

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, 関係探索段階の計算量は $L_{q^n}(1/3, c_1)$, 線型代数段階のそれは $L_{q^n}(1/3, c_2)$ となる. ただし

$$c_1 = \frac{2}{3\sqrt{\alpha D}} + \alpha D,\ c_2 = 2\alpha D$$

で, 次の条件が成り立つとする：

$$(D+1)\alpha \geq \frac{2}{3\sqrt{\alpha D}}.$$

3.2 Pinpointing

簡単な例として, 関数体篩法 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 (1-smooth である) 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 $a\in\mathbb{F}_q^*$ 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. さらに線型方程式の変数を実質的に $1/n$ 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, 線型方程式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, $A\neq0$, $B\neq0$, 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, $AB^{d_2} = a^{1-d_1 d_2} = a^{-n}$ 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

$$O\left(\frac{n(d_1+1)!(d_2+1)!}{q-1}\right)+1$$

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-hours を必要としたとの報告がある.

表 2: 文献 [14] の実験結果

Bitsize	Total time (CPU-hours)	Relation construction (CPU-hours)	Linear algebra (CPU-hours)	Indiv. Log. (CPU-hours)
1175	約 32000	3	32000	4
1425	約 32000	6	32000	< 12

4 更新履歴

更新日時	主な更新内容
2015 年 2 月	•概要を追加. •2 節. 表 1 とその解説を加筆.

参考文献

[1] L. M. Adleman, M-D. A. Huang, “Function field sieve method for discrete logarithms over finite fields,” Inf. Comput., 151 (1999), 5-16.

[2] G. Adj, A. Menezes, T. Oliveira, F. R. Henríquez, “Weakness of $\mathbb{F}_{3^{6\cdot 509}}$ for Discrete Logarithm Cryptography,” Proc. of Pairing 2013, LNCS 8365 (2013), 20-44.

[3] G. Adj, A. Menezes, T. Oliveira, F. R. Henríquez, “Computing Discrete Logarithms in $\mathbb{F}_{3^{6\cdot 137}}$ and $\mathbb{F}_{3^{6\cdot 163}}$ using Magma,” Proc. of WAIFI 2014, LNCS 9061 (2015), 3-22.

[4] R. Barbulescu, C. Bouvier, J. Detrey, P. Gaudry, H. Jeljeli, E. Thomé, M. Videau, P. Zimmermann, “Discrete Logarithm in $GF(2^{809})$ with FFS,” Proc. of Public Key Cryptography 2014, LNCS 8383 (2014), 221-238.

[5] R. Barbulescu, P. Gaudry, A. Joux, E. Thomé, “A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic,” Proc. of EUROCRYPT 2014, LNCS 8441 (2014), 1-16.

[6] D. Coppersmith, “Fast evaluation of logarithms in fields of characteristic two,” IEEE Transactions on Information Theory, 30/4 (1984), 587-593.

[7] F. Göloğlu, R. Granger, G. McGuire, J. Zumbrägel, “On the function field sieve and the impact of higher splitting probabilities - application to discrete logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$,” Proc. of CRYPTO 2013, LNCS 8043 (2013), 109-128.

[8] F. Göloğlu, R. Granger, G. McGuire, J. Zumbrägel, “Solving a 6120-bit DLP on a Desktop Computer,” Proc. of SAC 2013, LNCS 8282 (2013), 136-152.

[9] R. Granger, T. Kleinjung, J. Zumbrägel, “Discrete Logarithms in GF(2^9234),” `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1401&L=NMBRTHRY&F=&S=&P=8736`.

[10] 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 $\mathbb{F}_{2^{12\cdot 367}}$),” Proc. of CRYPTO 2014, LNCS 8617 (2014), 126-145.

[11] D. M. Gordon, K. S. McCurley, “Massively Parallel Computation of Discrete Logarithms,” Proc. of CRYPTO 1992, LNCS 740 (1992), 312-323.

[12] T. Hayashi, “Cryptanalysis of Pairing-based Cryptosystems Over Small Characteristic Fields,” Proc. of the Forum of Mathematics for Industry 2013, 1 (2013), 167-176.

[13] T. Hayashi, T. Shimoyama, N. Shinohara, T. Takagi, “Breaking Pairing-Based Cryptosystems Using η_T Pairing over $GF(3^{97})$,” Proc. of ASIACRYPT 2012, LNCS 7658 (2012), 43-60.

[14] A. Joux, “Faster index calculus for the medium prime case. Application to 1175-bit and 1425-bit finite fields,” Proc. of EUROCRYPT 2013, LNCS 7881 (2013), 177-193.

[15] A. Joux, “Discrete Logarithms in GF(2^1778),” `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1302&L=NMBRTHRY&F=&S=&P=2317`.

[16] A. Joux, "A new index calculus algorithm with complexity $L(1/4 + o(1))$ in small characteristic," Proc. of SAC 2013, LNCS 8282 (2013), 355-379.

[17] A. Joux, "Discrete Logarithms in GF(2^4080)," https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1303&L=NMBRTHRY&F=&S=&P=13682.

[18] A. Joux, "Discrete Logarithms in GF(2^6168) [=GF((2^257)^24)]," https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1305&L=NMBRTHRY&F=&S=&P=3034.

[19] A. Joux and R. Lercier, "The function field sieve is quite special," Proc. of ANTS 2002, LNCS 2369 (2002), 431-445.

[20] A. Joux and R. Lercier, "The function field sieve in the medium prime case," Proc. of EUROCRYPT 2006, LNCS 4004 (2006), 254-270.

[21] A. Joux, A. Odlyzko, C. Pierrot, "The Past, evolving Present and Future of Discrete Logarithm," Open Problems in Mathematical and Computational Science, Springer (2014), 5-36.

[22] A. Joux, C. Pierrot, "Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms - Simplified Setting for Small Characteristic Finite Fields," Proc. of ASIACRYPT 2014, LNCS 8873 (2014), 378-397.

[23] Kleinjung, "Discrete Logarithms in GF(2^1279)," https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1410&L=NMBRTHRY&F=&S=&P=1170.

[24] E. Thomé, "Computation of Discrete Logarithms in $\mathbb{F}_{2^{607}}$," Proc. of ASIACRYPT 2001, LNCS 2248 (2001), 107-124.

付録 7

暗号技術調査 WG (軽量暗号) 報告書

暗号技術調査 (軽量暗号) ワーキンググループ

2015 年 3 月

目次

はじめに

本報告書は、暗号技術調査 WG(軽量暗号) が 2013 年度および 2014 年度に調査・検討した内容をまとめたものである。

1 章では、総括として、軽量暗号の現状と今後の活動方針をまとめている。

2 章では、軽量暗号に関する現状調査として、軽量暗号技術において、産業上のニーズがあり、具体的な暗号アルゴリズムの設計、安全性評価、実装評価が学会等で発表されている技術分類について代表的な軽量暗号アルゴリズムの現状調査（サーベイ）を行った結果をまとめている。

3 章では、軽量暗号に関わる新しい技術動向や関連する外部動向についての調査、軽量暗号の活用事例および標準化動向についてまとめている。

4 章では、軽量暗号のアプリケーションとして、自動車セキュリティおよび制御システムへの応用についてヒアリングを行った内容をまとめている。

5 章では、特に軽量ブロック暗号について、実装詳細評価を行った結果をまとめている。

以上の調査は、2014 年 12 月までに入手できる情報を対象とした。但し、2015 年 1 月に開催された 2015 年暗号と情報セキュリティシンポジウム (SCIS2015) で発表された内容を一部含む。

本報告書は下記に示す軽量暗号 WG 委員で執筆を行った。所属は 2015 年 3 月時点のものである。

主査	本間　尚文	国立大学法人東北大学　大学院情報科学研究科　情報基礎科学専攻　准教授
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	岩田　哲	国立大学法人名古屋大学　大学院工学研究科　計算理工学専攻　准教授
委員	小川　一人	NHK 放送技術研究所　ハイブリッド放送システム研究部　上級研究員
委員	崎山　一男	国立大学法人電気通信大学　大学院　情報理工学研究科　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　情報技術総合研究所　情報セキュリティ技術部　開発第 1 グループ　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　CPU システムソリューション部　主任技師
委員	峯松　一彦	日本電気株式会社　クラウドシステム研究所　主任研究員
委員	三宅　秀享	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　研究主務
委員	渡辺　大	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

2

第 1 章

総括：軽量暗号の現状と今後の活動方針

1.1　CRYPTREC で扱う軽量暗号のスコープ

近年、リソースの限られたデバイスにも実装可能な「軽量暗号」(Lightweight Cryptography) の研究開発が進んでいる。これまで多くのアルゴリズムが発表され、国際標準化 (ISO/IEC 29192 など) も進んでいる。欧州では 2004 年から European Commission の第 6-7 次 Framework Programme の研究プロジェクト ECRYPT I, ECRYPT II のテーマとしても取り上げられてきた。日本も小型ハードウェア実装に適した暗号技術等で強みをもっている分野である。

低コスト・低消費電力で動作可能な軽量暗号技術は、今後もセンサー、車載機器、医療機器をはじめさまざまな用途での利用が期待されており、M2M (Machine to Machine), IoT (Internet of Things), CPS (Cyber Physical System) といった次世代のネットワークサービスを構築する上で有効なセキュリティ技術の一つとなることが期待される。

CRYPTREC では、主として電子政府で利用する暗号技術について検討を行っているが、電子政府のみに閉じることなく、さまざまな領域で利用される暗号技術についても技術調査を行い、社会に役立つ形で情報提供を行うことを目指している。軽量暗号技術が求められる製品やサービスにおいて、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目指し、2013 年度より CRYPTREC 暗号技術評価委員会の下に軽量暗号 WG が設置された。

軽量暗号としてこれまで提案されてきた暗号技術には、ハードウェア実装のサイズ、消費電力量、組み込みソフトウェア実装で必要なメモリサイズ等さまざまな性能指標で最適化されたものがあり、「軽量暗号」に対して一般的に合意されている定義はない。また、性能と安全性のトレードオフもあり、実際には色々な扱いが可能な幅がある。本 WG では、以上の状況を鑑み、「実装性能と安全性のトレードオフを勘案した上で、従来の暗号技術に対して特定の性能指標で優位性（軽量性）を持つように設計された暗号技術」をスコープとし、用途が想定される代表的な性能指標に対して優位性を主張する暗号を主な対象とする。

また、現時点で、公開鍵暗号系において「軽量暗号」として広くコンセンサスがとれている方式はほとんどないため、本報告書では共通鍵暗号系の軽量暗号を対象としている。

軽量暗号が求められるアプリケーションでの要求条件のうち、本報告書では代表的な性能指標として下記に注目する。

- ハードウェア実装における
  - 回路規模
  - 消費電力量
  - レイテンシ（リアルタイム性能）
- 組み込みソフトウェア実装における
  - メモリサイズ（ROM/RAM）

ハードウェア実装の回路規模は、半導体のコストに直結し、また、消費電力 (Power) の指標にもなり得ることが知られている。回路規模の小型化は、RFID をはじめとする回路実装面積の要求条件が厳しいアプリケーションで重要な要件である。また、バッテリや外部供給電源がなく、電磁誘導等で駆動するデバイスにおいても重要な要件である。

消費電力量（Energy）の低減は、人体へ埋め込まれたり密着装備される医療機器をはじめ、バッテリで駆動するあらゆるデバイスで求められる要件である。

レイテンシ（遅延時間）は 1 回の暗号化（復号）処理に必要な時間である。低遅延性はメモリ暗号化や車載機器などのリアルタイム性が求められるアプリケーションで必須の要件である。

組み込みソフトウェア実装では、組み込みマイコン上で実現されるさまざまなアプリケーションの一部として、暗号機能を実装することが多い。組み込みマイコンでは、ROM や RAM のサイズが限られており、小さく実装できる暗号ほど、選択できるマイコンの品種が増えたり、コストを下げられる等の利点がある。組み込みマイコンは家電機器やセンサー、車載向け等で広く利用されており、実装に必要なメモリサイズ (ROM/RAM) が少ないことはこれらのアプリケーションで重要な要件である。

性能指標	アプリケーションの例
回路規模 (消費電力, コスト)	RFID、低コストセンサー
消費電力量	医療機器、バッテリ駆動デバイス
レイテンシ（リアルタイム性能）	メモリ暗号化、車載機器、産業向け I/O デバイス制御
メモリサイズ (ROM/RAM)	家電機器、センサー、車載機器

1.2 既存暗号に対して優位性をもつ分野

ここで性能指標の視点から軽量暗号が既存暗号に対して優位性を持ちうる分野について述べる。

LSI への実装を想定した回路規模の視点では、現在提案されている軽量暗号と AES の差は数 kgate 程度である。2014 年現在、モバイル向けの SoC (System on a Chip) や GPU で主流となっている 40nm 以下のプロセスで設計される LSI においては、典型的なダイサイズは 50mm^2 から 150mm^2 であり、1mm^2 あたり 1.6Mgate 程度も搭載できるため [1]、数 kgate 程度の回路規模が暗号の優劣の指標とはなりえない。これは、回路全体の 0.1% 未満に関するゲート数削減の議論となるためである。一方で、文献 [2] のミューチップのような、ダイサイズが 50μm 角 (250μm^2) クラスのチップでは数 kgate の差がクリティカルな課題となり、暗号機能の搭載可否に影響を与えうる。現時点では、このサイズのチップはアセンブリの難易度が高いため、500μm 角程度のチップが RFID では主流となっているが、このケースにおいても利用するプロセスが 180nm など古いプロセスであれば、数 kgate の回路規模の差が実装可否に影響を与える可能性がある。

また一般に、回路規模が小さいほど、消費電力あるいは消費電力量は減る傾向にある。環境発電に代表される低消費電力が求められるアプリケーションにおいては、様々な観点で低消費電力化を図る設計が必要となる。軽量暗号を利用することで消費電力あるいは消費電力量に関する設計条件を緩和する効果が期待できる。

次にレイテンシ（リアルタイム性能）の視点では、AES に対して 2 倍の応答速度をおよそ 1/10 の回路規模で実現できる軽量暗号が存在する [3]。この文献の例では、20kgate 程度の回路を用いれば 10ns 以下で暗号演算が可能とされている。一方、AES で同様のリアルタイム性能を得るためには、200kgate 使ったとしても 15ns 必要である。現時点で、産業向け I/O デバイス制御に代表されるような μs オーダーのリアルタイム性能が求められる通信路において暗号技術は利用されていないが、このようなアルゴリズムを利用することで、チップへのコストインパクトなしに暗号技術を利用できる可能性がある。

4

最後にソフトウェア実装における軽量暗号の性能指標について述べる。プログラムサイズの観点での AES に対する軽量暗号の優位性として、AES に対しておよそ 1/4 の ROM サイズで実装可能な軽量暗号が存在する [4]。この文献の例では、ルネサスエレクトロニクス社製の組み込みマイコン RL78 を用いた性能評価が行われている。RL78 は産業分野や自動車など幅広く利用されているマイコンの一つであるが、文献 [4] ではそのプラットフォーム上で 220 Bytes の ROM サイズで暗号演算が可能であることが示されている。長期間にわたって利用されてきたレガシー製品に対して、暗号機能を新たに搭載するといったアップデートを施す場合、残された ROM 領域に暗号を実装する必要があり、軽量暗号でなければ搭載できないケースが起こりうる。また、新規に暗号機能を搭載する製品を開発する場合であっても、暗号が使用する ROM 領域の削減が実現できれば、製品単価の安いチップを選定することができる。たとえば RL78 では、ROM サイズを 1KB から 512KB までの間から選ぶことができる。

2020 年にはセンサー 1 兆個、IoT 機器 500 億台の時代が到来すると言われており、前述のようなローエンドのマイコンが利用されている機器においても暗号技術が必要になることが予想される。また、自動運転が実用化され、工場やプラントがクラウドとシームレスにつながる時代が来ると予想されている。このような時代においては、現時点で暗号技術が利用されていない領域であっても、今後活用の必要性が高まると考えられる。軽量暗号は、現時点で暗号技術を搭載していない、あるいは実装上の制約から想定すらしていない機器やシステムにおいて、将来的に実装面での制約を緩和する効果を期待できる。

1.3 軽量暗号で達成可能な安全性

世の中に提案されている様々な暗号技術は様々な性能指標により評価できる。CRYPTREC では様々な暗号技術を評価し、CRYPTREC 暗号リストを維持している。CRYPTREC 暗号リストのうち、電子政府推奨暗号リスト及び推奨候補暗号リストは CRYPTREC により安全性及び実装性能が確認された方式である。これはカテゴリ毎で想定されている範囲でどのような利用がなされたとしても、安全性の問題が生じないとされており、速度などの実装性能についても実装環境毎の差が少ないバランスのよいものを意味している。もちろん、リスト中に注釈がついているものはその注釈の限定の範囲での話である。以下、この節ではそのような方式は議論対象外とする。

一方、軽量暗号は前節で述べられたように従来の暗号技術に対して特定の性能指標で優位性を持つように設計されている。それぞれの性能指標の間には一般にトレードオフが存在することから、提案されている軽量暗号の中には安全性が電子政府推奨暗号や推奨候補暗号より低くなっている方式も存在する。例えば関連鍵攻撃について安全かどうかは保証せず、その分、速度を稼いでいると主張している方式もある。とはいえ、利用場面によってはこのような高い安全性は不要であり、電子政府推奨暗号や推奨候補暗号では高い安全性が消費電力など別の性能指標の足を引っ張っている場合もあることから、安全性の一部に目をつぶった軽量暗号の方が有利な場合もある。よって軽量暗号は利用法によっては有効な技術であるが、設計者が主張するもしくは第三者による安全性評価結果については十分に注意する必要がある。

軽量暗号と謳っている方式の多くはハードウェア実装の回路規模が小さいものが多い。ブロック暗号を実装するためには、ブロック長のビット数に応じた中間状態を保持することが必須であるため、軽量ブロック暗号はブロック長として 128 ビットより小さなものが選ばれることが多い。例えば 64 ビットブロック長の暗号を CTR モードで利用した場合については、鍵を変更せずに 2^{32} ブロックすなわち 32GB 以上のデータを処理すると高い確率で無作為に選んだビット列と区別できることが知られている。さらに最近の研究 [5] によると具体的にビット列を導出できることも明らかになってきた。逆に、64 ビットブロック暗号を CTR モードで利用したとしても、ひとつの鍵で処理するデータ量が十分に小さければ、無作為に選んだビット列と区別できる確率が十分に小さいため、そのリスクを許容できる場合は効率的な利用法となり得るだろう。また、標準的ではないが CTR モードの代わりに CENC モード [6] や Abdalla-Bellare の

方法 [7] を利用することによりリスクを減らしたり回避したりできることもある。さらに、利用プロトコルもしくはシステム中で関連鍵攻撃が起きないような鍵管理がされている場合は、関連鍵攻撃耐性のない方式を使うことにより、効率をあげることが出来得る。

ブロック長に関する安全性指標については、ここにあげた通り、限界がかなりのところまで知られている。しかし、その他の安全性に関する性能指標については残念ながら分かっていないことが多い。例えば選択平文攻撃は出来ないが既知平文攻撃は想定の必要があるといった場合には明らかとなっていないことが殆んどである。暗号技術の安全性について「どんな攻撃に対しても何も起きない」といった「最強」の安全性についての評価の研究は進んでいるが、一部の軽量暗号で達成しようとしているような条件付きの安全性については研究結果が少なく、あまり明らかになっていないというのが実情である。電子政府推奨暗号や推奨候補暗号を利用したとしてもリスクなしでの運用は困難であり、軽量暗号の利用でも、利用に応じたリスクを考慮しながらの運用が必要である。また、軽量暗号といっても、全てにおいて電子政府推奨暗号や推奨候補暗号より劣っているわけではない。64 ビットブロック長なら、それに応じた安全性、関連鍵攻撃耐性を考慮しないなら、それに応じた安全性が達成されているので、必要な安全性とリスクを考慮した軽量暗号の利用が求められる。

1.4 今後の活動方針に対する提言

軽量暗号 WG では、2015 年度以降の軽量暗号に関する CRYPTREC での活動方針として、以下のような案 (A)(B)(C) を検討してきた（図 1.1 参照)。

それぞれの活動の目的と意義をまとめると下記のようになる。

(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、軽量暗号に関する情報や専門的知見を得るのに活用されることを目的とする。

(B)「暗号技術ガイドライン（軽量暗号の詳細評価)」の発行
代表的な軽量暗号アルゴリズムの安全性及び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できることを目的とする。これにより、軽量暗号の利用が促進されたり、軽量暗号に関する第三者評価レポートとして国際標準化等への寄書として活用されることが期待できる。

(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。

■今後の活動方針　軽量暗号は、特定の性能指標において既存技術と比べて優位性を持ち、M2M, IoT, CPS といった次世代のネットワークサービスを構築する上で有効なセキュリティ技術と期待される一方、電子政府推奨暗号リスト掲載の暗号技術ほど高い安全性を保証していない方式も存在しており、利用において留意すべき点がある。よって、軽量暗号を選択・利用する際の技術的判断の一助となり、今後の利用促進をはかることを目的として暗号技術ガイドラインを発行するのが有益と考えられる。

軽量暗号に関連する技術分野は多岐にわたり、分野ごとに研究開発の状況が異なる。ガイドライン作成にあたっては、詳細評価が望ましい分野や現時点では既存文献のサーベイで十分な分野など、各分野の状況を精査した上で、(A)

6

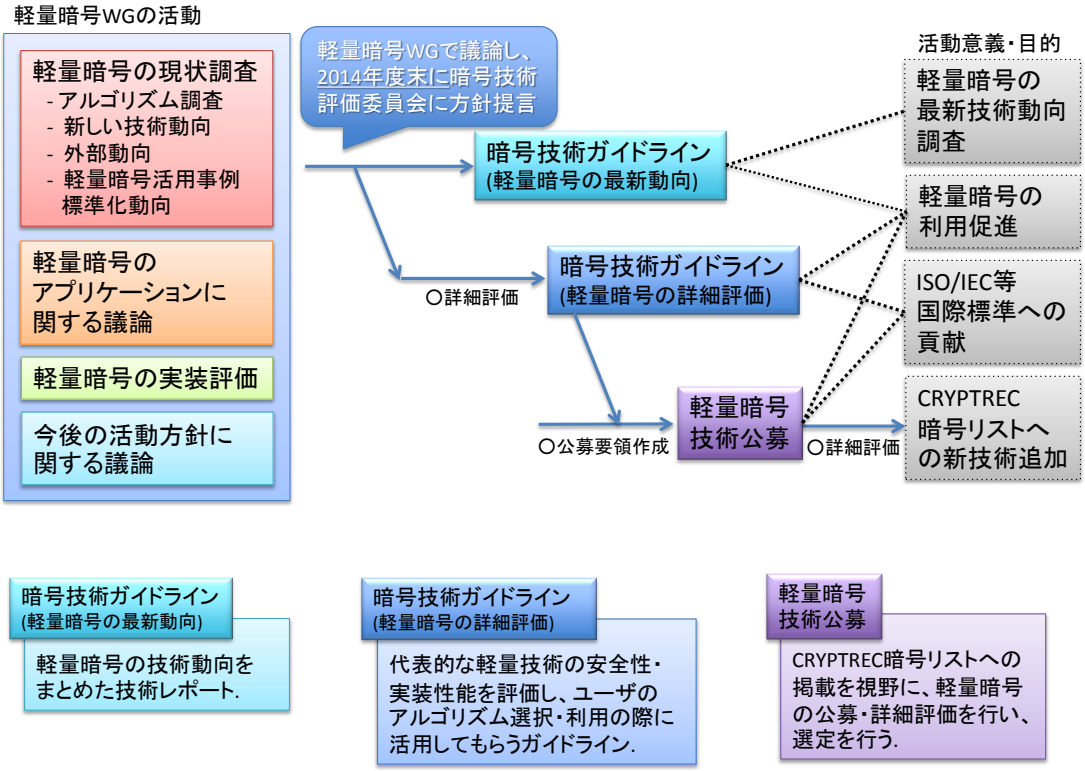


図 1.1　今後の活動方針案

と (B) のハイブリッド案でまとめるのが妥当と考えられる。詳細評価を行う技術分類は、新規評価の必要性（既存文献で十分な評価結果が得られるかどうか)、当該技術分野における我が国の技術の将来性、当該技術分野の現時点での注目度・重要度、評価結果から期待される学術的貢献等を鑑みて決定することが望ましい。

軽量暗号は、現時点では直ちに (C) の技術公募を行う段階ではないと考えるが、今後、IoT などの次世代ネットワークサービスで活用される可能性があることから、本 WG での検討が、長期的には電子政府システムの安全性向上にも資することが期待される。

参考文献

[1] STMicroelectronics, “CMP annual users meeting,” `http://cmp.imag.fr/aboutus/slides/Slides2013/05_ST_2013.pdf`, 2013.

[2] Mitsuo Usami, Hisao Tanabe, Akira Sato, Isao Sakama, Yukio Maki, Toshiaki Iwamatsu, Takashi Ipposhi and YasuoMiroslav Inoue, “A 0.05 × 0.05 mm^2 RFID Chip with Easily Scaled-Down ID-Memory,” ISSCC 2007, Digest of Technical Papers, pp. 482-483, 2007.

[3] Miroslab Kneevi, Ventzislav Nikov, and Peter Rombouts, “Low-Latency Encryption – Is “Lightweight= Light+ Wait”?” CHES 2012, pp. 426-446, 2012.

[4] Mitsuru Matsui and Yumiko Murakami, “Minimalism of Software Implementation - Extensive Performance Analysis of Symmetric Primitives on the RL78 Microcontroller,” FSE 2013, pp. 393-409, 2013.

[5] David A. McGrew, ”Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes,” preproceedings of FSE 2013, Session 4-1.

[6] Tetsu Iwata, “New Blockcipher Modes of Operation with Beyond the Birthday Bound Security”, FSE 2006, pp.310-327, 2006.

[7] Michel Abdalla, Mihir Bellare, “Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques,” ASIACRYPT 2000, pp. 546-559, 2000.

8

第 2 章

軽量暗号に関する現状調査: 軽量暗号アルゴリズム

2.1　軽量暗号に関する現状調査の概要

2013 年度および 2014 年度、軽量暗号 WG では、軽量暗号技術において、産業上のニーズがあり、具体的な暗号アルゴリズムの設計、安全性評価、実装評価が学会等で発表されている技術分類について、現状調査 (サーベイ) を行った。また、軽量暗号技術に関わる新しい技術動向や関連する外部動向についての調査や、軽量暗号の活用事例および標準化動向も行った。

これらの軽量暗号に関する現状調査を 2 章および 3 章にまとめる。

2 章の執筆担当者は下記の通りである。

第 2 章　軽量暗号アルゴリズム	
2.2 章　軽量ブロック暗号	青木委員、渋谷委員
2.3 章　軽量ストリーム暗号	渡辺委員
2.4 章　軽量ハッシュ関数	三宅委員
2.5 章　軽量メッセージ認証コード	渡辺委員
2.6 章　認証暗号	峯松委員、鈴木委員

2.2 軽量ブロック暗号

2.2.1 軽量ブロック暗号の安全性

本章では軽量暗号に分類されるブロック暗号の安全性に関する調査報告を行なう。軽量暗号に求められる安全性は暗号研究者の間でさえも合意されていない。もともと「『軽量』暗号」の名前の通り、安全性ではなく実装性能用件から始まった研究対象であり、「軽量とはいえ通常の暗号と同等の安全性が必要」という意見や、「通常利用しないような用途の安全性を犠牲にして軽量化を行なう」、また「通常利用しない用途の安全性は当然考慮せず、さらに通常使う用途に対しても長期間の安全性を保証せず、ぎりぎりを狙う」といった方式まである。従って、軽量暗号の利用に際しては、設計指針としてどこまでの安全性を考慮しているのかを理解して利用することが重要である。つまり従来型のブロック暗号の安全性と異なる部分が利用にあたって重要であることから本章では通常目的のブロック暗号に求められる安全性を調査する。

そもそも「何が『軽量ブロック暗号』か」という問に対して、軽量暗号という名前自体 buzz word と化しており難しい。広い意味で「軽量ブロック暗号」とされるものは [1] に詳しくあげられているが、AES など従来型のブロック暗号も含まれている。AES は電子政府推奨暗号であり、さらに事実上の世界標準であることから、本章では原則 AES より「軽量」なものを「軽量暗号」とした。軽量暗号の標準としては既に ISO/IEC で定められていることから ISO/IEC 29192 から中心に調査対象方式を選び、その他、共通鍵暗号の研究者の多くが「軽量」として引用している方式を調査対象とした[*1]。ここで、TDES, Camellia, CLEFIA については、平成 25 年に公表された CRYPTREC 暗号リストに掲載されており、安全性が十分に確認されている方式である。また、その後、本報告作成までの 2 年間の間に大きな問題は報告されていないので本章では調査対象外とする。

なお本章では、純粋にアルゴリズムそのものについての攻撃に対する安全性のみの調査を行ない、サイドチャネル攻撃や故障利用攻撃などは含めないこととする。また、秘密鍵の全数探索を高速化する手法、特に biclique を利用した中間一致攻撃的な手法 [4] がいくつかの暗号に対して提案されているが、効果は限定的であり、暗号の脆弱性として認められるのかどうかについても暗号研究者間で合意が得られていないのでこれも取り扱わないこととする。

表 2.1　軽量ブロック暗号の安全性評価

名称	提案文献	ブロック長	鍵長	仕様段数	攻撃可能段数	備考
LBlock	[23]	64	80	32	23	[6]
LED	[12]	64	64 ∼ 128	8/12	3/8	LED-64 と LED-128 に対応 [11]
Piccolo	[6]	64	80/128	25/31	9/11	whitening 鍵あり [17]
PRINCE	[2]	64	128	12	8	[9]
PRESENT	[5]	64	80/128	31	25(26)	26 段攻撃は全平文 [10]
PRINTcipher	[13]	48/96	80/160	48/96	48/96	[14] は弱鍵攻撃、[15] は関連鍵攻撃
TWINE	[19, 20]	64	80/128	36	23/25	[24, 21, 3]

[*1] 近年提案された Simon と Speck[8] については軽量暗号とみなされることが多い。提案論文そのものでは安全性評価が行なわれていないことから、解析論文が次々と出ている状態である。さらに、これらの方式は、パラメータが非常に多く、解析結果もそれぞれのパラメータに対して多数存在し、ここで最新情報を載せてもすぐに更新される可能性が高いことから今回は掲載を見送った。なお、現在 (2014 年 12 月) のところ、推奨パラメータでは破れていない。

参考文献

[1] Alex Biryukov and and Léo Perrin. State of the Art in Lightweight Cryptography. `http://cryptolux.org/index.php/Lightweight_Cryptography`, 2014.

[2] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225. Springer, 2012.

[3] Alex Biryukov, Patrick Derbez, and Léo Perrin. Differential Analysis and Meet-in-the-Middle Attack against Round-Reduced TWINE. *preproceedings of Fast Software Encryption Workshop 2015 (FSE 2015)*, 2015.

[4] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology — ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 344–371. Springer-Verlag, Berlin, Heidelberg, 2011.

[5] Andrey Bogdanov, Lars Ramkilde Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and Charlotte H. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems — CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer-Verlag, Berlin, Heidelberg, New York, 2007.

[6] Christina Boura, María Naya-Plasencia, and Valentin Suder. Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon. In Palash Sarkar and Tetsu Iwata editors, *Advances in Cryptology — ASIACRYPT 2014, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 179–199. Springer-Verlag, Berlin, Heidelberg, 2014.

[7] Özkan Boztas, Ferhat Karakoç, and Mustafa Çoban. Multidimensional Meet-in-the-Middle Attacks on Reduced-Round TWINE-128. LightSEC 2013.

[8] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The Simon and Speck Families of Lightweight Block Ciphers. IACR Cryptology ePrint Archive 2013/404.

[9] Anne Canteaut, María Naya-Plasencia, and Bastien Vayssière. Sieve-in-the-middle: Improved MITM attacks. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology — CRYPTO 2013, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 222–240, Berlin, Heidelberg, 2013. Springer-Verlag.

[10] Joo Yeon Cho. Linear cryptanalysis of reduced-round PRESENT. In Josef Pieprzyk, editor, *Topics in Cryptology - CT-RSA 2008: The Cryptographers' Track at the RSA Conference 2010*, volume 5985 of *Lecture*

Notes in Computer Science, pages 302–317, Berlin, Heidelberg, New York, 2010. Springer-Verlag.

[11] Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Key recovery attacks on 3-round Even-Mansour, 8-step LED-128, and full AES^2. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology — ASIACRYPT 2013, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 337–356. Springer-Verlag, Berlin, Heidelberg, 2013.

[12] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED block cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems — CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 326–341. Springer-Verlag, Berlin, Heidelberg, New York, 2011.

[13] Lars Ramkilde Knudsen, Gregor Leander, Axel Poschmann, and Matthew J. B. Robshaw. PRINTcipher: A block cipher for IC-printing. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems — CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 16–32. Springer-Verlag, Berlin, Heidelberg, New York, 2010.

[14] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A cryptanalysis of PRINTcipher: The invariant subspace attack. In Phillip Rogaway, editor, *Advances in Cryptology — CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 206–221, Berlin, Heidelberg, 2011. Springer-Verlag.

[15] Yuseop Lee, Kitae Jeong, Changhoon Lee, Jaechul Sung, and Seokhie Hong. Related-key cryptanalysis on the full PRINTcipher suitable for IC-printing. *International Journal of Distributed Sensor Networks*, 2014(Article ID 389476), 2014.

[16] David A. McGrew. Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes. In Shiho Moriai, editor, *preproceedings of Fast Software Encryption Workshop 2013 (FSE 2013)*, Singapore, 2013.

[17] 芝山直喜, 金子敏信. Piccolo の新しい高階差分特性. 信学技報 ISEC2014-34, 2014.

[18] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: An ultra-lightweight blockcipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems — CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 342–357. Springer-Verlag, Berlin, Heidelberg, New York, 2011.

[19] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE: A lightweight, versatile block cipher. In Gregor Leander and François-Xavier Standaert, editors, *ECRYPT Workshop on Lightweight Cryptography*, pages 146–169. ECRYPT II, 2011.

[20] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE : A lightweight block cipher for multiple platforms. In Lars Ramkilde Knudsen and Huapeng Wu, editors, *Selected Areas in Cryptography, 19th International Workshop, SAC 2012, Windsor, Ontario, Canada, August 15-16, 2012, Revised Selected Papers*, volume 7707 of *Lecture Notes in Computer Science*, pages 339–354, Berlin, Heidelberg, 2013. Springer-Verlag.

[21] Yanfeng Wang and Wenling Wu. Improved multidimensional zero-correlation linear cryptanalysis and applications to LBlock and TWINE. *Information Security and Privacy – 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings*, pages 1–16. 2014. Springer-Verlag.

[22] Long Wen, Meiqin Wang, Andrey Bogdanov, and Huaifeng Chen. Note of Multidimensional MITM Attack

on 25-Round TWINE-128. IACR Cryptology ePrint Archive 2014/425.

[23] Wenling Wu and Lei Zhang. LBlock: A Lightweight Block Cipher. In Javier Lopez and Gene Tsudik, *Applied Cryptography and Network Security — 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011. Proceedings*, volume 2011 of *Lecture Notes in Computer Science*, pages 327–344. Berlin, Heidelberg, 2012. Springer-Verlag.

[24] Xuexin Zheng and Keting Jia. Impossible Differential Attack on Reduced-Round TWINE. *Information Security and Cryptology – ICISC 2013*, volume 8565 of *Lecture Notes in Computer Science*, pages 123–143, 2014. Springer-Verlag.

2.2.2 軽量ブロック暗号の実装性能

本章では、軽量暗号技術の現状調査として、主要な軽量ブロック暗号アルゴリズム、および CRYPTREC 暗号リストの電子政府推奨暗号リストに含まれるブロック暗号アルゴリズムの実装性能 (ハードウェア、ソフトウェア) 調査結果をまとめる。

2.2.2.1 調査対象

調査対象とした軽量ブロック暗号アルゴリズムは、ISO/IEC 29192 軽量暗号のパート 2 ブロック暗号に記載されているブロック暗号 (PRESENT、CLEFIA)、および主要国際学会で発表されており、現段階で有力な攻撃法が発見されておらず、かつ十分な実装性能を持つと考えられるアルゴリズム (LED、Piccolo、TWINE) とした。また、参考として、CRYPTREC 暗号リストの “電子政府推奨暗号リスト” に含まれるブロック暗号 (3-key Triple DES、AES、Camellia) の実装性能も調査した。さらに、類似の実装特性を持つ低レイテンシ暗号 PRINCE の実装性能も調査した。表 2.2 にこれら調査対象アルゴリズムをまとめる。実装性能の調査を行う論文としては、十分信頼が置けるデータが得られることを考慮し、各対象アルゴリズムの提案論文、および主要国際会議で発表された論文を中心に調査を行った。調査結果については、様々な資料から得られた評価値をできる限り公平になるように並べた。しかしながら、全ての評価が同じ環境で行われているわけではなく、評価環境や実装者によって評価値が変化する可能性があるため、本調査の数値は参考程度である点に注意されたい。

表 2.2 調査対象ブロック暗号アルゴリズム基本情報

Algorithm	Block size [bit]	Key size [bit]	# rounds	Structure	Ref.
3-Key Triple DES	64	168	48	Feistel	電子政府推奨暗号
AES	128	128/192/256	10/12/14	SPN	電子政府推奨暗号
Camellia	128	128/192/256	18/24/24	Feistel	電子政府推奨暗号
PRESENT	64	80/128	31	SPN	ISO/IEC29192-2
CLEFIA	128	128/192/256	18/22/26	GFN	ISO/IEC29192-2
LED	64	64/65 128	32/48	SPN	[11]
Piccolo	64	80/128	25/31	GFN	[28]
TWINE	64	80/128	36	GFN	[30]
PRINCE	64	128	12	SPN	[6]

2.2.2.2 ハードウェア実装性能調査

ハードウェア実装性能調査としては、十分な評価が行われていると考えられる ASIC での実装性能評価を調査した。実装性能の評価指標は、大別すると、主に自身で電源を持たないような機器 (passive device) 向けの指標として消費電力 (Power)、自身で電源を持つような機器 (active device) 向けの指標として消費電力量 (Energy) の 2 つがある。このうち、消費電力 (Power) における効率を示す指標としてはゲート規模がよく知られている。一方、消費電力量 (Energy)

の効率を示す指標としては、((ゲート規模)×(1-block 処理に必要なサイクル数)/(ブロックサイズ)) によって計算される energy per bit や、(((1-cycle で処理するビット数)×10^9)/(ゲート規模)^2) によって計算される FOM(Figure of Merit) が知られている。これらの調査結果を表 2.3-2.5 にまとめる。表中、Mode は暗号化関数のみを実装している場合は Enc と記載し、暗号化関数、復号関数をともに実装している場合は Enc/Dec と記載している。また、Area の評価として用いている GE は gate equivalent の略であり、ゲート規模を表す。Cycles/block は 1-block の演算に必要なサイクル数を表し、Throughput は、100[kHz] での Throughput のみを調査している。また、表中 LED* は LED の推定値による評価結果を示している。

表 2.3　128 bit ブロック暗号のハードウェア実装性能

Algorithm	Key size [bit]	Mode	Area [GE]	Cycles/ block	Throughput @100kHz [kbps]	Tech. [μm]	Ref.
AES	128	Enc/Dec	3,400	1,032/1,165	12.4/11.0	0.35	[10]
		Enc	2,400	226	56.6	0.18	[20]
		Enc/Dec	12,454	11	1,163.6	0.13	[27]
		Enc/Dec	5,398	54	237.0	0.13	
		Enc	3,100	160	80.0	0.13	[12]
Camellia	128	Enc/Dec	6,511	44	290.9	0.13	[27]
		Enc/Dec	6,264	44	290.9	0.18	
CLEFIA	128	Enc	2,488	328	39.0	0.13	[2]
		Enc/Dec	2,604	328/320	39.0/40.0	0.13	
		Enc	2,678	176	72.7	0.13	
		Enc/Dec	4,950	36	355.6	0.09	[29]
		Enc/Dec	5,979	18	711.1	0.09	

2.2.2.3　ソフトウェア実装性能調査

ソフトウェア実装性能調査として、ハイエンド CPU、およびローエンド CPU による実装評価の調査を行った。結果を表 2.6-2.8 にまとめる。ハイエンド CPU では実行速度として、Cycles/byte (1-byte の演算に必要なサイクル数) を調査し、ローエンド CPU では、Cycles/byte、および ROM、RAM 使用量をそれぞれ調査した。表 2.6 における Type は実装手法を表しており、それぞれ、Table による表引きを主に使用した実装を Table、VPI(Vector Permute Instruction) を利用した実装を VPI、bitslice 実装を Bitslice と記述している。Bitslice 実装における block 数の記述は並列実行ブロック数を表しており、例えば 8-block と記述があるものは、8-block 並列実行の bitslice 実装を表している。また、TWINE の実装手法における Single は通常の 1-block を実行する実装手法、Double は 2-block 並列に実行する実装手法を表す。

2.2.2.4　まとめ

本章では、軽量暗号技術の現状調査として、128-bit ブロック暗号アルゴリズム AES、Camellia、CLEFIA、および 64-bit ブロック暗号アルゴリズム 3-Key Triple DES、LED、Piccolo、TWINE、PRINCE の軽量暗号用途でのハー

ドウェア、ソフトウェア実装性能を公知の論文から調査した結果をまとめた。

表 2.4　64-bit ブロック暗号のハードウェア実装性能 (flexible-key setting)

Algorithm	Key size [bit]	Mode	Area [GE]	Cycles/ block	Throughput @100kHz [kbps]	Tech. [μm]	Ref.
Triple-DES	168	Enc/Dec	5,504	48	133.3	0.13	[27]
PRESENT	80	Enc	1,000	563	11.4	0.35	[26]
			1,570	32	200.0	0.18	[5]
	128	Enc	2,587	63	101.6	0.35	[26]
			2,681	39	164.1	0.35	[26]
			1,391	559	11.4	0.18	[24]
			1,886	32	200.0	0.18	[5]
LED	64	Enc	966	1,248	5.1	0.18	[11]
	128	Enc	1,265	1,872	3.4		
LED* (推定値)	64	Enc	2,695	32	200.0	0.18	[1]
	80	Enc	1,040	1,872	3.4	0.18	[11]
		Enc	2,780	48	133.3	0.18	[1]
	96	Enc	1,116	1,872	3.4	0.18	[11]
		Enc	2,866	48	133.3	0.18	[1]
	128	Enc	3,036	48	133.3	0.18	[1]
Piccolo	80	Enc	1,048	432	14.8	0.13	[14, 28]
		Enc/Dec	1,109	432	14.8		
		Enc	1,499	27	237.0		
		Enc/Dec	1,638	27	237.0		
	128	Enc	1,338	528	12.1		
		Enc/Dec	1,397	528	12.1		
		Enc	1,776	33	193.9		
		Enc/Dec	1,942	33	193.9		
TWINE	80	Enc	1,503	36	177.8	0.09	[30]
		Enc/Dec	1,799	36	177.8		
		Enc	1,011	393	16.3		
	128	Enc	1,866	36	177.8		
		Enc/Dec	2,285	36	177.8		
PRINCE	128	Enc/Dec	3,491	12	533.3	0.13	[6]
			2,953	12	533.3	0.13	[3]
			8,577	1	6,400		

16

表 2.5　64-bit ブロック暗号のハードウェア実装性能 (fixed-key setting)

Algorithm	Key size [bit]	Mode	Area [GE]	Cycles/ block	Throughput @100kHz [kbps]	Tech. [μm]	Ref.
LED	64	Enc	688	1,280	5.0	0.18	[11]
	128	Enc	700	1,872	3.4		
LED* (推定値)	64	Enc	2,354	32	200.0	0.18	[1]
	80	Enc	690	1,872	3.4	0.18	[11]
			2,354	48	133.3	0.18	[1]
	96	Enc	695	1,872	3.4	0.18	[11]
			2,354	48	133.3	0.18	[1]
	128	Enc	2,354	48	133.3	0.18	[1]
Piccolo	80	Enc	616	432	14.8	0.13	[14, 28]
		Enc/Dec	675	432	14.8		
		Enc	1,051	27	237.0		
		Enc/Dec	1,199	27	237.0		
	128	Enc	654	528	12.1		
		Enc/Dec	721	528	12.1		
		Enc	1,083	33	193.9		
		Enc/Dec	1,249	33	193.9		

表 2.6　128-bit ブロック暗号 (AES、Camellia) のソフトウェア実装性能 (ハイエンド CPU)

Algorithm	Key size [bit]	Type	Cycles/byte	Platform	Ref.
AES	128	VPI (Enc/Dec)	6.66/9.12	Core i5 U560	[30]
			7.42/9.44	Core i7 2600S	
			10.28/12.37	Core i3 2120	
			14.72/17.82	Xeon E5620	
			12.16/14.39	Core2Quad Q9550	
			22.04/25.82	Core2Duo E6850	
		Table (Enc/Dec)	14.26/19.27	Core i5 U560	
			14.04/21.17	Core i7 2600S	
			19.03/28.68	Core i3 2120	
			31.60/42.69	Xeon E5620	
			22.74/30.94	Core2Quad Q9550	
			22.43/30.76	Core2Duo E6850	
		Bitslice (8-block)	9.32	Core2Quad Q6600	[16]
			7.59	Core2Quad Q9550	
			6.92	Core i7 920	
	128	Bitslice (1/2/16-block)	10.7/7.8/5.4	PowerPC G4	[13]
	192		12.8/9.3/6.7		
	256		14.9/10.8/7.9		
Camellia	128	Bitslice (128-block)	9.19	Core2Duo E6400	[19]

表 2.7　64-bit ブロック暗号のソフトウェア実装性能 (ハイエンド CPU)

Algorithm	Key size [bit]	Type	Cycles/byte	Platform	Ref.
PRESENT	80/128	Bitslice (8/16/32-blk)	8.46/6.52/4.73	Xeon E3-1280	[17]
			10.88/7.26/5.79	Core i7 870	
			13.55/10.98/7.55	Xeon E5410	
	80	Table/VPI/Bitslice	72.6/35.0/17.4	Core i3 2367M	[4]
			65.7/42.1/20.7	Xeon X5650	
			59.5/42.3/21.0	Core2Duo P8600	
	128	Table/VPI/Bitslice	72.5/35.0/18.9	Core i3 2367M	
			65.7/42.1/24.1	Xeon X5650	
			59.5/42.4/24.1	Core2Duo P8600	
LED	64	Table/VPI/Bitslice	76.0/36.0/12.2	Core i3 2367M	[4]
			70.9/48.1/13.1	Xeon X5650	
			62.8/47.4/14.2	Core2Duo P8600	
	128	Table/VPI/Bitslice	113.3/54.6/17.6	Core i3 2367M	
			105.9/67.4/19.0	Xeon X5650	
			93.5/68.7/20.2	Core2Duo P8600	
Piccolo	80	Bitslice (16-blk)	4.57	Xeon E3-1280	[17]
			5.69	Core i7 870	
			6.85	Xeon E5410	
	128		5.52	Xeon E3-1280	
			6.80	Core i7 870	
			8.23	Xeon E5410	
	80	Table/VPI/Bitslice	83.9/33.3/9.2	Core i3 2367M	[4]
			71.0/37.4/9.7	Xeon X5650	
			67.1/38.3/10.7	Core2Duo P8600	
	128		103.6/41.6/10.9	Core i3 2367M	
			87.5/47.4/12.5	Xeon X5650	
			83.6/47.2/13.0	Core2Duo P8600	
TWINE	80/128	Single/Double	9.47/4.77	Core i5 U560	[30]
			11.10/5.55	Core i7 2600S	
			15.06/7.55	Core i3 2120	
			13.62/6.87	Xeon E5620	
			15.16/7.93	Core2Quad Q9550	
			26.85/14.85	Core2Duo E6850	

表 2.8　ブロック暗号のソフトウェア実装性能 (ローエンド CPU)

Algorithm	Block size [bit]	Key size [bit]	ROM [byte]	RAM [byte]	Cycles/ byte [Enc/Dec]	Platform	Ref.
AES	128	128	1,912	432	125/181	ATmega163	[7]
			1,659	33	287.5/4381	ATtiny45	[9]
			970	84	7,743/10,862	RL78	[18]
			1,989	64	3,917/5,911		
			2,380	64	3,865/5,706		
Camellia	128	128	1,020	78	39,357/152,023	RL78	[18]
			2,033	64	4,337/4,477		
			2,047	74	4,125/4,244		
CLEFIA	128	128	1,309	76	18,062/18,759	RL78	[18]
			2,026	64	7,768/7,799		
			2,040	86	6,208/6,740		
PRESENT	64	80	2,398	528	1,199/1,228	ATmega163	[24]
			1,000	18	1,412.5/1,700	ATtiny45	[9]
			936	0	1,340.4/1404.3	ATtiny45	[22]
			1,794	18	1090.1/-	ATtiny45	
			426	18	11,340.6/12,728.1	ATtiny45	
			512	62	61,634/60,834	RL78	[18]
			1,009	54	13,883/14,014		
			1,855	48	9,007/8,920		
TWINE	64	80	1,304	414	271/271	ATmega163	[30]
			728	335	2,350/2,337		
			792	191	2,350/2,337		
			2,294	386	163/163		
PRINCE	64	128	2,382	220	225.4	ATtiny85	[23]

参考文献

[1] The LED block cipher, December 2013. Available from `https://sites.google.com/site/ledblockcipher/hardware`.

[2] Toru Akishita and Harunaga Hiwatari. Very compact hardware implementations of the blockcipher CLEFIA. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 278–292. Springer, 2011.

[3] Lejla Batina, Amitabh Das, Baris Ege, Elif Bilge Kavun, Nele Mentens, Christof Paar, Ingrid Verbauwhede, and Tolga Yalçin. Dietary recommendations for lightweight block ciphers: Power, energy and area analysis of recently developed architectures. In Hutter and Schmidt [15], pages 103–112.

[4] Ryad Benadjila, Jian Guo, Victor Lomné, and Thomas Peyrin. Implementing lightweight block ciphers on x86 architectures. In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, volume 8282 of *Lecture Notes in Computer Science*, pages 324–351. Springer, 2013.

[5] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher. In Paillier and Verbauwhede [21], pages 450–466.

[6] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225. Springer, 2012.

[7] Joppe W. Bos, Dag Arne Osvik, and Deian Stefan. Fast implementations of AES on various platforms. *IACR Cryptology ePrint Archive*, 2009:501, 2009.

[8] Christophe Clavier and Kris Gaj, editors. *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings*, volume 5747 of *Lecture Notes in Computer Science*. Springer, 2009.

[9] Thomas Eisenbarth, Zheng Gong, Tim Güneysu, Stefan Heyse, Sebastiaan Indesteege, Stéphanie Kerckhof, François Koeune, Tomislav Nad, Thomas Plos, Francesco Regazzoni, François-Xavier Standaert, and Loïc van Oldeneel tot Oldenzeel. Compact implementation and performance evaluation of block ciphers in ATtiny devices. In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *Progress in Cryptology - AFRICACRYPT*

2012 - 5th International Conference on Cryptology in Africa, Ifrance, Morocco, July 10-12, 2012. Proceedings, volume 7374 of *Lecture Notes in Computer Science*, pages 172–187. Springer, 2012.

[10] Martin Feldhofer, Johannes Wolkerstorfer, and Vincent Rijmen. AES implementation on a grain of sand. *Information Security, IEE Proceedings*, 152(1):13–20, 2005.

[11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED block cipher. In Preneel and Takagi [25], pages 326–341.

[12] Panu Hämäläinen, Timo Alho, Marko Hännikäinen, and Timo D. Hämäläinen. Design and implementation of low-area and low-power AES encryption hardware core. In *Ninth Euromicro Conference on Digital System Design: Architectures, Methods and Tools (DSD 2006), 30 August - 1 September 2006, Dubrovnik, Croatia*, pages 577–583. IEEE Computer Society, 2006.

[13] Mike Hamburg. Accelerating AES with vector permute instructions. In Clavier and Gaj [8], pages 18–32.

[14] Harunaga Hiwatari, Kyoji Shibutani, Takanori Isobe, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Compact hardware implementations of the ultra-lightweight block cipher Piccolo. Proceedings of the ECRYPT Workshop on Lightweight Cryptography, 2011.

[15] Michael Hutter and Jörn-Marc Schmidt, editors. *Radio Frequency Identification - Security and Privacy Issues 9th International Workshop, RFIDsec 2013, Graz, Austria, July 9-11, 2013, Revised Selected Papers*, volume 8262 of *Lecture Notes in Computer Science*. Springer, 2013.

[16] Emilia Käsper and Peter Schwabe. Faster and timing-attack resistant AES-GCM. In Clavier and Gaj [8], pages 1–17.

[17] Seiichi Matsuda and Shiho Moriai. Lightweight cryptography for the cloud: Exploit the power of bitslice implementation. In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings*, volume 7428 of *Lecture Notes in Computer Science*, pages 408–425. Springer, 2012.

[18] Mitsuru Matsui and Yumiko Murakami. Minimalism of software implementation - extensive performance analysis of symmetric primitives on the RL78 microcontroller. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 393–409. Springer, 2013.

[19] Mitsuru Matsui and Junko Nakajima. On the power of bitslice implementation on Intel Core2 processor. In Paillier and Verbauwhede [21], pages 121–134.

[20] Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang. Pushing the limits: A very compact and a threshold implementation of AES. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 69–88. Springer, 2011.

[21] Pascal Paillier and Ingrid Verbauwhede, editors. *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *Lecture Notes in Computer Science*. Springer, 2007.

[22] Konstantinos Papagiannopoulos and Aram Verstegen. Speed and size-optimized implementations of the PRESENT cipher for tiny AVR devices. In Hutter and Schmidt [15], pages 161–175.

[23] Kostas Papapagiannopoulos. High throughput in slices: The case of PRESENT, PRINCE and KATAN64

ciphers. In Nitesh Saxena and Ahmad-Reza Sadeghi, editors, *Radio Frequency Identification: Security and Privacy Issues - 10th International Workshop, RFIDSec 2014, Oxford, UK, July 21-23, 2014, Revised Selected Papers*, volume 8651 of *Lecture Notes in Computer Science*, pages 137–155. Springer, 2014.

[24] Axel Poschmann. Lightweight cryptography - cryptographic engineering for a pervasive world. *IACR Cryptology ePrint Archive*, 2009:516, 2009.

[25] Bart Preneel and Tsuyoshi Takagi, editors. *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, volume 6917 of *Lecture Notes in Computer Science*. Springer, 2011.

[26] Carsten Rolfes, Axel Poschmann, Gregor Leander, and Christof Paar. Ultra-lightweight implementations for smart devices - security for 1000 gate equivalents. In Gilles Grimaud and François-Xavier Standaert, editors, *Smart Card Research and Advanced Applications, 8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8-11, 2008. Proceedings*, volume 5189 of *Lecture Notes in Computer Science*, pages 89–103. Springer, 2008.

[27] Akashi Satoh and Sumio Morioka. Hardware-focused performance comparison for the standard block ciphers AES, Camellia, and Triple-DES. In Colin Boyd and Wenbo Mao, editors, *Information Security, 6th International Conference, ISC 2003, Bristol, UK, October 1-3, 2003, Proceedings*, volume 2851 of *Lecture Notes in Computer Science*, pages 252–266. Springer, 2003.

[28] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: an ultra-lightweight blockcipher. In Preneel and Takagi [25], pages 342–357.

[29] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-bit blockcipher CLEFIA (extended abstract). In Alex Biryukov, editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer, 2007.

[30] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE: A lightweight block cipher for multiple platforms. In Lars R. Knudsen and Huapeng Wu, editors, *Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers*, volume 7707 of *Lecture Notes in Computer Science*, pages 339–354. Springer, 2012.

2.3 軽量ストリーム暗号

本章では、軽量（lightweight）ストリーム暗号について報告する。

2.3.1 ECRYPT Stream Cipher project (eSTREAM)

eSTREAM は、EU における暗号技術研究 ECRYPT の一環として 2004〜2008 年に実施されたプロジェクトである。プロジェクトの中では、ストリーム暗号アルゴリズムの公募、および実装性能と安全性の両面から評価が行われた。eSTREAM プロジェクトでは、AES よりも性能が顕著であることを公募要件として求めており、ソフトウェア実装が高速であること (Profile I)、ハードウェア実装が軽量な暗号 (Profile II) のそれぞれの要件に特化したアルゴリズムを公募した。特にハードウェア実装の軽量性を追求した Profile II は、軽量暗号研究の流行を生んだ。CRYPTREC 軽量暗号 WG においては、low-latency 暗号など、処理速度の観点で軽量 (高速) と謳う暗号についても俎上に乗っているため、本報告では Profile I についても調査を行った。

表 2.9　eSTREAM Portfolio [1]

Profile 1 (ソフトウェア向け)	Profile 2 (ハードウェア向け)
HC-128 (128-bit), HC-256 (256-bit)	Grain-v1 (80-bit)
Rabbit (128-bit)	MICKEY 2.0 (80-bit, 128-bit)
Salsa20/12 (128-bit, 256-bit)	Trivium (80-bit)
SOSEMANUK (128-bit)	

当初の Portfolio では、Grain-128 が含まれていたが、2012 年の報告 [2] では Grain-128 を除外している。[2] によれば、Grain-128 は開発者自身がサポートしなくなったと報告されている。これは [11] で Grain-128 に弱鍵が存在する、およびセキュリティマージンが小さい、の 2 点が報告されたことが原因である。

2.3.1.1 Profile I (ソフトウェア実装が高速な暗号)

Profile I は PC、サーバ上で高速なソフトウェア向け暗号を指向しており、鍵長は 128 ビット以上である。eCRYPT II の 1 プロジェクトである VAMPIRE の成果である eBACS [9] で、さまざまな環境での処理速度を確認することができる。表 2.10 は、Intel Core i5（64 ビットモード）における評価結果である (詳細：Intel Core i5-2400S; 4 x 2495MHz; sandy, supercop-20120908)。

また、2009 TI Sitara AM3703 500MHz (ARM Cortex A8) 上での処理性能は表 2.11 のとおりである (詳細：armeabi (v7-A, Cortex A8); 2009 TI Sitara AM3703; 1 x 500MHz; h7silver, supercop-20130126)。

Profile I に属するアルゴリズムは、いずれも AES(AES-NI 不使用の場合) に比べて 3〜5 倍のスループットを実現している。AES 命令が実装されていない環境では利用に適するケースもある。現在、Salsa20 は TLS 用の暗号スイートとして提案が進められている [7]。

アルゴリズム構造は算術演算を用いるもの (Rabbit, Salsa20/12)、大きな内部状態を持ち、初期化に時間をかけるもの (HC-128, SOSEMANUK) の 2 系統に分かれる。後者のアルゴリズムは短いデータの処理には適していない。また、Profile I に属するアルゴリズムは、ハードウェア実装したときに論理規模が大きくなるケースが多いと考えられる。

HC-128, Rabbit は組み込み機器向けの SSL/TLS 実装 ChaSSL に実装されている [2]。また、Rabbit は

表 2.10　eSTREAM Portfolio Profile I アルゴリズムのソフトウェア実装性能（Intel Core i5）[8]

	処理速度 (cycle/B)				
	長いメッセージ	4096B	576B	64B	8B
HC-128	2.32	7.13	36.44	309.25	2472.00
Rabbit	4.41	4.58	5.41	13.06	80.00
Salsa20/12	2.40	2.44	2.70	4.94	56.50
SOSEMANUK	3.54	3.81	5.72	20.56	164.50
AES	11.33	11.41	11.78	15.75	77.50
KCipher-2(*)	4.01	4.22	5.50	17.45	111.51

CRYPTREC 電子政府推奨暗号との比較のため、KCipher-2 の処理性能を [14] に記載されている性能から見積もった。なお、[14] の評価環境は Intel Core2Duo である。

表 2.11　eSTREAM Portfolio Profile I アルゴリズムのソフトウェア実装性能（ARM Cortex A8）[8]

	処理速度 (cycle/B)				
	長いメッセージ	4096B	576B	64B	8B
Salsa20/12	5.52	5.84	8.14	28.50	264.75
AES	19.28	20.36	29.59	111.83	852.38

ISO/IEC 18033-4 [5] および RFC 4503 [7] に記載されている。

2.3.1.2　Profile II (ハードウェア実装規模／消費電力が小さい暗号)

Profile II は軽量なハードウェア実装向け暗号を指向しており、鍵長は 80 ビット以上である。軽量暗号の実装では、状態を保持するレジスタが論理回路の大半を占めることから、回路規模削減のために、Profile I に比べて短い鍵長を許容しているものと考えられる。鍵長 128 ビットレベルセキュリティを持つアルゴリズムに比べると、安全性が低く設定されているので、用途は限定されるべきである。

表 2.12 および図 2.1 は、文献 [10] から抜粋した Profile II (および AES) のハードウェア実装性能である。いずれのアルゴリズムも、論理規模、処理速度の両面で AES に比べて顕著な軽量性を実現している。軽量実装では、回路の動作周波数が低く抑えられているケースが多いと想定されるため、[10] では動作周波数を 10MHz, 100kHz に固定した場合の消費電力評価も行われている。消費電力はアルゴリズムによらず、論理規模に比例して増加する傾向が見られた。

2.3.2　ISO/IEC 29192-3

ISO/IEC JTC 1/SC 27 では、一般的な暗号アルゴリズムの標準を定めた ISO/IEC 18033 に加えて、軽量暗号の標準を ISO/IEC 29192 で定めている。ストリーム暗号は 2012 年に発行された Part 3 に収められており、eSTREAM Portfolio に掲載された Trivium (鍵長 80 ビット) と、CRYPTREC 推奨候補暗号に掲載された Enocoro (鍵長 80 ビットおよび 128 ビット) の 2 つのアルゴリズムが収録されている。Enocoro-80, Enocoro-128v2 のハードウェア実装性能を表 2.13 にまとめる。Trivium の実装性能については紹介済みなので割愛する。Enocoro の性能は eSTREAM Portfolio II に掲載のアルゴリズムと同程度である。消費電力に関する情報は見つかっていない。

表 2.12　eSTREAM Portfolio Profile II アルゴリズムのハードウェア実装性能 [10]

アルゴリズム	出力	最大動作周波数	スループット	論理規模	実装プロセス
	(bit/cycle)	(MHz)	(Mbps)	(kgate)	(μm)
Grain	1	724.6	724.6	1.3	0.13
	8	632.9	5063.2	2.2	
Trivium	1	327.9	327.9	2.6	
	8	471.7	3773.6	3.0	
Mickey 2.0	1	454.5	454.5	3.2	
Enocoro-80	8	274.7	2197.6	2.7	0.18
AES	2.37	131.2	311.0	5.4	0.11
	0.124	80.0	10.0	3.4	0.35

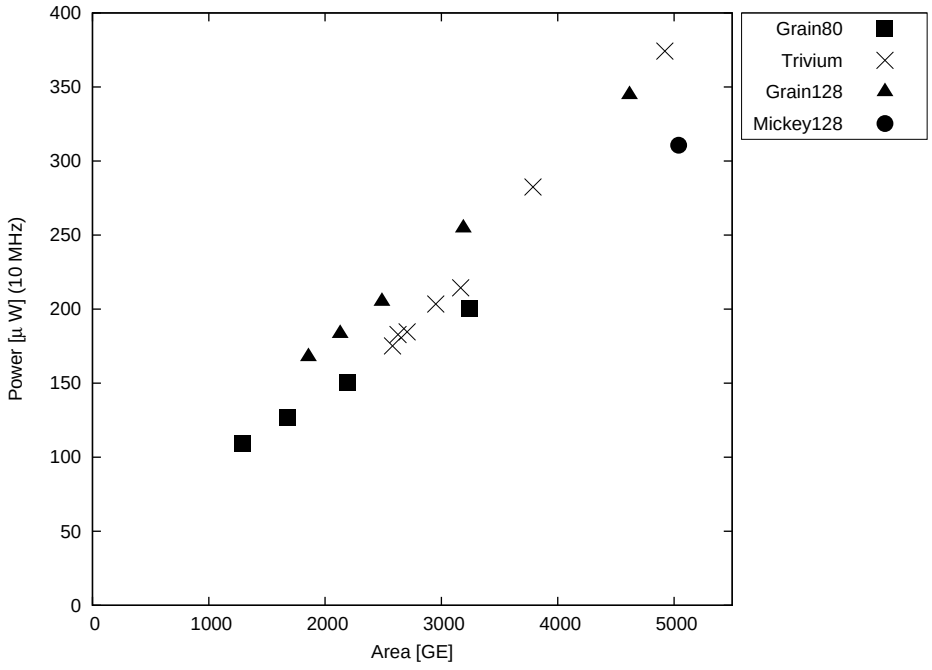


図 2.1　eSTREAM Portfolio Profile II アルゴリズムのハードウェア実装規模と消費電力 [10]

表 2.13　Enocoro のハードウェア実装性能

アルゴリズム	最大動作周波数 (MHz)	スループット (Mbps)	論理規模 (kgate)	実装プロセス (μm)
Enocoro-80 [12]	274.7	2197.6	2.7	0.18
Enocoro-128v2 [13]	440.0	3520.0	4.1	0.09

参考文献

[1] Steve Babbage, Christophe De Cannière, Anne Canteaut, Carlos Cid, Henri Gilbert, Thomas Johansson, Matthew Parker, Bart Preneel, Vincent Rijmen, and Matthew Robsha, “The eSTREAM Portfolio (rev. 1),” September 8, 2008.

[2] Carlos Cid and Matt Robshaw, The eSTREAM Portfolio in 2012, ECRYPT II, European Network of Excellence in Cryptology II, 2012.

[3] M. Robshaw and O. Billet, editors. New Stream Cipher Designs: The eSTREAM Finalists, LNCS 4986, pp. 267–293. Springer.

[4] M. Boesgaard, M. Vesterager, and E. Zenner. A Description of the Rabbit Stream Cipher Algorithm. Network Working Group, Request for Comments 4503. `http://tools.ietf.org/html/rfc4503`

[5] ISO/IEC 18033-4. Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers. 2005.

[6] ISO/IEC 29192-3:2012, Information technology – Security techniques – Lightweight cryptography – Part 3: Stream ciphers, 2012.

[7] A Description of the Rabbit Stream Cipher Algorithm, RFC4503.

[8] “The Salsa20 Stream Cipher for Transport Layer Security,” draft-josefsson-salsa20-tls-04, November 26, 2013.

[9] eBASC: ECRYPT Benchmarking of Stream Ciphers

[10] T. Good and M. Benaissa, “Hardware performance of eStream phase-III stream cipher candidates,” SASC2008, Feb 2008.

[11] I. Dinur and A. Shamir. Breaking Grain-128 with Dynamic Cube Attacks. In A. Joux, editor, Proceedings of FSE 2011, LNCS 6733, pp. 167–187, Springer, 2011.

[12] Watanabe, D., Ideguchi, K., Kitahara, J., Muto, K., Furuichi, H., Kaneko, T. “Enocoro-80: A Hardware Oriented Stream Cipher”. Third International Conference on Availability, Reliability and Security, pp. 1294–1300, IEEE Press, New York, 2008.

[13] 日立製作所, 「ストリーム暗号 Enocoro 評価書」, 2010.

[14] KDDI 研究所, 「ストリーム暗号 KCipher-2」, CRYPTREC シンポジウム 2010, 2010.

2.4 軽量ハッシュ関数

本章では、軽量暗号技術の現状調査として、代表的なハッシュ関数の安全性と実装性能に関する調査結果を報告する。

2.4.1 調査対象アルゴリズム

調査対象とするハッシュ関数アルゴリズムは、軽量ハッシュ関数として主要国際会議で提案された PHOTON、SPONGENT、QUARK、および、CRYPTREC 暗号リストに含まれる SHA-2、SHA-3 として選定された Keccak の 5 方式とする。調査文献として、SHA-2、SHA-3 については NIST の SHA-3 Competition から、その他のアルゴリズムについては提案論文や主要国際会議の論文を中心に調査した。

2.4.2 安全性

アルゴリズムの構造に基づいた Generic attacks に対する安全性に関し、各アルゴリズムの preimage attack、2nd-preimage attack、collision attack に対する計算複雑度を表 2.14 に示す。Sponge 構造である Keccak、PHOTON、SPONGENT、QUARK については、“Parameter” の “n” は hash size を、“c” は capacity を、“r” は rate を表している。Merkle-Damgard 構造である SHA-1、SHA-2 に関しては、それぞれ hash size、internal state size、message block size を表している。アルゴリズム特有の性質を利用した攻撃手法については、SHA-2 や Keccak に対しては数多くの報告があるが（CRYPTREC 技術報告書 [1],[2] 参照)、それ以外のアルゴリズムに対してはまだ十分に議論されていないため安全性に欠陥がある可能性がある。

2.4.3 ハードウェア実装性能

ハードウェア実装性能に関する調査結果を表 2.15, 2.16 に纏める。これらの評価値は様々な文献から抽出したものであり、同一環境で評価されたものではないことに注意されたい。参考情報として AES ベースのハッシュ関数の実装性能（推定値を含む）についても記載した。表中の “Area” はゲート規模を、“Latency” は internal permutation P (または internal block-cipher E) のクロック数を、“FOM(Figure of Merit)” はエネルギー効率を表す指標（スループットとゲート規模の二乗の比）を、“Power” は平均消費電力を表している（動作周波数 100kHz での性能を示す)。この結果より、軽量ハッシュ関数と呼ばれるアルゴリズムは、回路規模を数 kGE 程度に収めることを優先し、スループットはあまり高くない設計のものが多いことが分かる。

2.4.4 ソフトウェア実装性能

ソフトウェア実装性能については、軽量暗号という観点から非力な CPU（Atmel AVR ATtiny45 8-bit RISC microcontroller）での性能を示した CARDIS2012 の発表論文 [12] を引用する（表 2.17)。

2.4.5 まとめ

CRYPTREC 暗号リストに記載の SHA-2 と SHA-3 として選定された Keccak、および軽量ハッシュ関数に分類される PHOTON、SPONGENT、QUARK について、提案論文を中心に安全性と実装性能について調査した。軽量ハッシュ関数は 64〜128 ビットセキュリティの安全性での実装性能を重視したものが多く、ハードウェア実装性能において

表 2.14　各アルゴリズムの安全性

Algorithm	Hash [bit]	Parameter[bit] n	c	r	Security[bit] Pre	2nd-Pre	Col	Source
SHA-1	160	160	160	512	160	160	80	[8]
SHA-256	256	256	256	512	256	256	128	[8]
Keccak-f[200]*1	128	200	128	72	128	128	64	[5]
Keccak-f[400]*1	160	400	256	144	160	160	80	[5]
PHOTON-80	80	80	80	20	64	40	40	[8]
PHOTON-128	128	128	128	16	112	64	64	[8]
PHOTON-160	160	160	160	36	124	80	80	[8]
PHOTON-224	224	224	224	32	192	112	112	[8]
PHOTON-256	256	256	256	32	224	128	128	[8]
SPONGENT-88	88	88	80	8	80	40	40	[10]
SPONGENT-128	128	128	128	8	120	64	64	[10]
SPONGENT-160	160	160	160	16	144	80	80	[10]
SPONGENT-224	224	224	224	16	208	112	112	[10]
SPONGENT-256	256	256	256	16	240	128	128	[10]
U-QUARK	128	136	128	8	128	64	64	[11]
D-QUARK	160	176	160	16	160	80	80	[11]
S-QUARK	224	256	224	32	224	112	112	[11]

SHA-2 と比較すると、回路規模の面で大きな優位性があるものの、速度面では必ずしも優れているわけではなく、レイテンシは勝るものもあるがスループットに関しては概ね劣っていることが分かった。以上の観点から、今回調査した軽量ハッシュ関数は、特に回路規模に制限があるデバイスや低レイテンシが要求されるアプリケーションでの利用が適していると考えられる。

*1 Keccak-f[] は置換関数であることに注意

表 2.15　ハードウェア実装性能

Algorithm	Area [GE]	Latency [clk]	Throughput [kbps]	FOM	Power [uW]	Proc. [nm]	Source
SHA-1	6,812	450	113.78	24.52	11.0	250	[3]
SHA-256	8,588	490	104.48	14.17	11.2	250	[4]
KECCAK-f[200]	2,520	900	8.00	12.60	5.60	130	[5]
	4,900	18	400.0	166.6	27.6	130	[5]
KECCAK-f[400]	5,090	1,000	14.40	5.56	11.5	130	[5]
	10,560	20	720.00	64.57	78.1	130	[5]
KECCAK-f[1600]	20,790	1,200	90.66	2.10	44.9	130	[5]
	47,630	24	4,533	19.98	315.1	130	[5]
AES-based DM scheme-128	>4,400	-	<12.4	-	-	-	[7]
AES-based Hirose scheme-256	>9,800	-	<12.4	-	-	-	[7]
PHOTON-80/20/16	865	708	2.82	37.73	1.59	180	[8]
	1,168	132	15.15	111.13	2.70	180	[8]
	1,067	708	2.82	24.77	14.0	45	[9]
	1,567	132	15.15	61.70	39.9	45	[9]
PHOTON-128/16/16	1,122	996	1.61	12.78	2.29	180	[8]
	1,708	156	10.26	35.15	3.45	180	[8]
	1,394	996	1.61	8.29	17.2	45	[9]
	2,172	156	10.26	21.75	49.6	45	[9]
PHOTON-160/36/36	1,396	1332	2.70	13.87	2.74	180	[8]
	2,117	180	20.00	44.64	4.35	180	[8]
	1,741	1332	2.70	8.91	19.4	45	[9]
	2,849	180	20.00	24.64	65.8	45	[9]
PHOTON-224/32/32	1,735	1716	1.86	6.19	4.01	180	[8]
	2,786	204	15.69	20.21	6.50	180	[8]
	2,142	1716	1.86	4.05	22.6	45	[9]
	3,586	204	15.69	12.20	78.8	45	[9]
PHOTON-256/32/32	2,177	996	3.21	6.78	4.55	180	[8]
	4,362	156	20.51	10.78	8.38	180	[8]
	2,675	996	3.21	4.49	51.6	45	[9]
	5,335	156	20.51	7.21	248.	45	[9]

30

表 2.16　ハードウェア実装性能 (続)

Algorithm	Area [GE]	Latency [clk]	Throughput [kbps]	FOM	Power [uW]	Proc. [nm]	Source
SPONGENT-88	738	990	0.81	14.9	1.57	130	[10]
	1,127	45	17.78	139	2.31	130	[10]
	869	990	0.81	10.7	16.5	45	[9]
	1,237	45	17.78	116	38.7	45	[9]
SPONGENT-128	1,060	2,380	0.34	3.03	2.20	130	[10]
	1,687	70	11.43	40.2	3.58	130	[10]
	1,257	2,380	0.34	2.15	21.1	45	[9]
	1,831	70	11.43	34.1	53.2	45	[9]
SPONGENT-160	1,329	3,960	0.40	2.26	2.85	130	[10]
	2,190	90	17.78	37.1	4.47	130	[10]
	1,572	3,960	0.40	1.62	24.6	45	[9]
	2,406	90	17.78	30.7	73.5	45	[9]
SPONGENT-224	1,728	7,200	0.22	0.7	3.73	130	[10]
	2,903	120	13.33	15.8	5.97	130	[10]
	2,070	7,200	0.22	0.5	31.4	45	[9]
	3,220	120	13.33	12.9	96.0	45	[9]
SPONGENT-256	1,950	9,520	0.17	0.45	4.21	130	[10]
	3,281	140	11.43	10.6	6.62	130	[10]
	2,323	9,520	0.17	0.32	34.2	45	[9]
	3,639	140	11.43	8.63	110.	45	[9]
U-QUARK	1,379	544	1.47	7.73	2.44	180	[11]
	2,392	68	11.76	20.6	4.07	180	[11]
	1,744	544	1.47	4.83	51.2	45	[9]
	3,215	68	11.76	11.4	89.4	45	[9]
D-QUARK	1,702	704	2.27	7.84	3.10	180	[11]
	2,819	88	18.18	22.9	4.76	180	[11]
	2,200	704	2.27	4.69	58.6	45	[9]
	3,695	88	18.18	13.3	87.7	45	[9]
S-QUARK	2,296	1,024	3.13	5.94	4.35	180	[11]
	4,640	64	50.0	23.2	8.39	180	[11]
	3,001	1,024	3.13	3.48	81.6	45	[9]
	6,155	64	50.0	13.2	146	45	[9]

表 2.17　ソフトウェア実装性能

Algorithm	Digest size [bits]	Code size [bytes]	RAM data [bytes]	RAM state & others [bytes]	RAM stack	Cycle count (8byte msg)	Cycle count (50byte msg)	Cycle count (100byte msg)	Cycle count (500byte msg)
SHA-256	256	1090	64	73	6	33,600	33,600	66,815	266,105
Keccak[r =40, c =160]	160	752	5	45	3	58,063	162,347	278,269	1,205,627
Keccak[r =144, c =256]	256	608	18	92	4	90,824	181,466	317,221	1,313,291
Keccak[r =1088, c =512]*	256	868	136	240	4	178,022	178,022	179,494	716,483
PHOTON-160/36/36	160	764	9	39	11	620,921	1,655,364	2,793,265	11,999,914
PHOTON-256/32/32	256	1,244	4	68	10	254,871	486,629	787,896	3,105,396
SPONGENT-160/160/80	160	598	10	60	6	795,294	2,783,241	4,771,186	20,674,746
SPONGENT-256/256/128	256	364	16	96	5	1,542,923	3,856,916	6,170,900	25,454,100
D-QUARK	176	974	2	42	5	631,871	1,516,685	2,570,035	10,996,835
S-QUARK	256	1106	4	60	5	708,783	1,417,611	2,339,023	9,427,023

参考文献

[1] 盛合志帆, ハッシュ関数の安全性に関する技術調査報告書, CRYPTREC 技術報告書 No.0213, http://www.cryptrec.go.jp/estimation.html#2004, 2004.

[2] 金子敏信, SHA-256/-384/-512 の評価報告, CRYPTREC 技術報告書 No.0503, http://www.cryptrec.go.jp/estimation.html#2005, 2005.

[3] Mooseop Kim and Jaecheol Ryou, Power Efficient Hardware Architecture of SHA-1 Algorithm for Trusted Mobile Computing. In Sihan Qing, Hideki Imai, and Guilin Wang, editors, *Information and Communications Security, 9th International Conference — ICICS 2007*, volume 4861 of *Lecture Notes in Computer Science*, pages 375-385, Springer-Verlag, Berlin, Heidelberg, 2007.

[4] Mooseop Kim, Jaecheol Ryou, and Sungik Jun, Efficient Hardware Architecture of SHA-256 Algorithm for Trusted Mobile Computing. In Moti Yung, Peng Liu, and Dongdai Lin, editors, *Information Security and Cryptology — ISC 2008*, volume 5487 of *Lecture Notes in Computer Science*, pages 240-252, Springer-Verlag, Berlin, Heidelberg, 2009.

[5] Elif Bilge Kavun and Tolga Yalcin, A Lightweight Implementation of Keccak Hash Function for Radio-Frequency Identification Applications, In Siddika Berna Ors Yalcin, editor, *Radio Frequency Identification: Security and Privacy Issues — RFIDsec 2010*, volume 6370 of *Lecture Notes in Computer Science*, pages 258-269, Springer-Verlag, Berlin, Heidelberg, 2010.

[6] Luca Henzen, Pietro Gendotti, Patrice Guillet, Enrico Pargaetzi, Martin Zoller, and Frank K. Gürkaynak, Developing a Hardware Evaluation Method for SHA-3 Candidates, In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems — CHES 2012*, volume 6225 of *Lecture Notes in Computer Science*, pages 248-263, Springer-Verlag, Berlin, Heidelberg, 2010.

[7] Andrey Bogdanov, Gregor Leander, Christof Paar, Axel Poschmann, Matt J. B. Robshaw, and Yannick Seurin, Hash Functions and RFID Tags: Mind the Gap, In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems — CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, pages 283-299, Springer-Verlag, Berlin, Heidelberg, 2008.

[8] Jian Guo, Thomas Peyrin, and Axel Poschmann, The PHOTON Family of Lightweight Hash Functions, In Phillip Rogaway, editor, *Advances in Cryptology — CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 222-239, Springer-Verlag, Berlin, Heidelberg, 2011.

[9] Andrey Bogdanov, Miroslav Knežević, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede, SPONGENT: The Design Space of Lightweight Cryptographic Hashing, volume 62, issue 10, pages 2041-2053, IEEE Transactions on Computers, 2013.

[10] Andrey Bogdanov, Miroslav Knežević, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede,

SPONGENT: A Lightweight Hash Function, In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems — CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 312-325, Springer-Verlag, Berlin, Heidelberg, 2011.

[11] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, Mara Naya-Plasencia, Quark: A Lightweight Hash, In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems — CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 1-15, Springer-Verlag, Berlin, Heidelberg, 2010.

[12] Josep Balasch, Barış Ege, Thomas Eisenbarth, Benoit Gérard, Zheng Gong, Tim Güneysu, Stefan Heyse, Stéphanie Kerckhof, François Koeune, Thomas Plos, Thomas Pöppelmann, Francesco Regazzoni, François-Xavier Standaert, Gilles Van Assche, Ronny Van Keer, Loïc van Oldeneel tot Oldenzeel, and Ingo von Maurich, Compact Implementation and Performance Evaluation of Hash Functions in ATtiny Devices, In Stefan Mangard, editor, *Smart Card Research and Advanced Applications — CARDIS 2012*, volume 7771 of *Lecture Notes in Computer Science*, pages 158-172, Springer-Verlag, Berlin, Heidelberg, 2013.

2.5 軽量メッセージ認証コード

本章では、軽量なメッセージ認証コード (Message Authentication Code: MAC) に関する調査報告を行う。

MAC は、nonce 入力の有無によって、probabilistic MAC と deterministic MAC に分けられる。nonce 入力を持つ probabilistic MAC は、リプレイ攻撃に耐性を持つ。また、Wegman と Carter が提案した、universal hash function から MAC を構成する方法 [9] は nonce 入力が必須である。universal hash function をベースとする MAC は、代数的演算を用いることを特徴としてお、64 ビットレジスタ上での演算などを高速に行うことができる実装環境では優れた処理性能を発揮する。

一方、ブロック暗号から構成する CMAC [18] や、ハッシュ関数から構成する HMAC [2, 26] は deterministic MAC として定義される（nonce を prefix とすることで probabilistic MAC として用いることもできる)。このような、暗号プリミティブからモードとして MAC を定義する場合、実装環境に合わせて軽量な暗号プリミティブを使用することで、軽量な MAC となることが期待できる。

2.5.1 universal hash function を用いる構成法

Wegman と Carter により、ユニバーサルハッシュ関数 h から安全な MAC を構成できることが知られている [27]。Wegman-Carter 方式による MAC の構成は $MAC(m,k,r) = h(m,k) + b(r)$ で定義される。ただし、ここで $b(r)$ は one-time key である。主要なユニバーサルハッシュ関数はいずれも代数的な演算で構成されており、これらの演算が高速に実行できる環境では優れた処理性能を実現する。

まず、Wegman らが提案した多項式を用いる方式 (polynomial hashing) では、ユニバーサルハッシュ関数は $h(m,k) = \sum_i m_i k^i$ で定義される。polynomial hashing のアルゴリズム例として GMAC [13] や Poly1305 [3] がある。GMAC の演算は標数 2 の拡大体 GF(2^{128}) 上で、また、Poly1305 の演算は素体 $GF(2^{130}-5)$ 上で定義される。Saarinen は GMAC に弱鍵があることを指摘している [25]。また、Procter らは、この脆弱性が多項式の取り方に依らず存在すること、および任意の鍵を弱鍵と見做せることを示した [24]。しかし、Procter の攻撃では、弱鍵を検出する識別子のメッセージ長と、弱鍵の空間の大きさが等価であるため、現実的な脅威ではないと考えられる。

[15] によれば、Intel Haswell アーキテクチャ上では GMAC (GHASH) の漸近的な処理速度は 0.4 cycle/Byte である。また、表 2.18 は、[4] で提供されている Poly1305-AES の処理性能から抜粋したものである。

表 2.18　Poly1305-AES の処理速度 [4](単位：cycles/Byte)

	データ長			
	64	256	1024	long
Pentium III	16.3	6.9	5.1	4.4
Pentium 4	18.7	8.0	5.3	4.5
Athlon	13.1	5.7	3.7	3.2

また、Halevi と Krawczyk は内積を用いる方式 MMH を提案した [17]。MMH はメッセージ $m = \{m_1, \ldots, m_n\}$ と等長の鍵ストリーム $k = \{k_1, \ldots, k_n\}$ に対して $h(m,k) = \sum_i m_i \cdot k_i$ 定義される。UMAC [7] や Badger [8] は MMH と同じく内積方式であるが、MMH が有限体上の演算を用いて定義されているのに対して、ソフトウェア実装に適した $Z/2^wZ$ 上の演算を用いる点が異なる。

MMH 方式では、一般に鍵をメッセージと等長のビット列に伸長して内積を計算する。したがって、他の方式に比べて事前処理に要するコストが大きくなる。また、拡大鍵を保持するためのメモリ使用量が増大する傾向にあり、複数の相手と通信を行うようなケースでは、メモリを圧迫する可能性がある。[7] や [8] では、安全に拡大鍵を使い回す方法や、tree-hash との組み合わせにより拡大鍵の量を削減する方法が紹介されている。

表 2.19 は、[21] で報告されている UMAC の処理性能である。報告されている数値からの推定になるが、UMAC の性能には、少くとも鍵を伸長する事前処理は含まれていないと考えられる。

表 2.19　Pentium 4 上での UMAC の処理速度 [21](単位：cycles/Byte)

	データ長			
タグ長	64	256	1024	long
32	8.3	2.4	0.9	0.6
64	12.0	3.5	1.4	1.0
96	15.1	4.5	1.9	1.5

また、表 2.20 は [8] で報告されている、タグ長が 64 ビットの Badger の処理速度である。

表 2.20　Pentium III および Pentium 4 上での Badger の処理速度 [8]

	事前処理	メッセージ処理	最終処理
Pentium III	4,093 cycles	2.2 cycles/Byte	433 cycles
Pentium 4	5,854 cycles	1.3 cycles/Byte	800 cycles

上に挙げた方式の実装性能はいずれも、CPU が 64 ビットアーキテクチャやベクトル演算を利用可能な環境、もしくは多大な事前計算テーブルをメモリに展開できる環境において実現されたものであり、計算機能力が貧弱な環境には適していない可能性が高い。

2.5.2　暗号プリミティブを用いる構成法

暗号プリミティブから MAC を構成する方法として、ブロック暗号から構成する CMAC [18] や、ハッシュ関数から構成する HMAC [2, 26] がある。ISO/IEC 9797 [28, 29] には、CMAC や HMAC の他にも、CBC-MAC のバリエーションなどが規定されている。Bertoni らが [5] でスポンジ関数を提案して以降、置換をベースとする暗号機能の研究がさかんになった。MAC の構成法としては、secret-prefix 方式が一般的であり、Bertoni らにより、その安全性が証明されている [6]。多くの軽量ハッシュ関数はスポンジ関数から構成されているので、上記の secret-prefix 方式を用いることが可能である。スポンジ関数の secret-prefix 方式は最終処理が不要であるため、メッセージ長が短い場合には、HMAC に比べて処理時間が短いことが期待される。

暗号プリミティブが疑似ランダム関数 (疑似ランダム置換) であることを利用するのではなく、その写像の一様性のみを利用する方式も存在する。Daemen らは、メッセージ処理を行う関数として、AES のラウンド関数 4 段 (鍵無し) を用いる Pelican を提案した [10, 11]。Pelican 2.0 [11] の安全性は証明されていない。しかし、現実的な攻撃も報告されていない。Minematsu らは、同じく AES のラウンド関数 4 段 (鍵付き) を用いる PC-MAC-AES を提案した [22]。PC-MAC-AES は、ベースとなる関数の最大差分確率を前提として安全性が証明されている。したがって、安全性の

観点では、Pelican よりも PC-MAC-AES が優れている。いずれのアルゴリズムも、AES 以外の軽量ブロック暗号をベースに構成することが可能であるが、事前に最大差分確率の評価が必須である。

実装性能では、Pelican や PC-MAC-AES は、いずれも漸近的な性能が CMAC-AES の 2.5 倍である。ただし、いずれも事前処理や最終処理に AES の暗号化 1 回以上の処理を行うため、メッセージ長が短い場合にはアドバンテージが小さくなる。また、PC-MAC-AES の処理速度は拡大鍵の量とトレードオフの関係にあり、漸近的な処理速度に近づくためには、メモリ使用量が増大する。したがって、実装性能の観点では Pelican が優位である場合が多い。

これらの他に、独自の暗号プリミティブを用いる方式として、Mouha らは非線形置換を用いる Chaskey を提案した [23]。Chaskey は 1-key Even-Mansour ブロック暗号の CMAC と解釈することが可能である。また、非線形置換は Skein, SipHash [1] と同様、ARX 演算をベースにしている。事前処理、最終処理が無いため、短いメッセージに対して効率的であると考えられる。表 2.21 は [23] で報告されている、Chaskey の処理速度である。

表 2.21　Cortex-M 上での Chaskey の処理速度 (cycles/Byte) [23]

	データ長	
	16	128
Cortex-M0	21.3	18.3
Cortex-M3/M4	10.6	7.0

参考文献

[1] Jean-Philippe Aumasson and Daniel J. Bernstein. “SipHash: A Fast Short-Input PRF”. *INDOCRYPT*, LNCS 7668, pages 489–508, Springer, 2012.

[2] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. “Keying Hash Functions for Message Authentication”. *Advances in Cryptology, CRYPTO'96*, LNCS 1109, pages 1–15, Springer, 1996.

[3] Daniel J. Bernstein. “The Poly1305-AES Message-Authentication Code”. *Fast Software Encryption, FSE'05*, LNCS 3557, pages 32–49, Springer, 2005.

[4] Daniel J. Bernstern. “Poly1305-AES speed tables”. `http://cr.yp.to/mac/speed.html`.

[5] Gyido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche, “Sponge functions,” ECRYPT Hash Workshop, May 2007.

[6] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche, “On the security of the keyed sponge construction”. *Symmetric Key Encryption Workshop, SKEW'11*, 2011.

[7] John Black, Shai Halevi, Hugo Krawczyk, Ted Krovetz, and Phillip Rogaway. “UMAC: Fast and Secure Message Authentication”. *Advances in Cryptology, CRYPTO'99*, LNCS 1666, pages 216–233. Springer, 1999.

[8] M. Boesgaard, T.Christensen and E. Zenner, “Badger – A fast and provably secure MAC.” *Applied Cryptgraphy and Network Security*, LNCS 3531, pagets 176–191, Springer, 2005.

[9] J. Lawrence Carter and Mark N. Wegman. “Universal Classes of Hash Functions”. *J. Comput. Syst. Sci.*, 18(2):143–154, 1979.

[10] Joan Daemen and Vincent Rijmen. “A New MAC Construction ALRED and a Specific Instance ALPHA-MAC”. *Fast Software Encryption, FSE'05*, LNCS 3557, pages 1–17, Springer, 2005.

[11] Joan Daemen and Vincent Rijmen. “The MAC Function Pelican 2.0”. *IACR Cryptology ePrint Archive*, 2005:88, 2005. `https://eprint.iacr.org/2005/088.pdf`.

[12] Morris Dworkin. “Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication”. NIST special publication 800-38b, May 2005. `http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf`.

[13] Morris Dworkin. “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC”. NIST special publication 800-38d, November 2007. `http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf`.

[14] Shimon Even and Yishay Mansour. “A Construction of a Cioher From a Single Pseudorandom Permutation”. *Advances in Cryptology, ASIACRYPT*, LNCS 739, pages 210–224. Springer, 1991.

[15] Shay Gueron. “AES-GCM software performance on the current high end CPUs as a performance baseline for CAESAR competition.” *Directions in Authenticated Ciphers, DIAC 2013*. 2013.

[16] Niels Ferguson. "Authentication weaknesses in GCM". Comments submitted to NIST Modes of Operation Process, May 2005.

[17] Shai Halevi and Hugo Krawczyk, "MMH: Software message authentication in the Gbit/second rate". *Fast Software Encryption, FSE'97*, LNCS 1267, pages 172–189, Springer, 1997.

[18] Tetsu Iwata and Kaoru Kurosawa. "OMAC: One-Key CBC MAC". *Fast Software Encryption, FSE'03*, LNCS 2887, pages 129–153. Springer, 2003.

[19] Antoine Joux. "Authentication Failures in NIST version of GCM". Comments submitted to NIST Modes of Operation Process, June 2006.

[20] Ted Krovetz. "Message Authentication on 64-Bit Architectures". *Selected Areas in Cryptography*, LNCS 4356, pages 327–341. Springer, 2006.

[21] Ted Krovetz. "UMAC Performance". `http://web.cs.ucdavis.edu/~rogaway/umac/2004/perf04.html`

[22] Kazuhiko Minematsu and Yukiyasu Tsunoo. "Provably Secure MACs From Differentially-uniform Permutations and AES-based Implementations," *Fast Software Encryption, FSE'06*, LNCS 4047, pp. 226–241, 2006.

[23] Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. "Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers." *Selected Areas in Cryptography, SAC'14*, 2014.

[24] Gordon Procter and Carlos Cid. "On Weak Keys and Forgery Attacks Against Polynomial-Based MAC Schemes," *Fast Software Encryption, FSE'13*, LNCS 8424, pp. 287–304, Springer, 2014.

[25] Markku-Juhani O. Saarinen. "Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes." *Fast Software Encryption, FSE'12*, 2012.

[26] James M. Turner. "The Keyed-Hash Message Authentication Code (HMAC)". FIPS PUB 198-1, National Institute of Standards and Technology, July 2008. `http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf`.

[27] Mark N. Wegman and J. Lawrence Carter. "New Hash Functions and Their Use in Authentication and Set Equality". *J. Comput. Syst. Sci.*, 22(3):265–279, 1981.

[28] ISO/IEC 9797-1:2011, Information technology – Security tecniques – Message authentication codes (MACs) – Part 1: Mechanisms using a block cipher, 2011.

[29] ISO/IEC 9797-2:2011, Information technology – Security tecniques – Message authentication codes (MACs) – Part 2: Mechanisms using a dedicated hash-function, 2011.

[30] ISO/IEC 9797-3:2011, Information technology – Security tecniques – Message authentication codes (MACs) – Part 3: Mechanisms using a universal hash function, 2011.

2.6 認証暗号

2.6.1 認証暗号の安全性

2.6.1.1 はじめに

共通鍵暗号を用いて、送りたい平文の暗号化と、改ざん検知のための認証タグの付与とを同時に行う、認証暗号（Authenticated Encryption, AE）と呼ばれる機能が知られている。本章では、AE について、特に安全性の側面から調査した結果を報告する。

まず、AE の形式的な定義、およびその安全性の概念として知られているものを整理し 2.6.1.2 章で報告する。基本的に AE の安全性は、暗号文が平文の関する情報をどれだけ隠しているか（秘匿性）と、不正な暗号文をどれだけ正確に検知できるか（真正性）の二つの軸で評価されている [7, 46]。ただし、これらを複合した単一評価軸の存在や、平文以外の入力変数である初期ベクトルなどの形式、生成モデルの違いによりいくつかバリエーションを生じている。これらの違いを意識した安全性の比較が必要である。

次に 2.6.1.6 章以降にて具体的な構成方法を紹介する。AE の構成方法は多岐にわたり、特に用いる暗号学的プリミティブによって全体構成が大きく変化する。ここではもっとも普及しているアプローチの一つである、ブロック暗号をベースとした方式、すなわちブロック暗号利用モード（以下モード）により実現される方式に絞って説明を行い、これらが満たす安全性を示す。

2.6.1.2 認証暗号の形式と安全性

■基本的な入出力　まず、認証暗号の入出力について解説する。認証暗号の処理は一般に暗号化と復号からなる。秘密鍵 K を共有する 2 者間において、暗号化関数の入力は、もっとも典型的な場合、

- 初期ベクトル（Initial Vector, IV）N
- 平文 M
- ヘッダ H

となる。ここで、初期ベクトル N は暗号化のために補助的に用いる変数であり、通常暗号文と共に通信される（従って受信側は初期ベクトルを同期する必要がない)。初期ベクトルの長さは固定の場合も可変長の場合もある。典型的な生成方法は乱数によるものか、暗号化側が保持し、逐次更新する状態変数（カウンターなど）を用いるもの、あるいはその両方の組み合わせによるものである。

平文 M は暗号化の対象となる情報であり、一般に可変長の系列である。

ヘッダ H は associated data (AD) とも呼ばれ、暗号化はされないものの改ざんは防ぎたい情報のことを指す。例えば通信プロトコルのバージョン、パラメータ、中継ポイントでのルーティング情報などがある。こちらも一般に可変長の系列である。

なお厳密にはヘッダの存在しない方式を AE と呼び、ヘッダがある方式を AEAD（AE with AD）と呼ぶことがあるが、本稿では区別せず AE と呼ぶ。AEAD は方式によってはヘッダが存在せず、長さ 0 の変数と解釈して処理を行うことが可能であり、その意味では AE を包含する概念といえる。さらに、平文 M が存在しない場合を認める方式もあり、この場合の意図する処理はヘッダ H に対する、IV 付きのメッセージ認証コード（Message Authentication Code, MAC）となる。

暗号化処理の出力は、

- 暗号文 C
- タグ T

となる。暗号文 C の長さは通常 M と同じであり、タグ T は固定長である。送信する情報は (N, A, C, T) の 4 つ組となる。

復号処理の入力は上記 4 つ組であり、出力結果は、もし送信された情報が改ざんされていないと判断（受理）された場合には復号された平文 M となり、改ざんがあったと判断した場合は、単一のエラーメッセージとなる。

■入出力形式のバリエーション　基本的な AE には IV は必須であるが、方式によってはこれを不要とするものがある。例えば ANSI のスマートメータ関連規格（C12.22）において定義されている EAX-prime という方式では、IV とヘッダを組み合わせた変数を Cleartext と呼んでいる。また、いわゆる Deterministic AE (DAE), On-line AE (OAE) と呼ばれる AE のクラスにおいては、IV は存在せず、もし存在する場合には暗黙にヘッダに含まれるものとされていることが多い。

2.6.1.3　安全性の概念 – IV 付きの場合

上述のように、安全性の概念は典型的に秘匿性（Privacy）と完全性（Authenticity・Integrity）に分けて説明される。秘匿性とは、送信内容である (N, A, C, T) を得た攻撃者が元の平文 M に対する情報を得ることの困難性を表す指標であり、より端的には、暗号化関数の出力である (C, T) と同じ長さの乱数との判別困難性をもって表される。完全性とは、攻撃者が改ざんに成功することの困難性を表す指標である。ここで、改ざんとは、観測した正規の (N, A, C, T) とは異なる $(N', A', C', T') \neq (N, A, C, T)$ を、鍵を知ることなく生成し、これを受信者が受理する事象を指す。完全性は改ざん成功確率を攻撃者のクラスに関して最大値をとることで評価される。

よりフォーマルに記載するために、以下の表記を導入する。まず、$\mathcal{A}^{O_1, O_2, \ldots, O_c}$ を攻撃者 $\mathcal{A}$ が c 個のオラクル $O_1, \ldots, O_c$ に任意の順序でアクセスする環境を示すものとする。次に $\mathsf{AE}[\tau]$ を、τ-bit のタグを持つ AE であるとし、その暗号化と復号の関数をそれぞれ $\mathsf{AE}\text{-}\mathcal{E}_\tau$ と $\mathsf{AE}\text{-}\mathcal{D}_\tau$ とする。秘匿性の定義は以下で与えられる。まず $\mathsf{AE}[\tau]$ への nonce-respecting な q 選択平文攻撃とは $\mathsf{AE}\text{-}\mathcal{E}_\tau$ に対して $(N_1, H_1, M_1), \ldots, (N_q, H_q, M_q)$ を逐次的・適応的に与えて、$(C_1, T_1), \ldots, (C_q, T_q)$ を得ることをいう。ただしどの $i < j$ についても $N_i \neq N_j$ となることが条件である。ここで \$ を、(N, H, M) が与えられたもとで常に (C, T) と同じ長さの乱数を返す、ランダムビットオラクルであるとする。すると AE へ nonce-respecting な選択平文を行う攻撃者 $\mathcal{A}$ に対する PRIV アドバンテージは

$$\mathtt{Adv}^{\mathtt{priv}}_{\mathsf{AE}[\tau]}(\mathcal{A}) \stackrel{\text{def}}{=} \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathsf{AE}\text{-}\mathcal{E}_\tau} \Rightarrow 1] - \Pr[\mathcal{A}^{\$} \Rightarrow 1].$$

と定義される。

次に完全性を定義する。$\mathcal{A}$ が $\mathsf{AE}[\tau]$ に対する選択暗号文攻撃を行う場合、$\mathsf{AE}\text{-}\mathcal{E}_\tau$ と $\mathsf{AE}\text{-}\mathcal{D}_\tau$ の両方に任意の順序でアクセスできる。$\mathcal{A}$ は nonce-respecting な選択平文クエリを $\mathsf{AE}\text{-}\mathcal{E}_\tau$ へ行うが、$\mathsf{AE}\text{-}\mathcal{D}_\tau$ には IV に関する制約はない。つまり暗号化クエリで用いた IV を復号クエリに用いてもよいし、復号クエリで重複した IV を用いてもよい。ただし自明な答えが返ってくる、暗号化で聞いた結果をそのまま復号に与えることだけは禁じる。このような攻撃者 $\mathcal{A}$ について、AE の完全性は、

$$\mathtt{Adv}^{\mathtt{auth}}_{\mathsf{AE}[\tau]}(\mathcal{A}) \stackrel{\text{def}}{=} \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathsf{AE}\text{-}\mathcal{E}_\tau, \mathsf{AE}\text{-}\mathcal{D}_\tau} \text{ forges }]$$

で定義される。ここで右辺は、エラーシンボルである $\perp$ 以外を $\mathsf{AE}\text{-}\mathcal{D}_\tau$ から得るのイベントの確率を指す。

なお PRIV/AUTH といった表記については論文によっては異なる名称をとる場合もあるので注意が必要である。後述の IV なしのケースについても同様。

2.6.1.4 安全性の概念 – IV なしの場合

■Deterministic AE　IV が存在しない場合、暗号化の入力が (H, M)（もし H が存在すれば）で、出力が (C, T)、送信内容が (H, C, T) となる。また復号処理は (H, C, T) を入力とし、受理すれば M を出力、そうでなければ $\perp$ 出力となる。

このような AE の安全性については、大きく二つのバリエーションがある。一つ目は、Privacy については、平文の一致情報以上は漏らさないことを求める方式である。Authenticity については (H, C, T) に対する改ざん困難性を要求する。この概念は最初に Rogaway と Shrimpton によって提案され、Deterministic AE (DAE) と呼ばれることから、DAE security とも呼ばれている。

IV 付きの場合と同様に PRIV/AUTH で評価する場合について述べる。まず秘匿性は、$\mathsf{AE}[\tau]$ を DAE とみなし、AE-$\mathcal{E}_\tau$ へクエリ (H, M) を重複して行わない $\mathcal{A}$ について,

$$\mathtt{Adv}^{\mathtt{dpriv}}_{\mathsf{AE}[\tau]}(\mathcal{A}) \stackrel{\text{def}}{=} \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathsf{AE}\text{-}\mathcal{E}_\tau} \Rightarrow 1] - \Pr[\mathcal{A}^{\$} \Rightarrow 1]$$

で評価する。一方完全性は IV 付きのケースと同様

$$\mathtt{Adv}^{\mathtt{dauth}}_{\mathsf{AE}[\tau]}(\mathcal{A}) \stackrel{\text{def}}{=} \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathsf{AE}\text{-}\mathcal{E}_\tau, \mathsf{AE}\text{-}\mathcal{D}_\tau} \text{ forges }],$$

で評価する。DAUTH の forge の意味は、non-trivial な復号のクエリ (H, C, T)（すなわち (H, M) を暗号化クエリして (C, T) を得ていない）について $\perp$ 以外のレスポンスを得ることを指す。それぞれの指標を DPRIV, DAUTH とここでは呼ぶことにする。なお Rogaway と Shrimpton は同時にこの二つをまとめた指標として DAE-advantage を提案している。これは、

$$\mathtt{Adv}^{\mathtt{dae}}_{\mathsf{AE}[\tau]}(\mathcal{A}) \stackrel{\text{def}}{=} \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathsf{AE}\text{-}\mathcal{E}_\tau, \mathsf{AE}\text{-}\mathcal{D}_\tau} \Rightarrow 1] - \Pr[\mathcal{A}^{\$, \perp} \Rightarrow 1]$$

という指標である。これは、攻撃者が DAE の暗号化と復号に両方アクセスできるもとで、自明な質問をしないで、random-bit oracle と $\perp$-oracle (常に $\perp$ を返すオラクル）の組と、実際の DAE 暗号化、復号の組との判別を行う困難性を示すものである。両者は基本的に等価な関係にあり、DPRIV と DAUTH（の上界）が求まれば、DAE-advantage の上界が求まり、またその逆も可能であることが示されている [48]。単一指標のほうがシンプルな表現ではあるが、従来指標との整合性、および実際の証明手続きを考えると、二軸での指標にも実用的価値が見いだせると思われる。

DPRIV が求めるものは、本質的に暗号文のどのビットも平文全体の情報を反映することであり、従って DAE には原理上平文全体を読み込まない限り暗号文の最初のブロックが計算できず、従ってオンライン処理（1 パス処理）が不可能である。

■On-line AE　もう一つのケースが、秘匿性において異なる平文間の prefix の一致だけ漏れることを許容し、それより後ろは漏らさない、とするものである。このような機能は一般的に On-line Cipher と呼ばれ、Bellare らの研究 [5] に端を発するものである。認証暗号として完全性も満たすよう拡張された方式も提案されており、On-line AE (OAE) と呼ばれている。

まず秘匿性は、$\mathsf{AE}[\tau]$ を OAE とみなし、AE-$\mathcal{E}_\tau$ へクエリ (H, M) を重複して行わない $\mathcal{A}$ について,

$$\mathtt{Adv}^{\mathtt{opriv}}_{\mathsf{AE}[\tau]}(\mathcal{A}) \stackrel{\text{def}}{=} \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathsf{AE}\text{-}\mathcal{E}_\tau} \Rightarrow 1] - \Pr[\mathcal{A}^{\$^O} \Rightarrow 1]$$

で評価する。一方完全性は IV 付きのケースと同様

$$\mathtt{Adv}^{\mathtt{oauth}}_{\mathsf{AE}[\tau]}(\mathcal{A}) \stackrel{\text{def}}{=} \Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\mathsf{AE}\text{-}\mathcal{E}_\tau, \mathsf{AE}\text{-}\mathcal{D}_\tau} \text{ forges }],$$

で評価する。本質的に等価な別の定義として、$\mathtt{Adv}^{\mathtt{oauth}}$ はまた、$\perp$ を常にエラーシンボル $\perp$ を返すオラクルと定義したうえで、$(\mathsf{AE}\text{-}\mathcal{E}_\tau, \mathsf{AE}\text{-}\mathcal{D}_\tau)$ と $(\mathsf{AE}\text{-}\mathcal{E}_\tau, \perp)$ との判別のアドバンテージと定義されることもある [11]。

なお $\$^O$ は random-bits on-line oracle と呼ばれる、prefix が一致する部分のみ同じ乱数を返すオラクルである。より正確には、ヘッダが同じ二つの入力 (H, M), (H, M'), $M \neq M'$ について、M, M' を n-bit ブロックに分割した表現を $M = M[1], \ldots, M[m]$, $M' = M'[1], \ldots, M'[m']$ とし、Length of Longest common prefix (LLCP) を、$\mathrm{LLCP}_n(M, M') = \max_i\{M[1], \ldots, M[i] = M'[1], \ldots, M'[i]\}$ とする。対応する暗号文が $C = C[1], \ldots, C[m]$, $C' = C'[1], \ldots, C'[m']$ のとき、$\mathrm{LLCP}_n(M, M') = i$ なら まず $C[1], \ldots, C[i] = C'[1], \ldots, C'[i]$ がランダムに選択され、残りの系列が独立かつランダムに選ばれる。このようなオラクルは過去のクエリを保持しその都度サンプリング (lazy sampling) を行うことで実現可能である。

また、Fleischmann ら [11] は DAE のケースと同様に、OPRIV と OAUTH をまとめた指標である CCA3-security を提案し、OPRIV と OAUTH との等価性を説明している。

DAE とは異なり、OAE は秘匿性の部分は On-line cipher と同等の安全性要件と同じであるため、オンライン処理が可能である。

■Nonce-misuse との関連　DAE, OAE ともに、IV がヘッダの一部に含まれているケースを考えることが可能である。この場合、上記の安全性基準は、IV が nonce として暗号化に用いられている限りは通常の IV 付き AE の安全性を保証し、IV の重複が暗号化で発生する場合には DAE/OAE 本来の安全性が保証される、ということを意味する。この性質は、特に DAE について Rogaway と Shrimpton により Misuse-resistent AE (MRAE) [48] と呼ばれているが、OAE に関しては達成できる安全性が DAE よりも弱いため、OAE も含めて MRAE と呼称すべきかどうかについては議論がある（例えば CAESAR メーリングリスト [1] の議論参照)。

2.6.1.5　計算量的仮定

上記の安全性概念・基準を達成するにあたり、用いられるブロック暗号に対する計算量的仮定としては以下のものがある。ブロック暗号のブロックサイズを n ビット、またその暗号化関数を E_K, 復号関数を D_K とすると、

- 疑似ランダム関数（Pseudorandom Function, PRF)：選択平文攻撃において n-bit ランダム関数との計算量的判別困難性を有する鍵付き関数。
- 疑似ランダム置換（Pseudorandom Permutation, PRP)：選択平文攻撃において n-bit ランダム置換との計算量的判別困難性を有する鍵付き関数。
- 強疑似ランダム置換（Strong Pseudorandom Permutation, SPRP)：選択暗号文攻撃において n-bit ランダム置換との計算量的判別困難性を有する鍵付き関数。
- 関連鍵安全性（Related-key Security)：攻撃者が関連鍵を入力できる環境における、上記の計算量仮定のいずれか。例えば定数 c を鍵差分として入力できる PRP の場合、$K, K' = K \oplus c$ においてペア $(E_K, E_{K'})$ と ペアの独立なランダム置換 $(\mathsf{P}, \mathsf{P}')$ の判別困難性を意味する。

2.6.1.6　方式説明における記法

次節から具体的な方式を取り上げ、それらの概略と、証明可能安全性について述べる。AE の実現方法は多様であるため、ここではブロック暗号をベースとした暗号利用モードにより実現されている例を中心に取り扱う。仕様の解説はおおまかなものにとどめる。また、安全性の評価を簡潔にするため、以下ではすべて n-bit ブロック暗号を用いるものとし、

- q：暗号化クエリの回数
- q_v：復号クエリの回数
- σ_p：暗号化のクエリ (N, A, M) のトータルのブロック長
- σ_a：暗号化のクエリ (N, A, M) および復号のクエリ (N, A, C, T) のトータルのブロック長
- τ：タグのビット長

というパラメータ群を用いて攻撃者 $\mathcal{A}$ を定義し、$\mathcal{A}$ に対する安全性評価指標（バウンド）を表すことにする。攻撃者 $\mathcal{A}$ の計算量を便宜的に t とするが、本稿におけるバウンドの式では陽には現れないため省略する。また特段断らない限り、バウンド中の定数は略すこととする。実際の定数、および具体的なパラメータの設定においては、必要に応じて引用文献を参照のこと。認証暗号方式 XXX について、$\mathtt{XXX}[E, \tau]$ を、用いるブロック暗号が E で、タグ長が τ ビットとした実現例とする。多くの場合 $1 \leq \tau \leq n$ である。また、$\mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}')$, $\mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{A}')$ を $\mathcal{A}$ から求まる $\mathcal{A}'$ による、E に対する疑似ランダム置換、および強疑似ランダム置換との判別可能性を表すものとする。$\mathcal{A}'$ のパラメータは、計算量を含め $\mathcal{A}$ から決まるため方式ごとに定義が必要だが、以下では、$\mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}')$ 中の $\mathcal{A}'$ はすべて $O(\sigma_p)$（定数は一般に小さい）回の CPA クエリを行う、計算量 $O(t\sigma_p)$ の攻撃者となる。同様に $\mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{A}')$ 中の $\mathcal{A}'$ はすべて $O(\sigma_a)$ 回の CCA クエリを行う、計算量 $O(t\sigma_a)$ の攻撃者となる。使うブロック暗号の鍵の数が 2 以上の場合、一般的にこれらの項にも係数が出てくるが、こちらも省略するものとする。

2.6.1.7 IV 付き、レート 2 の方式

平文 M の 1 ブロックあたりの処理に必要なブロック暗号の回数をレートと呼ぶことにする。このような方式は、一般的に安全な暗号化のモード（カウンターモードなど）とメッセージ認証コード（CMAC など）を異なる鍵で適切に組み合わせることで構成可能であり、これを generic composition と呼ぶ。以下で説明するものの中には generic composition と類似した構成も含まれるが、鍵が共通であるため、generic composition の安全性結果（[6, 41] など）を直接引用することはできない。

■CCM　設計者: Housley, Whiting, Ferguson により 2002 年に作られた [54]。
構成：CBC-MAC で (N, H, M) を処理して中間タグ T' を生成したのち、N および H, M の長さ情報からカウンターモード暗号化の IV を生成し、M と T' を連結した系列を暗号化し、暗号文 C とタグ T とする。いわゆる MAC-then-Enc という generic composition の形式をとる（ただし鍵は単一である）。このため、本質的に On-line 処理ができない。IV 長は 1 ブロック未満に制限されている。また、CBC-MAC 入力のフォーマットが本来不要な複雑さを持つ、という問題がある。
安全性：Johnson [23] により以下の安全性証明がなされている。

$$\mathtt{Adv}^{\mathtt{priv}}_{\mathrm{CCM}[E,\tau]}(\mathcal{A}) \leq \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n}$$
$$\mathtt{Adv}^{\mathtt{auth}}_{\mathrm{CCM}[E,\tau]}(\mathcal{A}) \leq \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n} + \frac{q_v}{2^\tau}$$

つまり、クエリの総ブロック長が $2^{n/2}$ より十分小さく、復号クエリの回数が 2^τ より十分小さい限り、CCM は PRIV/AUTH の双方の意味において、用いるブロック暗号の疑似ランダム性に帰着される安全性を有するといえる。

このタイプのバウンドは IV 付き AE の中でもっともよく見られるものである。

■GCM　設計者: McGrew と Viega により 2004 年に作られた [30]。
構成：$n = 128$-bit のブロック暗号によるカウンターモード GCTR と、有限体 $\mathrm{GF}(2^n)$ 上の乗算を用いたユニバーサ

ルハッシュ関数である GHASH とを組み合わせている。全体構成としては Enc-then-MAC の構成に近い。IV N は任意長をとれるが、特に $|N| = 96$ の場合、$I = N$ とし I の下 32-bit をインクリメントした値を初期値とした GCTR で M を暗号化し C を得たのち、GHASH を (A, C) へ適用し、$E_K(I)$ との XOR によりタグ T を生成する。これ以外の長さでは $I = \mathrm{GHASH}(N)$ としたのち同様の処理を行う。なお、処理量としては平文 m ブロック、ヘッダ a ブロック、IV x ブロックにつき $m + 1$ 回のブロック暗号コール、$a + m + x$ 回の GF 乗算を必要とする。乗算のコストと実装規模（コードサイズ、事前計算量など）は無視できないため、ブロック暗号のレートとしては 1 であるが、トータルの計算コスト、実装規模は下記のレート 1 の方式と同等ととらえることはできない。

安全性：当初、McGrew, Viega により安全性証明がなされた [31] が、後に岩田らにより誤りが発見され、成功確率は現実的ではないが理論的攻撃が示された [20]。これは 96-bit 以外の IV を用いる時にカウンタ衝突確率の上界評価が当初の証明より大幅に増加することを利用している。同時に、証明の誤りを修正した以下のバウンドが示された。

$$\mathtt{Adv}^{\mathtt{priv}}_{\mathrm{GCM}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n} + \frac{2^{22} q \sigma_p \ell_N}{2^n}$$
$$\mathtt{Adv}^{\mathtt{auth}}_{\mathrm{GCM}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n} + \frac{2^{22} (q + q_v) \sigma_a \ell_N}{2^n} + \frac{q_v \ell_A}{2^\tau}$$

ただし ℓ_N と ℓ_A は暗号化および復号で用いた最大の IV ブロック長と、最大のヘッダブロック長である。上記のバウンドは特別に大きい係数 2^{22} のみ省略せずに記載している。またこの係数は IV を 96-bit に固定することで 1 とすることが可能であるため、安全性を確保する上ではこの設定が望ましい。

■EAX　設計者：Bellare, Rogaway, Wagner により 2004 年に作られた [7]。
構成：CMAC で N を処理した結果 $\widetilde{N}$ を初期値としたカウンターモードで M を暗号化し、C を得たのち、H, C を個別に CMAC で処理した結果の XOR をとり、さらに $\widetilde{N}$ との XOR もとることでタグ T を生成する。N は任意の可変長変数である。CMAC は 3 回コールされるが、それぞれ最初に異なる定数ブロックを挿入することで、独立な疑似ランダム関数として振る舞うようにしている。いわゆる MAC-then-Enc という generic composition の形式をとるが、鍵は単一である。
安全性：Bellare, Rogaway, Wagner により安全性証明がなされている。この証明は AUTH のバウンドが $q_v = 1$ のケースについてのみ扱っており、汎用的な変換方法を用いて $q_v \ge 1$ のケースのバウンドに変換すると、次数 3 の項 $\sigma^2 q_v / 2^n$ が出現するためバースデーバウンドではなくなることが知られていたが、最近峯松らの結果により改善された [36]。ここでは改善されたバウンドで示す。

$$\mathtt{Adv}^{\mathtt{priv}}_{\mathrm{EAX}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n}$$
$$\mathtt{Adv}^{\mathtt{auth}}_{\mathrm{EAX}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n} + \frac{q_v}{2^\tau}$$

■CLOC と SILC　設計者：Iwata, Minematsu, Guo, Morioka による CLOC [17, 16] と、Iwata, Minematsu, Guo, Morioka, Kobayashi による SILC [18, 19] がある。いずれも CFB と CBC-MAC との組み合わせをベースとし、事前計算を要する入力マスクを無くし、実行中に必要なメモリ量を減らす構造をとり、また 64-bit ブロック暗号の利用も定義するなど、ローエンドデバイスでの動作を意識した方式となっている。CLOC は組み込みソフトウェアを、SILC は小規模ハードウェアを主なターゲットとおいている。安全性：CLOC は [17, 16] により、SILC は [19] により、下記のタイプの標準的なバースデーバウンド安全性が示されている。また、AUTH に関しては Nonce が暗号化で再利用されても安全性が保証されるという特徴を持つ。

$$\mathtt{Adv}^{\mathtt{priv}}_{\mathrm{CLOC}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n}$$
$$\mathtt{Adv}^{\mathtt{auth}}_{\mathrm{CLOC}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n} + \frac{q_v}{2^\tau}$$

$$\mathtt{Adv}^{\mathtt{priv}}_{\mathrm{SILC}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n}$$
$$\mathtt{Adv}^{\mathtt{auth}}_{\mathrm{SILC}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n} + \frac{q_v}{2^\tau}$$

■CHM と CIP　ここまで示したのはすべて $2^{n/2}$ ブロックの質問によりバウンドが 1 になり安全性保証がなくなる、安全性に関していわゆるバースデー限界のある方式である。一方岩田 [15, 14] により、バースデー限界を超えた安全性を保証する方式が提案されている。CHM と CIP の二つがあり、いずれもカウンターモードの変種である CENC と、代数的なユニバーサルハッシュ関数との組み合わせである。カウンターモードは鍵ストリーム系列と乱数との判別が $O(2^{n/2})$ ブロック出力させることで可能となるのに対し、CENC は周期的にブロック暗号を追加コールし、その結果をカウンターモード出力へ加算することでバースデー限界を超えた安全性を保証するものである。正整数 w を用いて周期を 2^w（2^w ブロックおきに追加のコールを行う）とした場合、CENC のレートは $1 + 1/2^w$ となり、安全性のバウンドはおおよそ $\sigma^3/2^{2n} + \sigma/2^n$ となる。w は大きいほうがレートが下がるが安全性バウンドと事前計算量などに影響を及ぼすため、$n = 128$ のときは $4 \sim 8$ 程度が推奨される。CHM と CIP についてもほぼ同様の安全性バウンドが得られる。暗号化のレートもほぼ CENC 同様だが、平文ブロック数の GF(2^n) 乗算を要するため、前述のルールに従うとレートは $2 + 1/2^w$ となる。

2.6.1.8　IV 付き、レート 2 未満の方式

■OCB　設計者：正確には 3 つのバージョンが知られており、OCB1,2,3 と呼称される。OCB1 は Rogaway [47] により 2001 年に, OCB2 は同じく Rogaway [45] により 2004 年に、OCB3 は Krovetz と Rogaway [26] により 2011 年に作られた。

構成：ECB 暗号化の上下のブロックをマスク系列で XOR している。マスク系列は、IV N と何番目のブロックかを表すインデックス $i = 1, 2, \ldots$ とをブロック暗号で処理して、i についてシーケンシャルに生成する。平文 M をマスク付き ECB 暗号化した出力が暗号文 C となり、タグ T は平文の全ブロックの XOR（チェックサムと呼ばれる）を特別なマスクを入力側に付けた 1 ブロック ECB で暗号化することで得られる。これはヘッダが存在しないときの処理であり、ヘッダがある場合、並列実行可能な MAC である PMAC をヘッダに適用した結果と上記の T との XOR をタグとする。PMAC は上記のマスク付き ECB の出力全ブロックの XOR をもう一度マスク付き 1 ブロック ECB 暗号化するものである。復号においてはマスク付き ECB の復号をしたのち、得られた平文のチェックサムを暗号化して、タグとの一致をチェックする。この処理にはブロック暗号の復号関数を要する。この構造により、レート 1 を達成している。

OCB の各バージョンでマスク系列生成方式に違いがある。OCB1,3 は Gray code をベースとしており、基準となる n 個のブロック値をブロック暗号を用いて事前計算し、Gray code が示す順序に従って基準のブロック値を逐次的に XOR していくことでマスクを生成するのに対し、OCB2 はほぼ事前計算なしに逐次的に GF(2^n) 上の 2 倍算を繰り返すことでマスクを生成する。

安全性：各提案論文 [47, 45, 26] によりそれぞれのバージョンの安全性証明がなされている。基本的にはいずれも以下

の形で示される。

$$\mathtt{Adv}^{\mathtt{priv}}_{\mathrm{OCB}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n}$$
$$\mathtt{Adv}^{\mathtt{auth}}_{\mathrm{OCB}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n} + \frac{q_v}{2^\tau}$$

ただし、調査した限りでは、OCB1 のみ上記の AUTH バウンドにおいて $q_v = 1$ のケースしか示されていないようである。

なお、最近の結果として、青木と安田 [3] により、OCB の各バージョンとも強疑似ランダム置換よりも弱い条件に帰着できることが示された。上記のバウンドにおいて PRIV は PRP のみで証明できることはほぼ自明であるが、[3] によると、AUTH においてもブロック暗号復号の結果に対する予測不能性（系列全体がランダムでなくとも満たしうる性質）があればよいことが分かる。

■類似方式　ほぼ OCB1 と同時期に発表された方式として Julta [25] による IAPM, IACBC, Gligor, Donescu [12] による XCBC がある。これらは構造的には OCB と同じ（もしくは ECB の内部にさらにブロック間のチェインを挟むものもある）であるが、マスク生成の部分に関して OCB がもっとも洗練されているといえる。

OCB と類似した構造で、マスクを用いずに ECB のブロックをチェインさせて、すなわち CBC 暗号化のような処理を行ってレート 1 の AE を達成しようとする試みもある（例えば PCBC とその変種 [33, 38], IOBC [39],IOC [44]）。OCB 以前に考えられた方法が多い。また [39] によるとそのほぼすべてに攻撃が発見されており、現在のところ安全性証明が与えられた方式はないとみられる。

■CCFB　設計者: Lucks [28] により 2005 年に作られた。
構成：ブロック暗号の入出力の一部のみを用いた CFB モードにより暗号化を行う。CFB で使われない入力部分は処理ブロックのインデックスが与えられ、出力部分は逐次的に XOR をとることでチェックサムとしている。ヘッダが存在しない基本的なバージョンでは、CFB のチェイン値の初期値は IV である。ヘッダが存在するバージョンを CCFB+H と呼ぶが、このバージョンでは、ヘッダを（0^n プリペンドした）CMAC へ適用した結果と IV の XOR をチェインの初期値とする。IV は 1 ブロックの値である。暗号化が終わった時点のチェイン値を暗号化し、チェックサムとの XOR を行いタグとする。タグの長さを τ ビットとすると、チェックサムの長さもこれと等しい。またチェイン値を a-bit とすると $a + \tau = n$ を満たすこととなる。例えば $n = 128$ のケースで $a = 96$, $\tau = 32$ とすることが提案されている。センサーネット系のメッセージ認証コードは 32-bit タグのケースが多く、そのようなケースにフィットすると考えられる。上記の構造により、ブロック暗号 1 回につき a-bit 平文を処理可能であるため、レートは n/a となる。例えば $a = (2/3)n$, $\tau = (1/3)n$ とするとレートは 1.5 となる。原理上は $n/(n-1)$ まで 1 に近づけられるが、タグの短さは AUTH バウンドの劣化に直結するため、適切なバランスを取る必要がある。並列処理が不可能であるが、1 パス暗号化が可能であり、逐次的な処理には適している[*2]。また OCB と異なり、ブロック暗号の暗号化関数のみを用いる。

安全性：Lucks [28] により以下の安全性証明がなされている。

$$\mathtt{Adv}^{\mathtt{priv}}_{\mathrm{CCFB}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^a}$$
$$\mathtt{Adv}^{\mathtt{auth}}_{\mathrm{CCFB}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^a} + \frac{1}{2^\tau}$$

ただし AUTH は $q_v = 1$ のケースを扱っている。

[*2] ただし論文のタイトルには Two-pass とある。

■復号関数を用いない方式　OCB がブロック暗号の復号関数を用いるのに対し、レート 1 を保持したままブロック暗号の暗号化関数のみで全体を構成しようとする試みがある。Liting らの iFeed [55, 1] は CBC 暗号化に似た形式（より具体的には暗号化が CBC 復号に類似）を持ち, レート 1 であるが復号が並列処理できない。峯松の OTR [35, 1] では 2 ラウンドフェイステル置換の構造を取り入れることで、2 ブロック単位での並列化が暗号化と復号で可能となっている。いずれも下記に示す標準的なバースデーバウンドの安全性を有している。ブロック暗号の強擬似ランダム性は必要とせず、擬似ランダム性のみを必要とする点が OCB とは異なる。iFeed の安全性証明は Liting ら [56] に記載されている。

$$\mathtt{Adv}^{\mathtt{priv}}_{\mathrm{iFeed}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n}$$
$$\mathtt{Adv}^{\mathtt{auth}}_{\mathrm{iFeed}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n} + \frac{q_v}{2^\tau}$$

また OTR に関しては [35, 34] に記載されている。

$$\mathtt{Adv}^{\mathtt{priv}}_{\mathrm{OTR}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n}$$
$$\mathtt{Adv}^{\mathtt{auth}}_{\mathrm{OTR}[E,\tau]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n} + \frac{q_v}{2^\tau}$$

2.6.1.9　On-line AE 方式

■McOE　設計者: Fleischmann, Forler, Lucks, Wenzel [11] により 2012 年に作られた。
構成：Bellare らによる On-line cipher [4, 5] のアイディアをベースとした構成である。Rogaway と Zhang による、Tweakable ブロック暗号 [27] を用いた On-line cipher の構成方法 TC3 [49] に、さらにメッセージ認証の機能を追加した構成ともとらえることができる。

McOE ではまず、n-bit ブロック暗号 E_K をベースに、n-bit tweak, n-bit ブロックを持つ Tweakable ブロック暗号 $\widetilde{E}_K$ を構成する。構成方法は二つあり、それぞれ McOE-G, McOE-X と呼ばれる。McOE-X で用いる $\widetilde{E}_K$ では、tweak と鍵の XOR により tweak を処理する。具体的には E_K の鍵長 $|K| = n$ であり、平文 M, Tweak T について暗号文は $C = \widetilde{E}_K(T, M) = E_{K \oplus T}(M)$ となる。McOE-G で用いる $\widetilde{E}_K$ では、GF(2^n) 上の要素 X と Y の乗算 $H_Y(X)$ を用いる。具体的には、$|K| = 2n$ であり、$K = (K_1, K_2)$, $|K_i| = n$ と分けたのち、平文 M, Tweak T について暗号文は $C = \widetilde{E}_K(T, M) = E_{K_1}(M \oplus H_{K_2}(T)) \oplus H_{K_2}(T)$ となる。このようにして構成された $\widetilde{E}_K$ を用いて、TC3 の暗号化である Tweak chaining を行う。これは i 番目の平文ブロック $M[i]$ について暗号文ブロック $C[i]$ を $\widetilde{E}_K(S[i], M[i])$ とするものである。$S[i]$ はチェインさせる tweak であり、$S[i+1] = M[i] \oplus C[i]$ として更新する。初期値 $S[0]$ は 0^n である。タグの生成には、最初にヘッダを Tweak chaining で暗号化した結果（の最終ブロック）を Z とし、平文の後ろに Z を連結したのち Tweak chaining で暗号化した結果得られる最終ブロックをタグ T とする。なお平文がブロックサイズの等倍におさまらない場合は、tag-splitting と呼ばれる処理をさらに導入する必要がある（CBC 暗号化における Ciphertext stealing と呼ばれる処理に近い）。タグの長さは常に n bit である。

安全性：[11] により安全性証明がなされている。ここでは簡単のため tag-splitting の不要な、平文が常にブロックサイズの等倍であるケースのバウンドを示す（実際には CCA3 という $\mathtt{Adv}^{\mathtt{opriv}}$ と $\mathtt{Adv}^{\mathtt{oauth}}$ を組み合わせた評価で示して

いるが、証明の内部にて下記のように分解がなされている)。McOE-X と McOE-G それぞれ、

$$\mathtt{Adv}^{\mathtt{opriv}}_{\text{McOE-G}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n},$$
$$\mathtt{Adv}^{\mathtt{oauth}}_{\text{McOE-G}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n},$$
$$\mathtt{Adv}^{\mathtt{opriv}}_{\text{McOE-X}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{rk\text{-}sprp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n},$$
$$\mathtt{Adv}^{\mathtt{oauth}}_{\text{McOE-X}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{rk\text{-}sprp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n}$$

ここで $\mathtt{Adv}^{\mathtt{rk\text{-}sprp}}_{E}(\mathcal{A}')$ は鍵差分 T を入力できるもとでの CCA 攻撃へのアドバンテージ（すなわち、T を tweak とした Tweakable ブロック暗号の CCA セキュリティ）を示す。

McOE-G では安全性がブロック暗号の強疑似ランダム性に帰着されるが、McOE-X では $C = \widetilde{E}_K(T, M) = E_{K \oplus T}(M)$ という暗号化が T ごとに独立と見なせる、という計算量的仮定、すなわち 2.6.1.5 節で述べた関連鍵安全性（Related-key Security）を要する。鍵に Tweak を加算する部分を利用した McOE-G へのアタックが [32] で提案されているが、基本的には計算量 $O(2^{n/2})$ であり、証明自体の決定的な誤りを指摘するものとはなっていない。ただし、このアタックは鍵回復を可能とするものであり、証明が考慮する識別攻撃・改ざん攻撃よりも強い。また [32] は証明における計算量的仮定の置き方に関する問題を示しており、同種の構成を考える際の参考とはなるであろう。

■COPA　設計者: Andreeva ら [2] により 2013 年に作られた。
構成：McOE と異なり、On-line cipher のアイディアを明示的には利用していない。Tweakable ブロック暗号である XEX [45] をベースに、ECB ライクなレイヤーを二つずらして重ねることで構成されている。暗号化のレートは 2 であり、暗号化にはブロック暗号暗号化関数を 2 回、復号にはブロック暗号復号関数を 2 回用いる。CPA-secure な On-line cipher である COPE と、COPE をベースとした On-line AE の COPA が提案されている。タグの長さは n-bit に固定されている。

安全性：[2] で示されている。

$$\mathtt{Adv}^{\mathtt{opriv}}_{\text{COPA}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n}$$
$$\mathtt{Adv}^{\mathtt{oauth}}_{\text{COPA}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n}$$

2.6.1.10　Deterministic AE 方式

■SIV　設計者: Rogaway と Shrimpton [48] により 2006 年に作られた。Deterministic AE(DAE) の最初の提案である。
構成：基本的には平文 M、およびヘッダ A が存在すれば A と M の連結、に対して MAC 関数を適用したのち、得られた出力 V をカウンターモードの初期値として用いて、平文を暗号化する。出力は V とカウンターモードの暗号化結果 C を連結した系列である。復号においては、V を用いて C を復号した後、復号結果 $\widetilde{M}$ を MAC 関数へ適用した結果が V と一致するかでメッセージ認証を行う。MAC 関数とカウンターモードの鍵は独立である。MAC 関数は並列実行可能で、vector-input (pseudorandom) function と呼ばれる形式を持つ、String-to-Vector (S2V) と呼ばれる関数である。これは、一つのバイナリ系列を vector として、vector の系列に対する PRF ととらえることができる[*3]。S2V

[*3] 原理上は Vector-input PRF は容易に単一の可変長入力 PRF と入力の符号化で構成可能であるが、S2V は vector に関するある種のインクリメンタル計算が可能という特徴を持つ。

は可変長（バイナリ系列）入力 PRF を部品として定義される。論文では CMAC を部品としている。レートは 2 であり、ブロック暗号の暗号化関数のみを利用する。タグ長は n bit 以下で設定可能である（が、安全性のバウンドは n の場合のみ扱っているとみられる；$\tau < n$ の場合は $q_v/2^\tau$ がバウンドに加算されると考えられる）。

安全性：[48] により示されている。なお、上述のように [48] では DAE security という単一の指標を中心に説明されているが、DPRIV と DAUTH の二つの指標で導出することが可能である（[48] の Proposition 9 を用いる）。

$$\mathtt{Adv}^{\mathtt{dae}}_{\mathrm{SIV}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n}$$
$$\mathtt{Adv}^{\mathtt{dpriv}}_{\mathrm{SIV}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_p^2}{2^n}$$
$$\mathtt{Adv}^{\mathtt{dauth}}_{\mathrm{SIV}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n}$$

■HBS　設計者: 岩田と安田 [22] により 2009 年に作られた。

構成：SIV がブロック暗号の二つの鍵を用いて構成されているのに対し、HBS ではブロック暗号と Polynomial hashing とを組み合わせ、かつ一つのブロック暗号の鍵のみを用いる。Polynomial hashing の鍵の係数を調節して、ヘッダとメッセージを二つの vector とした vector-input 関数としている。大域的な構成は SIV と似ているが、復号でのタグの検証においてブロック暗号の復号関数を用いるため、全体の安全性はブロック暗号の強疑似ランダム性に帰着される。レートは 1 であり、追加としてヘッダ a ブロック、平文 m ブロックに対して $a+m+2$ 回の $\mathrm{GF}(2^{128})$ 乗算を要する。タグに対してブロック暗号復号関数を適用するため、タグ長は n bit に固定されている。

安全性：[22] により示されている。

$$\mathtt{Adv}^{\mathtt{dae}}_{\mathrm{HBS}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n}$$

■BTM　設計者: 岩田と安田 [21] により 2009 年に作られた。

構成：BTM は HBS におけるブロック暗号の復号関数の利用を無くすことを目的に開発された。Polynomial hash の利用などは HBS と同様である。結果として、全体の安全性はブロック暗号の疑似ランダム性に帰着される。レートは 1 であり、追加としてヘッダ a ブロック、平文 m ブロックに対して $a+m-1$ 回の $\mathrm{GF}(2^{128})$ 乗算を要する。タグに対してブロック暗号復号関数を適用しなくてよいため、タグ長は $\tau \le n$ bit に設定することが可能である。

安全性：[22] により示されている（タグ長 n bit のケースであるとみられる）。

$$\mathtt{Adv}^{\mathtt{dae}}_{\mathrm{BTM}[E,n]}(\mathcal{A}) \le \mathtt{Adv}^{\mathtt{prp}}_{E}(\mathcal{A}') + \frac{\sigma_a^2}{2^n}$$

2.6.1.11　その他

■軽量暗号技術との関連性　ブロック暗号を用いた認証暗号の軽量化に関しては、いくつかのアプローチがある。もっとも全体軽量化に貢献すると思われるのは軽量ブロック暗号を用いることであるが、その多くが 64-bit ブロックサイズであるために、ここで紹介した多くの方式が 32-bit データセキュリティ、すなわち、$2^{32} * 8$ byte $\approx$ 34 Gbyte よりも十分少ないデータ量を処理したところで、鍵の更新が必要となる。例えばカウンターモード（ないしカウンターモードを含んだ AE）を 64-bit ブロック暗号で運用した場合に、PRIV アドバンテージが $\sigma^2/2^{64}$ であるとして、これを 2^{-20} 以下におさえるにはおおよそ $2^{5.5}$ Mbyte のデータ処理の後に鍵更新が必要となる。これは帯域の制限されたセンサーネットなどでセッション鍵生成を頻繁に行う環境であれば実用的だが、一般的にはきわめて制約が強いと思われ

る。なお 128-bit ブロック暗号であれば PRIV を 2^{-20} におさえるのに鍵更新が必要となるデータ処理は $2^{28.5}$ GByte となり、一般的に十分と思われる。

一方、n-bit ブロック暗号で $n/2$-bit 以上のデータセキュリティを保証する AE としては岩田 [15, 14] の方式が知られるのみであり、またこれらの方式は比較的ブロック暗号の外側の処理としてオーバーヘッドが比較的大きい（例えば汎用の $GF(2^n)$ 乗算を有する点で）ため、軽量ブロック暗号のメリットを消してしまう懸念がある。

AE としての複雑さや処理のオーバーヘッドを下げる試みとしては前述の EAX-prime やその改良 [37] があげられる。これらは EAX と比べて、処理の前に必要なブロック暗号のコール回数や、処理中に保持すべきメモリ量を減らしている。またこれらの設計思想をさらに推し進めた CLOC, SILC もある。また、CCFB も安全性のバウンドに強い制約はあるものの、モードとしての処理のオーバーヘッドはかなり小さく、センサーネットでの実装に適することが知られている [24]。ただし、プラットフォームによっては用いるブロック暗号自体の影響が大きく、モードの選択は全体性能において大きな違いをもたらさない可能性もある。

また、一般にセンサーネットで重要とされる消費電力については、計算よりも通信部分の電力消費が大きい。Struik [52] により指摘されているように、組み込み環境で AE による保護を考えるときには、AE 適用による通信量の増分（IV とタグ）を考慮し、ここを小さくするように無駄のないプロトコルを設計することが重要であろう。この場合、IV なし、タグ無しなどの暗号化方式を適切なリスク分析のもと用いることも一つの手段である。

■想定する安全性モデルから逸脱した場合の影響　暗号化、およびメッセージ認証について、安全性のバウンドを超えたデータ量を処理した場合にどのような攻撃が起こりうるかはいくつかの論文で議論されている。例えば McGrew [29] は CTR, CFB, CBC の三つの基本的な暗号化のモードにおいて処理量がバースデーバウンドを超えた場合に、ほぼデータ量の対数に比例して線形に平文ビットが漏れることを示した。また、MAC の場合については Black と Cochran [8] が、一度偽造が成功した場合にその情報をもとにどのような偽造が可能となるかを様々な MAC について調査した。ここでの結果は、該当する MAC を用いた AE についても当てはまることが予想される。ただし AE についてこのような観点から網羅的に安全性評価を試みた研究は見つかっていない。このように安全性の保証を超えた使い方をした場合、いわゆるミスユースに対する安全性の議論は今後重要になるかもしれない。

バースデーバウンドとはやや異なるが、いわゆる弱鍵を利用した攻撃もいくつか提案されている。特に多項式ハッシュ（およびそれを用いている GCM）について数多く報告があり、Sarrinen による cycling attack [51]、これを拡張した Procter と Cid [43] などの研究がある。鍵空間の部分集合 D について、D に鍵が入っているかを $|D|$ よりも少なくテストできるとき、D が弱鍵集合であるというのが従来の定義 [13] であったが、Procter と Cid はこの定義に従った場合、多項式ハッシュの鍵のほぼありとあらゆる部分集合が弱鍵集合とされてしまうことを示した。多項式ハッシュの脆弱性を指摘しているとも受け取れるが、証明可能安全性と矛盾するものではなく、ある意味では弱鍵集合の定義自体の意味を見直す必要があることも示唆している。

2.6.1.12　まとめ

認証暗号の安全性定義と、ブロック暗号に基づく具体的な方式とを調査した結果を報告した。5 章で述べたように、軽量な認証暗号を実現するために部品として軽量ブロック暗号を用いるだけでは解決できない課題がいくつかあり、またそれらの解決には認証暗号より上位のレイヤーでの解決が求められるケースもありそうである。また近年、ブロック暗号を用いず、ハッシュ関数やその部品をベースとする方式や、ブロック暗号のラウンド関数を部品として用いる方式などが提案されてきており、これらの動向にも注意が必要と思われる。

参考文献

[1] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness. `http://competitions.cr.yp.to/caesar.html`.

[2] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, and Kan Yasuda. Parallelizable and authenticated online ciphers. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013*, volume 8269 of *Lecture Notes in Computer Science*, pages 424–443. Springer, 2013.

[3] Kazumaro Aoki and Kan Yasuda. The Security of the OCB Mode of Operation without the SPRP Assumption. In Susilo and Reyhanitabar [53], pages 202–220.

[4] Mihir Bellare, Alexandra Boldyreva, Lars R. Knudsen, and Chanathip Namprempre. Online Ciphers and the Hash-CBC Construction. In Joe Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 292–309. Springer, 2001.

[5] Mihir Bellare, Alexandra Boldyreva, Lars R. Knudsen, and Chanathip Namprempre. On-line ciphers and the hash-cbc constructions. *J. Cryptology*, 25(4):640–679, 2012.

[6] Mihir Bellare and Chanathip Namprempre. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In Tatsuaki Okamoto, editor, *ASIACRYPT*, volume 1976 of *Lecture Notes in Computer Science*, pages 531–545. Springer, 2000.

[7] Mihir Bellare, Phillip Rogaway, and David Wagner. The EAX Mode of Operation. In Roy and Meier [50], pages 389–407.

[8] John Black and Martin Cochran. MAC Reforgeability. In Dunkelman [10], pages 345–362.

[9] Anne Canteaut, editor. *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*. Springer, 2012.

[10] Orr Dunkelman, editor. *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers*, volume 5665 of *Lecture Notes in Computer Science*. Springer, 2009.

[11] Ewan Fleischmann, Christian Forler, and Stefan Lucks. McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes. In Canteaut [9], pages 196–215.

[12] Virgil D. Gligor and Pompiliu Donescu. Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes. In Mitsuru Matsui, editor, *FSE*, volume 2355 of *Lecture Notes in Computer Science*, pages 92–108. Springer, 2001.

[13] Helena Handschuh and Bart Preneel. Key-Recovery Attacks on Universal Hash Function Based MAC Algo-

rithms. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 144–161. Springer, 2008.

[14] Tetsu Iwata. New Blockcipher Modes of Operation with Beyond the Birthday Bound Security. In Matthew J. B. Robshaw, editor, *FSE*, volume 4047 of *Lecture Notes in Computer Science*, pages 310–327. Springer, 2006.

[15] Tetsu Iwata. Authenticated Encryption Mode for Beyond the Birthday Bound Security. In Serge Vaudenay, editor, *AFRICACRYPT*, volume 5023 of *Lecture Notes in Computer Science*, pages 125–142. Springer, 2008.

[16] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, and Sumio Morioka. CLOC: Compact Low-Overhead CFB. `http://competitions.cr.yp.to/round1/clocv1.pdf`.

[17] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, and Sumio Morioka. CLOC: authenticated encryption for short input. *Proceedings of Fast Software Encryption 2014*, 2014:157, 2014.

[18] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, and Eita Kobayashi. SILC: SImple Lightweight CFB. `http://competitions.cr.yp.to/round1/silcv1.pdf`.

[19] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, and Eita Kobayashi. SILC: SImple Lightweight CFB. DIAC: Directions in Authenticated Ciphers, 2014. `http://2014.diac.cr.yp.to/`.

[20] Tetsu Iwata, Keisuke Ohashi, and Kazuhiko Minematsu. Breaking and Repairing GCM Security Proofs. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO*, volume 7417 of *Lecture Notes in Computer Science*, pages 31–49. Springer, 2012.

[21] Tetsu Iwata and Kan Yasuda. BTM: A Single-Key, Inverse-Cipher-Free Mode for Deterministic Authenticated Encryption. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *Selected Areas in Cryptography*, volume 5867 of *Lecture Notes in Computer Science*, pages 313–330. Springer, 2009.

[22] Tetsu Iwata and Kan Yasuda. HBS: A Single-Key Mode of Operation for Deterministic Authenticated Encryption. In Dunkelman [10], pages 394–415.

[23] Jakob Jonsson. On the Security of CTR + CBC-MAC. In Kaisa Nyberg and Howard M. Heys, editors, *Selected Areas in Cryptography*, volume 2595 of *Lecture Notes in Computer Science*, pages 76–93. Springer, 2002.

[24] Marcos A. Simplício Jr., Bruno Trevizan de Oliveira, Paulo S. L. M. Barreto, Cintia B. Margi, Tereza Cristina M. B. Carvalho, and Mats Näslund. Comparison of Authenticated-Encryption schemes in Wireless Sensor Networks. In Chun Tung Chou, Tom Pfeifer, and Anura P. Jayasumana, editors, *IEEE 36th Conference on Local Computer Networks, LCN 2011, Bonn, Germany, October 4-7, 2011*, pages 450–457. IEEE, 2011.

[25] Charanjit S. Jutla. Encryption Modes with Almost Free Message Integrity. In Birgit Pfitzmann, editor, *EUROCRYPT*, volume 2045 of *Lecture Notes in Computer Science*, pages 529–544. Springer, 2001.

[26] Ted Krovetz and Phillip Rogaway. The Software Performance of Authenticated-Encryption Modes. In Antoine Joux, editor, *FSE*, volume 6733 of *Lecture Notes in Computer Science*, pages 306–327. Springer, 2011.

[27] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. *J. Cryptology*, 24(3):588–613, 2011.

[28] Stefan Lucks. Two-Pass Authenticated Encryption Faster Than Generic Composition. In Henri Gilbert and Helena Handschuh, editors, *FSE*, volume 3557 of *Lecture Notes in Computer Science*, pages 284–298. Springer, 2005.

[29] David A. McGrew. Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes. *Pre-proceedings of Fast Software Encryption 2013*. Available from `http://eprint.iacr.org/2012/623`.

[30] David A. McGrew and John Viega. The Galois/Counter mode of operation (GCM). NIST Submission, 2004. Available from `http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html`.

[31] David A. McGrew and John Viega. The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In Anne Canteaut and Kapalee Viswanathan, editors, *INDOCRYPT*, volume 3348 of *Lecture Notes in Computer Science*, pages 343–355. Springer, 2004.

[32] Florian Mendel, Bart Mennink, Vincent Rijmen, and Elmar Tischhauser. A Simple Key-Recovery Attack on McOE-X. In Josef Pieprzyk, Ahmad-Reza Sadeghi, and Mark Manulis, editors, *CANS*, volume 7712, pages 23–31. Springer, 2012.

[33] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.

[34] Kazuhiko Minematsu. Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions. *IACR Cryptology ePrint Archive*, 2013:628, 2013.

[35] Kazuhiko Minematsu. Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions. In Nguyen and Oswald [42], pages 275–292.

[36] Kazuhiko Minematsu, Stefan Lucks, and Tetsu Iwata. Improved Authenticity Bound of EAX, and Refinements. In Susilo and Reyhanitabar [53], pages 184–201.

[37] Kazuhiko Minematsu, Stefan Lucks, Hiraku Morita, and Tetsu Iwata. Attacks and security proofs of EAX-prime. In Moriai [40], pages 327–347.

[38] Chris J. Mitchell. Cryptanalysis of Two Variants of PCBC Mode When Used for Message Integrity. In Colin Boyd and Juan Manuel González Nieto, editors, *ACISP*, volume 3574 of *Lecture Notes in Computer Science*, pages 560–571. Springer, 2005.

[39] Chris J. Mitchell. Analysing the IOBC Authenticated Encryption Mode. In Colin Boyd and Leonie Simpson, editors, *ACISP*, volume 7959 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2013.

[40] Shiho Moriai, editor. *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*. Springer, 2014.

[41] Chanathip Namprempre, Phillip Rogaway, and Thomas Shrimpton. Reconsidering Generic Composition. In Nguyen and Oswald [42], pages 257–274.

[42] Phong Q. Nguyen and Elisabeth Oswald, editors. *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*. Springer, 2014.

[43] Gordon Procter and Carlos Cid. On Weak Keys and Forgery Attacks Against Polynomial-Based MAC Schemes. In Moriai [40], pages 287–304.

[44] Francisco Recacha. Input and Output Chaining. NIST Submission, 2013. Available from `http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html`.

[45] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, *ASIACRYPT*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004.

[46] Phillip Rogaway. Nonce-Based Symmetric Encryption. In Roy and Meier [50], pages 348–359.

[47] Phillip Rogaway, Mihir Bellare, and John Black. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Trans. Inf. Syst. Secur.*, 6(3):365–403, 2003.

[48] Phillip Rogaway and Thomas Shrimpton. A Provable-Security Treatment of the Key-Wrap Problem. In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 373–390. Springer, 2006.

[49] Phillip Rogaway and Haibin Zhang. Online Ciphers from Tweakable Blockciphers. In Aggelos Kiayias, editor, *CT-RSA*, volume 6558 of *Lecture Notes in Computer Science*, pages 237–249. Springer, 2011.

[50] Bimal K. Roy and Willi Meier, editors. *Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers*, volume 3017 of *Lecture Notes in Computer Science*. Springer, 2004.

[51] Markku-Juhani Olavi Saarinen. Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes. In Canteaut [9], pages 216–225.

[52] Rene Struik. Revisiting design criteria for AEAD ciphers targeting highly constrained networks. DIAC: Directions in Authenticated Ciphers, 2013. `http://2013.diac.cr.yp.to/`.

[53] Willy Susilo and Reza Reyhanitabar, editors. *Provable Security - 7th International Conference, ProvSec 2013, Melaka, Malaysia, October 23-25, 2013. Proceedings*, volume 8209 of *Lecture Notes in Computer Science*. Springer, 2013.

[54] Douglas Whiting, Russ Housley, and Niels Ferguson. Counter with CBC-MAC (CCM). NIST Submission, 2002. Available from `http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html`.

[55] Liting Zhang, Sui Han, Wenling Wu, and Peng Wang. iFeed: the Input-Feed AE Modes. Rump Session of FSE 2013, 2013. slides from `http://fse.2013.rump.cr.yp.to/`.

[56] Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. iFeed[AES] v1. `http://competitions.cr.yp.to/round1/ifeedaesv1.pdf`.

2.6.2　認証暗号の実装性能

本章では、軽量暗号技術の現状調査として、主要な認証暗号の実装性能 (ハードウェア、ソフトウェア) 調査結果をまとめる。

2.6.2.1　調査内容

■Grain-128a　Grain-128 は 2004 年に eSTREAM のハードウェア部門に提案されたアルゴリズムであり、eSTREAM の Winner の一つである。文献 [1] に示されるハードウェア性能を表 2.22 にまとめる。文献 [1] ではゲートカウントの見積もりのみを実施している。

表 2.22　Grain-128a のゲートカウント見積もり

機能	速度モード毎のゲートカウント [gate]					
	1×	2×	4×	8×	16×	32×
暗号化のみ	2145.5	2243	2438	2828	3608	5168
32bitMAC 付き暗号化	2769.5	2867	3174	3788	5016	7472

■ALE　ALE は FSE 2013 で Rijmen らによって提案されたアルゴリズムである。AES-NI を積極的に利用することが可能な設計が採られている。認証暗号専用 (Dedicated) の設計ではあるが、モードの設計にも近く、性能比較も AES のモードとの比較をしている。文献 [2] に示される AES の Serial 実装（S-box 1 つを使いまわして暗号化演算を行う HW 実装）をベースにした 65nm CMOS スタンダードセルライブラリによる実装評価結果を表 2.23 に纏める。

表 2.23　ALE の回路性能

Design	Area[gate]	Clock cycles / block	Overhead cycles / message	Power [uW]
AES-ECB	2,435	226	-	87.84
AES-OCB2	4,612	226	452	171.23
AES-OCB2 e/d	5,916	226	452	211.01
ASC-1 A	4,793	370	904	169.11
ASC-1 A e/d	4,964	370	904	193.71
ASC-1 B	5,517	235	904	199.02
ASC-1 B e/d	5,632	235	904	207.13
AES-CCM	3,472	452	-	128.31
AES-CCM e/d	3,765	452	-	162.15
ALE	2,579	105	678	94.87
ALE e/d	2,700	105	678	102.32

ここで、ASC-1 は文献 [2] で示されるアルゴリズムであり、ALE の原型と呼べるアルゴリズムである。ALE は AES-OCB2 に対して半分の回路規模で 2 倍の処理速度が得られる。

図 2.2 に文献 [2] に記載される Sandy Bridge (AES-NI) 利用時のソフトウェア性能を示す。図から ALE は AES-OCB3 と同程度の処理性能を持つことがわかる。

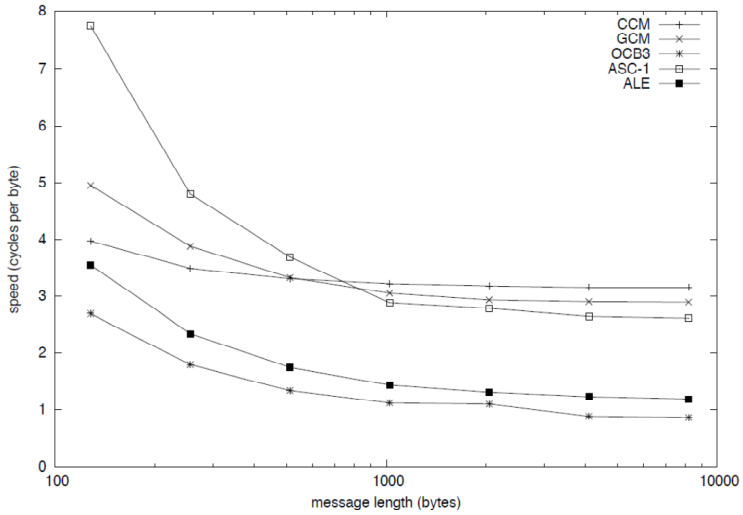


図 2.2　ALE のソフトウェア性能

■FIDES　FIDES は CHES 2013 で提案された認証暗号であり、以下のような特徴を持つ。

・ 論理回路として 793 gate で実装可能
・ Sponge 構造で 5bit、 6bit S-box を持つ
・ 鍵長、ステートが 80bit、160bit と 96bit、192bit の 2 種類ある

表 2.24 に文献 [3] に記載されるハードウェア性能を示す。文献 [3] では 3 種類の CMOS プロセスを用いた評価結果を示している。表中、Threshold implementation とはハードウェアにおけるサイドチャネル対策のための一方式を指す。

表 2.24　FIDES のハードウェア性能

Design	Security (bits)	Area (GE)	Frequency (kHz)	Latency	Throughput (kb/s)	Power (μW)
	Advanced NXP 90 nm CMOS process, typical PVT (25 °C, 1.2 V)					
FIDES-80-S	80	793	100	47	10.64	N/A
FIDES-80-4S	80	1178	100	23	21.74	N/A
FIDES-80-R	80	2922	100	1	500.00	N/A
FIDES-80-T	80	2876	100	47	10.64	N/A
FIDES-96-S	96	1001	100	47	12.77	N/A
FIDES-96-4S	96	1305	100	23	26.09	N/A
FIDES-96-R	96	6673	100	1	600.00	N/A
FIDES-96-T	96	4792	100	47	12.77	N/A
	NANGATE 45 nm CMOS process, typical PVT (25 °C, 1.1 V)					
FIDES-80-S	80	1244	100	47	10.64	N/A
FIDES-80-4S	80	1819	100	23	21.74	N/A
FIDES-80-R	80	4023	100	1	500.00	N/A
FIDES-80-T	80	4696	100	47	10.64	N/A
FIDES-96-S	96	1584	100	47	12.77	N/A
FIDES-96-4S	96	2023	100	23	26.09	N/A
FIDES-96-R	96	9180	100	1	600.00	N/A
FIDES-96-T	96	7541	100	47	12.77	N/A
	UMC 130 nm CMOS process, typical PVT (25 °C, 1.2 V)					
FIDES-80-S	80	1153	100	47	10.64	1.97
FIDES-80-4S	80	1682	100	23	21.74	2.82
FIDES-80-R	80	4175	100	1	500.00	7.90
FIDES-80-T	80	4267	100	47	10.64	7.47
FIDES-96-S	96	1453	100	47	12.77	2.49
FIDES-96-4S	96	1870	100	23	26.09	3.12
FIDES-96-R	96	8340	100	1	600.00	14.82
FIDES-96-T	96	6812	100	47	12.77	11.84

Fides-xy-S : Serial architecture (1 S-box).

Fides-xy-4S : Architecture with 4 S-boxes.

Fides-xy-R : Round-based architecture (32 S-boxes).

Fides-xy-T : Threshold implementation (1 S-box).

■Phelix　Phelix は 2004 年に eSTREAM に提案された MAC 付きストリーム暗号である。Phase 2 で落選で落選している。表 2.25 に文献 [4] に記載されるソフトウェア性能を示す。文献 [4] では Pentium M CPU での速度性能が示されている。

表 2.25　Phelix のソフトウェア性能

Operation	Version	Packet Size (N)			Approximate
		64 bytes	256 bytes	1024 bytes	Equation (clks)
Encrypt	C	41.6 cpb	20.3 cpb	15.0 cpb	$1810 + 13.2N$
Decrypt	C	42.3 cpb	21.1 cpb	15.8 cpb	$1610 + 14.0N$
Encrypt	ASM	18.5 cpb	9.8 cpb	7.4 cpb	$810 + 6.6N$
Decrypt	ASM	18.2 cpb	9.6 cpb	7.4 cpb	$750 + 6.7N$

cbp: clocks per byte

■Mode of Operation　AES-NI 前提で CCM、GCM、OCB3 など認証暗号用のモードに対する速度性能評価が文献 [5, 6, 7, 8] などで実施されている。表 2.26 にそれぞれの評価結果をまとめる。

表 2.26　暗号利用モードのソフトウェア性能 (Sandy Bridge)

Mode	cbp	data	Source
ECB	0.702	4KB	[6]
	0.853	8KB	OpenSSL 1.0.1c
CTR	0.691	4KB	[6]
	0.79	16KB	[RWC2013]
	0.916	8KB	OpenSSL 1.0.1c
OCB2	1.016	4KB	[6] (連続 2 倍)
	1.350	4KB	[6] (通常 2 倍)
OCB3	0.818	4KB	[6]
	0.87	4KB	[9]
GCM	2.47	16KB	[7]
	2.53	4KB	[7]
	2.564	4KB	[6]
	2.899	8KB	OpenSSL 1.0.1c

■CAESAR プロジェクト提案暗号　認証暗号アルゴリズムの公募プロジェクトである CAESAR プロジェクトへ提案されているアルゴリズムについて、提案者らが提示している実装性能を以下に示す。なお、既に鍵の全数探索よりも効率のよい攻撃方法が見つかっているアルゴリズムを含め、まとめている点に留意されたい。

表 2.27 に、FPGA の性能評価結果をまとめる。3 つのアルゴリズムで性能値が示されている。

表 2.28 に、ASIC の性能評価結果をまとめる。5 つのアルゴリズムで性能値が示されている。表 2.29 は、具体的な実装結果ではないが、ゲート規模の見積もりなどを実施しているアルゴリズムの性能値をまとめた結果である。5 つのアルゴリズムで性能値が示されている。

表 2.30 に、Mode of operation の提案で、Ivy Bridge マイクロアーキテクチャを実装ターゲットとしたソフトウェアの性能評価結果をまとめる。3 つのアルゴリズムで性能値が示されている。同様に表 2.31 には Dedicated としての提案に対する性能値をまとめる。

表 2.27　CAESAR 候補の FPGA 性能 (実装値)

Algorithm	Platform	Area	Freq. (MHz)	Throughput (Mbps)	Source
ICEPOLE	Xilinx Virtex6	1501 (slices/ALUT)	N/A	41,364	[21]
	Altera Stratix IV	4564 (slices/ALUT)	N/A	38,779	[21]
KIASU-BC	Xilinx Virtex5	1989 (slices)	N/A	1,080	[24]
pi-Cipher	Xilinx Virtex6	41 (slices)	N/A	N/A	[32]

表 2.28　CAESAR 候補の ASIC 性能 (実装値)

Algorithm	Area	Freq. (MHz)	Throughput (Mbps)	Source
CLOC	17137.75 (GE)	100	685.71	[17]
Minalpher-P	2810 (GE)			
NORX	62000 (GE)	125	10240	[30]
SCREAM-10 (Enc-/Dec-only)*1	12,951 (μm^2)	751	4577	[36]
SCREAM-10 (Enc-/Dec-only)*2	17,292 (μm^2)	446	5190	[36]
SCREAM-10 (Enc+Dec)*1	17,292 (μm^2)	751	4577	[36]
SCREAM-10 (Enc+Dec)*2	25,974 (μm^2)	446	5190	[36]
iSCREAM-12 (Enc-/Dec-only)*1	13,375 (μm^2)	740	3789	[36]
iSCREAM-12 (Enc-/Dec-only)*2	17,024 (μm^2)	448	4411	[36]
iSCREAM-12 (Enc+Dec)*1	13,375 (μm^2)	740	3789	[36]
iSCREAM-12 (Enc+Dec)*2	17,024 (μm^2)	448	4411	[36]
SILC	15675.5 (GE)	100	764.12	[38]

*1 1 round per cycle

*2 2 rounds per cycle

60

表 2.29　CAESAR 候補の ASIC 性能 (概算値)

Algorithm	Area (GE)	Source
Deoxys-BC-128-128	3400	[18]
Deoxys-BC-256-128	4400	[18]
Deoxys-128-128	4600	[18]
Deoxys-128-128	5600	[18]
Joltik$^{\neq}$-64-64	2100	[19]
Joltik$^{\neq}$-80-48	2100	[19]
Joltik$^{\neq}$-96-96	2600	[19]
Joltik$^{\neq}$-128-64	2600	[19]
Joltik$^{=}$-64-64	2600	[19]
Joltik$^{=}$-80-48	2600	[19]
Joltik$^{=}$-96-96	3100	[19]
Joltik$^{=}$-128-64	3100	[19]
KIASU$^{\neq}$	4000	[23]
KIASU$^{=}$	5000	[23]
LAC	1300	[25]
Sablier	1925	[35]

表 2.30　CAESAR 候補 (Mode of operation) のソフトウェア性能 (Ivy Bridge)

Algorithm	Speed (cpb)	Message length (bytes)	Source
AES-CPFB (Enc)	2	1500	[13]
	1.47	32768	[13]
AES-CPFB (Dec)	7.5	1500+	[13]
AES-SILC	4.9	long	[38]
PRESENT-SILC	42	long	[38]
LED-SILC	40	long	[38]
Scream-10	7.1	long	[36]
iScream-12	9.1	long	[36]

表 2.31　CAESAR 候補 (Dedicated) のソフトウェア性能 (Ivy Bridge)

Algorithm	Speed (cpb)	Message length (bytes)	Source
ICEPOLE (without special instruction sets)	9	N/A	[22]
Minalpher	23.1	31	[27]
	14.4	8192	[27]
	14.4	65536	[27]

表 2.32 に、Mode of operation の提案で、Sandy Bridge マイクロアーキテクチャを実装ターゲットとしたソフトウェアの性能評価結果をまとめる。5 つのアルゴリズムで性能値が示されている。同様に表 2.33 には Dedicated としての提案に対する性能値をまとめる。

表 2.32: CAESAR 候補 (Mode of operation) のソフトウェア性能 (Sandy Bridge)

Algorithm	Speed (cpb)	Message length (bytes)	Source
AES-JAMBU	17.7	64	[14]
	14.54	128	[14]
	13.06	256	[14]
	12.27	512	[14]
	11.86	1024	[14]
	11.60	4096	[14]
AEGIS-128L(Enc/Dec)	3.68/3.81	64	[11]
	2.05/2.12	128	[11]
	1.23/1.27	256	[11]
	0.83/0.85	512	[11]
	0.63/0.63	1024	[11]
	0.48/0.48	4096	[11]
AEGIS-128(Enc/Dec)	3.37/3.78	64	[11]
	1.99/2.17	128	[11]
	1.30/1.36	256	[11]
	0.96/1.02	512	[11]
	0.80/0.84	1024	[11]
	0.66/0.67	4096	[11]
AEGIS-256(Enc/Dec)	3.51/4.00	64	[11]
	2.10/2.35	128	[11]
	1.34/1.51	256	[11]
	1.03/1.09	512	[11]
	0.86/0.90	1024	[11]
	0.70/0.74	4096	[11]
Deoxys$^{\neq}$-128-128	2.30	128	[18]
	1.73	256	[18]
	1.45	512	[18]
	1.36	1024	[18]
	1.15	2048	[18]
	1.13	4096	[18]
Deoxys$^{\neq}$-256-128	4.26	128	[18]
	2.53	256	[18]

62

Algorithm	Speed (cpb)	Message length (bytes)	Source
	1.92	512	[18]
	1.57	1024	[18]
	1.48	2048	[18]
	1.32	4096	[18]
Deoxys$^{=}$-128-128	4.50	128	[18]
	3.42	256	[18]
	2.84	512	[18]
	2.61	1024	[18]
	2.43	2048	[18]
	2.33	4096	[18]
Deoxys$^{=}$-256-128	7.89	128	[18]
	5.13	256	[18]
	3.55	512	[18]
	3.07	1024	[18]
	2.75	2048	[18]
	2.59	4096	[18]
KIASU$^{\neq}$	1.02	4096	[23]
KIASU$^{=}$	1.98	4096	[23]
Tiaoxin	2.49	128	[41]
	1.45	256	[41]
	0.91	512	[41]
	0.65	1024	[41]
	0.50	2048	[41]
	0.44	4096	[41]
	0.40	8192	[41]
	0.38	2^{16}	[41]

表 2.33　CAESAR 候補 (Dedicated) のソフトウェア性能 (Sandy Bridge)

Algorithm	Speed (cpb)	Message length (bytes)	Source
ACORN	72.1	64	[10]
	41.5	128	[10]
	26.3	256	[10]
	18.6	512	[10]
	14.7	1024	[10]
	12.8	2048	[10]
	11.9	4096	[10]

表 2.34 に、Mode of operation の提案で、Haswell マイクロアーキテクチャを実装ターゲットとしたソフトウェアの性能評価結果をまとめる。9 つのアルゴリズムで性能値が示されている。同様に表 2.35 に Dedicated としての提案に対する性能値をまとめる。

表 2.34: CAESAR 候補 (Mode of operation) のソフトウェア性能 (Haswell)

Algorithm	Speed (cpb)	Message length (bytes)	Source
AES-COPA	1.44	128(short)	[12]
	1.29	2048(long)	[12]
AEZ	0.38(検証失敗時)	1500	[15]
	0.89	1500	[15]
	0.72	16384	[15]
AEGIS-128L(Enc/Dec)	3.44/3.45	64	[11]
	1.88/1.88	128	[11]
	1.11/1.09	256	[11]
	0.71/0.70	512	[11]
	0.51/0.50	1024	[11]
	0.37/0.35	4096	[11]
AEGIS-128(Enc/Dec)	3.29/2.98	64	[11]
	1.92/1.77	128	[11]
	1.24/1.16	256	[11]
	0.91/0.86	512	[11]
	0.73/0.81	1024	[11]
	0.61/0.60	4096	[11]
AEGIS-256(Enc/Dec)	3.98/3.88	64	[11]
	2.28/2.22	128	[11]
	1.42/1.39	256	[11]

64

Algorithm	Speed (cpb)	Message length (bytes)	Source
	0.99/0.98	512	[11]
	0.78/0.77	1024	[11]
	0.62/0.62	4096	[11]
Deoxys$^{\neq}$-128-128	2.25	128	[18]
	1.84	256	[18]
	1.64	512	[18]
	1.55	1024	[18]
	1.49	2048	[18]
	1.46	4096	[18]
Deoxys$^{\neq}$-256-128	3.68	128	[18]
	2.66	256	[18]
	2.14	512	[18]
	1.88	1024	[18]
	1.76	2048	[18]
	1.69	4096	[18]
Deoxys$^{=}$-128-128	4.07	128	[18]
	3.43	256	[18]
	3.12	512	[18]
	2.97	1024	[18]
	2.89	2048	[18]
	2.85	4096	[18]
Deoxys$^{=}$-256-128	5.68	128	[18]
	4.44	256	[18]
	3.82	512	[18]
	3.51	1024	[18]
	3.36	2048	[18]
	3.28	4096	[18]
HS1-SIV	0.8	N/A	[20]
KIASU$^{\neq}$	0.74	4096	[23]
KIASU$^{=}$	1.39	4096	[23]
Marble	1.6	8192	[26]
Silver(Enc/Dec)(AES-NI)	10.8/9.6	44	[39]
	1/1.2	1536	[39]
	0.73/0.81	long	[39]
Silver(Enc/Dec)(non-AES-NI)	30.4/28.2	44	[39]
	11.85/13.59	1536	[39]
	11.45/12.9	long	[39]
Tiaoxin	0.31	8192	[41]

Algorithm	Speed (cpb)	Message length (bytes)	Source
	0.28	long	[41]

表 2.35　CAESAR 候補 (Dedicated) のソフトウェア性能 (Haswell)

Algorithm	Speed (cpb)	Message length (bytes)	Source
ICEPOLE (without special instruction sets)	8	N/A	[22]
Minalpher	5.76	8192	[28]
MORUS-640(Enc/Dec)	7.72/7.99	64	[29]
	1.18/1.23	4096	[29]
	1.11/1.16	long	[29]
MORUS-1280(Enc/Dec)	8.28/8.46	64	[29]
	0.78/0.80	4096	[29]
	0.69/0.69	long	[29]
NORX64-6-1(Ref/AVX2)*3	1248.00/748.24	8	[30]
	156.61/93.23	64	[30]
	9.85/5.71	576	[30]
	7.77/4.47	1536	[30]
	7.00/3.98	4096	[30]
	6.63/3.73	long	[30]
NORX64-4-1(Ref/AVX2)*3	863.12/509.51	8	[30]
	106.94/63.38	64	[30]
	6.71/3.83	576	[30]
	5.27/3.01	1536	[30]
	4.76/2.66	4096	[30]
	4.50/2.51	long	[30]

*3 Ref: 移植可能な C レファレンス実装、AVX2: AVX2 利用の最適実装

最後に表 2.36 として、上記のいずれの分類にも含まれない候補のソフトウェアの性能評価結果をまとめる。

表 2.36: CAESAR 候補のソフトウェア性能 (Others)

Algorithm	Platform	ROM/RAM (bytes)	Speed (cpb)	Message length (bytes)	Source
HS1-SIV	MIPS32	N/A	16	N/A	[20]
	Cortex-A9	N/A	5	N/A	[20]

Algorithm	Platform	ROM/RAM (bytes)	Speed (cpb)	Message length (bytes)	Source
LAC	Core i7-3612QM	N/A	720	12	[25]
			589	16	[25]
			440	32	[25]
			256	64	[25]
			206	128	[25]
			174	256	[25]
			152	512	[25]
			144	1024	[25]
			140	2048	[25]
			138	4096	[25]
Minalpher	RL78	1275/470	514	long	[27]
NORX32-6-1 (Ref/NEON)*4	Samsung Exynos 4412 Prime (Cortex-A9)	N/A	794.12/541.00	8	[30]
			128.66/77.78	64	[30]
			42.14/22.79	576	[30]
			35.45/18.36	1536	[30]
			32.35/16.70	4096	[30]
			31.56/15.66	long	[30]
NORX32-4-1 (Ref/NEON)*4	Samsung Exynos 4412 Prime (Cortex-A9)	N/A	663.75/434.88	8	[30]
			97.94/61.73	64	[30]
			30.50/16.40	576	[30]
			24.94/12.77	1536	[30]
			22.86/11.41	4096	[30]
			21.57/10.57	long	[30]
NORX64-6-1 (Ref/AVX)*5	Core i7-2630QM	N/A	304.00/198.00	8	[30]
			37.75/24.81	64	[30]
			11.54/7.52	576	[30]
			9.08/5.90	1536	[30]
			8.14/5.24	4096	[30]
			7.69/4.94	long	[30]
NORX64-4-1 (Ref/AVX)*5	Core i7-2630QM	N/A	208.00/133.50	8	[30]
			26.00/16.69	64	[30]
			7.94/5.03	576	[30]
			6.24/3.91	1536	[30]
			5.59/3.49	4096	[30]
			5.28/3.28	long	[30]
NORX64-6-1 (Ref/AVX)*5	Core i7-3667U	N/A	371.50/276.00	8	[30]
			34.87/25.44	64	[30]

Algorithm	Platform	ROM/RAM (bytes)	Speed (cpb)	Message length (bytes)	Source
			10.59/7.71	576	[30]
			8.32/6.03	1536	[30]
			7.46/5.37	4096	[30]
			7.04/5.04	lonog	[30]
NORX64-4-1	Core i7-3667U	N/A	310.00/218.00	8	[30]
(Ref/AVX)[*5]			24.93/17.18	64	[30]
			7.43/5.16	576	[30]
			5.86/4.01	1536	[30]
			5.24/3.59	4096	[30]
			4.92/3.37	long	[30]
POET	Core i5-4300U	N/A	4.61	128	[34]
			4.24	256	[34]
			4.13	512	[34]
			4.02	1024	[34]
			3.92	2048	[34]
OMD-SHA256	Core i5-2415M	N/A	44.56	128	[31]
			28.77	4096	[31]
OMD-SHA512	Core i5-2415M	N/A	45.93	128	[31]
			23.28	4096	[31]
Scream-10[*6]	Cortex A15	N/A	21.8	long	[36]
	Atom Cedarview	N/A	55	long	[36]
	Core i7 Nehalem	N/A	9.3	long	[36]
	Atmel AVR	3221/80	7646(E)/7672(D)	N/A	[36]
	Atmel AVR	1723/80(Enc-only)	7646	N/A	[36]
	Atmel AVR	1751/80(Dec-only)	7672	N/A	[36]
iScream-12[*6]	Cortex A15	N/A	26.2	long	[36]
	Atom Cedarview	N/A	65	long	[36]
	Core i7 Nehalem	N/A	11.2	long	[36]
	Atmel AVR	1975/64	8724(E)/8724(D)	long	[36]
	Atmel AVR	1595/64(Enc-only)	8724	N/A	[36]
	Atmel AVR	1593/64(Dec-only)	8724	N/A	[36]
STRIBOB	Core i7 860	N/A	25.3	N/A	[40]

[*4] Ref: 移植可能な C レファレンス実装、NEON: NEON 利用の最適実装

[*5] Ref: 移植可能な C レファレンス実装、AVX: AVX 利用の最適実装

[*6] tweakable block cipher のみの実装

2.6.2.2　まとめ

本節では、主要な認証暗号の実装性能 (ハードウェア、ソフトウェア) 調査結果をまとめた。本調査は CAESAR プロジェクトがスタートし、第二ラウンド進出アルゴリズムを選定している段階で実施しているため、数多くのアルゴリズムについて性能値を掲載している。しかしながら、これらはあくまで著者らの主張に基づいた提示であり、本資料記載のデータを用いてアルゴリズム間の比較を行う目的にはそぐわないことに注意されたい。

今後、安全性やサイドチャネル対策との関連性を含めプロジェクトでの絞り込みについて動向を注視していく必要があると考える。

参考文献

[1] Martin Ågren, Martin Hell, Thomas Johansson and Willi Meier: Grain-128a: a new version of Grain-128 with optional authentication. IJWMC 5(1): 48-59, 2011.

[2] Andrey Bogdanov, Florian Mendel, Francesco Regazzoni, Vincent Rijmen and Elmar Tischhauser: ALE: AES-Based Lightweight Authenticated Encryption. FSE2013.

[3] Begül Bilgin, Andrey Bogdanov, Miroslav Knezevic, Florian Mendel and Qingju Wang: FIDES: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware. CHES2013.

[4] Doug Whiting, Bruce Schneier, Stefan Lucks and Frédéric Muller: Phelix Fast Encryption and Authentication in a Single Cryptographic Primitive. https://www.schneier.com/paper-phelix.pdf

[5] Kazumaro Aoki, Tetsu Iwata and Kan Yasuda: How Fast Can a Two-Pass Mode Go? A Parallel Deterministic Authenticated Encryption Mode for AES-NI. DIAC 2012

[6] Kazumaro Aoki: Optimization of mode implementations on Sandy Bridge. SCIS 2013

[7] Shay Gueron: AES-GCM for Efficient Authenticated Encryption - Ending the Reign of HMAC-SHA-1? https://crypto.stanford.edu/RealWorldCrypto/slides/gueron.pdf

[8] Shay Gueron: AES-GCM software performance on the current high end CPUs as a performance baseline for CAESAR competition? http://2013.diac.cr.yp.to/slides/gueron.pdf

[9] Phillip Rogaway, Mihir Bellare, John Black, Ted Krovetz, and Tom Shrimpton: The Evolution of Authenticated Encryption.
http://hyperelliptic.org/DIAC/slides/sweden-rogaway-ae-2012b.pdf

[10] Hongjun Wu, "ACORN: A Lightweight Authenticated Cipher (v1),"
http://competitions.cr.yp.to/round1/acornv1.pdf

[11] Hongjun Wu, Bart Preneel, "AEGIS: A Fast Authenticated Encryption Algorithm (v1),"
http://competitions.cr.yp.to/round1/aegisv1.pdf

[12] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, Kan Yasuda, "AES-COPA v.1," http://competitions.cr.yp.to/round1/aescopav1.pdf

[13] Miguel Montes, Daniel Penazzi, "AES-CPFB v1,"
http://competitions.cr.yp.to/round1/aescpfbv1.pdf

[14] Hongjun Wu, Tao Huang, "JAMBU Lightweight Authenticated Encryption Mode and AES-JAMBU (v1),"
http://competitions.cr.yp.to/round1/aesjambuv1.pdf

[15] Viet Tung Hoang, Ted Krovetz, Phillip Rogaway, "AEZ v3: Authenticated Encryption by Enciphering,"
http://web.cs.ucdavis.edu/~rogaway/aez/aez.pdf

[16] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, "CLOC: Compact Low-Overhead CFB,"

http://competitions.cr.yp.to/round1/clocv1.pdf

[17] Tetsu Iwata, "CAESAR candidate SILC," http://2014.diac.cr.yp.to/slides/iwata-silc.pdf

[18] Jérémy Jean, Ivica Nikolić, Thomas Peyrin, "Deoxys v1," http://competitions.cr.yp.to/round1/deoxysv1.pdf

[19] Jérémy Jean, Ivica Nikolić, Thomas Peyrin, "Joltik v1," http://competitions.cr.yp.to/round1/joltikv1.pdf

[20] Ted Krovetz, "HS1-SIV," http://2014.diac.cr.yp.to/slides/krovetz-hs1.pdf

[21] Pawel Morawiecki, Kris Gaj, Ekawat Homsirikamol, Krystian Matusiewicz, Josef Pieprzyk, Marcin Rogawski, Marian Srebrny, Marcin Wójcik, "ICEPOLE v1," http://competitions.cr.yp.to/round1/icepolev1.pdf

[22] Marcin Rogawski, "CAESAR candidate ICEPOLE", http://2014.diac.cr.yp.to/slides/rogawski-icepole.pdf

[23] Jérémy Jean, Ivica Nikolić, Thomas Peyrin, "KIASU v1," http://competitions.cr.yp.to/round1/kiasuv1.pdf

[24] Thomas Peyrin, "CAESAR candidate KIASU," http://competitions.cr.yp.to/round1/kiasuv1.pdf

[25] Lei Zhang, Wenling Wu, Yanfeng Wang, Shengbao Wu, Jian Zhang, "LAC: A Lightweight Authenticated Encryption Cipher," http://competitions.cr.yp.to/round1/lacv1.pdf

[26] Jian Guo, "Marble Specification Version 1.1," http://competitions.cr.yp.to/round1/marblev11.pdf

[27] Yu Sasaki, Yosuke Todo, Kazumaro Aoki, Yusuke Naito, Takeshi Sugawara, Yumiko Murakami, Mitsuru Matsui, Shoichi Hirose, "Minalpher v1," http://competitions.cr.yp.to/round1/minalpherv1.pdf

[28] Kazumaro Aoki, "Observations on Prøst and Minalpher," https://www.cryptolux.org/mediawiki-esc2015/images/c/cb/Slide.pdf

[29] Hongjun Wu, Tao Huang, "The Authenticated Cipher MORUS (v1)," http://competitions.cr.yp.to/round1/morusv1.pdf

[30] Jean-Philippe Aumasson, Philipp Jovanovic, Samuel Neves, "NORX v1," http://competitions.cr.yp.to/round1/norxv1.pdf

[31] Simon Cogliani, Diana-Ştefania Maimuţ, David Naccache, Rodrigo Portella do Canto, Reza Reyhanitabar, Serge Vaudenay, Damian Vizár, "OMD A Compression Function Mode of Operation for Authenticated Encryption," http://2014.diac.cr.yp.to/slides/reyhanitabar-omd.pdf

[32] Danilo Gligoroski, Hristina Mihajloska, Simona Samardjiska, Håkon Jacobsen, Mohamed El-Hadedy, Rune Erlend Jensen, "π-Cipher v1," http://competitions.cr.yp.to/round1/picipherv1.pdf

[33] Danilo Gligoroski, "CAESAR candidate PiCipher," http://2014.diac.cr.yp.to/slides/gligoroski-picipher.pdf

[34] Farzaneh Abed, Scott Fluhrer, John Foley, Christian Forler, Eik List, Stefan Lucks, David McGrew, Jakob Wenzel, "The POET Family of On-Line Authenticated Encryption Schemes," http://competitions.cr.yp.to/round1/poetv101.pdf

[35] Bin Zhang, Zhenqing Shi, Chao Xu, Yuan Yao, Zhenqi Li, "Sablier v1," http://competitions.cr.yp.to/round1/sablierv1.pdf

[36] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici, François Durvaux, Lubos Gaspar, Stéphanie Kerckhof, "SCREAM & iSCREAM Side-Channel Resistant Authenticated Encryption with

Masking," http://competitions.cr.yp.to/round1/screamv1.pdf

[37] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, Eita Kobayashi, "SILC: SImple Lightweight CFB," http://competitions.cr.yp.to/round1/silcv1.pdf

[38] Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, Eita Kobayashi, "SILC: SImple Lightweight CFB," http://2014.diac.cr.yp.to/slides/iwata-silc.pdf

[39] Daniel Penazzi, Miguel Montes, "Silver and AESCPFB," http://2014.diac.cr.yp.to/slides/penazzi-silver-cpfb.pdf

[40] Markku-Juhani O. Saarinen, "The STRIBOBr1 Authenticated Encryption Algorithm," http://competitions.cr.yp.to/round1/stribobr1.pdf

[41] Ivica Nikolić, "Tiaoxin–346," http://competitions.cr.yp.to/round1/tiaoxinv1.pdf

第 3 章

軽量暗号に関する現状調査: 軽量暗号に関わる新しい技術動向

3 章の執筆担当者は下記の通りである.

第 3 章　軽量暗号に関わる新しい技術動向	
3.1 章　低レイテンシ暗号	崎山委員
3.2 章　サイドチャネル攻撃耐性	成吉委員
3.3 章　CAESAR プロジェクト	岩田委員
3.4 章　軽量暗号の活用事例および標準化動向	小川委員

3.1　低レイテンシ暗号

3.1.1　はじめに

低レイテンシ暗号 (Low-Latency Cryptography) に関する論文のうち、特に欧州で研究が活発であるブロック暗号を用いた Low-Latency Encryption/Decryption について技術動向調査を行った。ハードウェア実装に関する論文 [1, 2, 3] を紹介し、今後の展望について述べる。

3.1.2　Low-Latency Cryptography 研究のモチベーション

暗号処理における低レイテンシ性は、暗号処理時の応答速度を重視するデータ通信アプリケーションに求められている。例えば、車の自動運転支援システム（Car2X communication)、セキュア・ストレージ及び CPU と外部ストレージ間のデータを暗号化するバス・エンクリプションである。半導体加工技術の高精度化（CMOS プロセスのの微細化）による集積回路の信号遅延時間短縮が大きく期待できない中、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自体を大幅に削減する必要がある。これが、軽量暗号が新たに求められる理由のひとつと考える。現在広く使われている AES ブロック暗号では、回路規模、レイテンシともに上述のようなアプリケーションが求める性能要求を満たさない。例えば、1〜2 ns のレイテンシ性能を実現する AES 暗号ハードウェアは、現在の回路技術では実装が困難である。

3.1.3 ブロック暗号による Low-Latency Encryption/Decryption の性能評価

Knežević らによって CHES2012 で発表された論文 [1] では、暗号処理回路を 1 サイクルあるいは 2 サイクルでが完了するように実装し、数 10 MHz〜数 100 MHz のオーダーの最大動作周波数での処理時間をレイテンシとしている。つまり、レイテンシは数 ns〜数 10ns 程度となる。本報告では簡単のために、1 サイクルで処理が完了する場合についてのみ紹介する。90 nm CMOS テクノロジで合成した場合、 AES-128 のレイテンシは 14.8 ns、mCrypton-128 では 9.7 ns、PRESENT-128 では 14.3 ns と報告されている。Encryption/Decryption 両機能を搭載した場合、 AES-128 のレイテンシは約 17.8ns となり、性能の低下が見られるが、mCrypton-128 と PRESENT-128 ではそれぞれ 9.8 ns と 14.8 ns でとなる、ほとんど差異がないと評価されている。 3 つの暗号方式それぞれの回路規模は、AES-128, mCrypton-128, PRESENT-128 の順に、約 360 kGE、50 kGE、80 kGE（GE: Gate Equivalent の略、回路面積を表す単位）である。この結果から、mCrypton-128 が優れているように見えるが、安全性を犠牲にしている可能性がある。また、低レイテンシ暗号の場合には、回路規模はそれほど重要ではなく、むしろレイテンシに重きを置いた評価が好ましいと思われる。

Borghoff らによる ASIACRYPT2012 の発表論文 [2] で、低レイテンシのブロック暗号 PRINCE が提案された。4 ビット S-box による非線形演算と線形演算で構成されるデータ・パスは 64 ビット長で、鍵は 128 ビット長である。AES の鍵スケジュールと比べて、非常に単純な鍵スケジュール方式を採用している。回路規模は、約 8 kGE と報告されている。レイテンシは、45 nm CMOS テクノロジで 4.7 ns、90 nm CMOS テクノロジで 13.9 ns と報告されている。

SCIS2014 で、鈴木らは PRESENT と PRINCE の低レイテンシ実装を発表した [3]。PRESENT と PRINCE を 45 nm CMOS テクノロジで合成した結果、回路規模はそれぞれ 22 kGE と 8 kGE となり、レイテンシは 9.03 ns と 5.49 ns となった。ちなみに AES では 174 kGE で 12.25ns のレイテンシであった。ただし、以上の回路規模の数値は、暗号処理回路のみに基づくものであり、ARM プロセッサ向けの周辺モジュール用のバス・インターフェイス回路分（AMBA APB: 約 2 kGE）は含まない。この論文 [3] では、RFID タグへの実装に関する興味深い考察が与えられている。RFID タグ・チップのシリコン・ダイのサイズは、基板実装上の制限を受け、300μm 角程度が限界（下限）とされている。CMOS プロセスの微細化にともない、シリコンダイに実装できる回路規模が増大する。例えば 90 nm プロセスでは、300μm 角のシリコン・ダイに 30 kGE のロジック回路が搭載可能である。つまり、PRESENT と PRINCE は 90 nm（より微細な）CMOS テクノロジを用いることで、RFID タグに搭載できる。ただし、パッシブ RFID タグでは、低消費電力が重要となるため、この点は留意する必要がある。

3.1.4 まとめ

ここでは、低レイテンシを実現するいくつかの軽量ブロック暗号に関する技術動向調査を行った。ブロック暗号 PRINCE は、鍵拡張の単純化やデータ・パスの 64 ビット化により、回路規模の低減と低レイテンシ化の両方を同時に実現した。回路規模に対するレイテンシ性能は、アプリケーションによっては十分な性能と言える水準にあると考える。複数ラウンドを 1 サイクルで実装することは、サイドチャネル耐性の向上に繋がることが報告されている [4]。低レイテンシ実装においても同様の耐性向上が期待できるため、今後は、軽量暗号実装における耐タンパー性評価を併せて考える必要があると思われる。

参考文献

[1] Miroslav Knežević, Ventzislav Nikov, Peter Rombouts. Low-Latency Encryption - Is "Lightweight = Light + Wait"? In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems — CHES 2012*, volume 7428 of *Lecture Notes in Computer Science*, pages 426-446,, Springer-Verlag, Berlin, Heidelberg, 2012.

[2] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knežević, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and-Tolga Yalçin. PRINCE — A Low-Latency Block Cipher for Pervasive Computing Applications — Extended Abstract. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology — ASIACRYPT 2012 — 18th International Conference on the Theory and Application of Cryptology and Information Security*, volume 7658 of *Lecture Notes in Computer Science*, pages 208-225, Springer-Verlag, Berlin, Heidelberg, 2012

[3] 鈴木大輔, 菅原健, 佐伯稔. 軽量/低遅延暗号のハードウェア実装性能について. *2014* 年 暗号と情報セキュリティシンポジウム — *SCIS 2014*, 6 pages, 2014.

[4] Shivam Bhasin, Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, Unrolling Cryptographic Circuits, Unrolling Cryptographic Circuits: A Simple Countermeasure Against Side-Channel Attacks. In Josef Pieprzyk, editor, *Topics in Cryptology — CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010*, volume 5985 of *Lecture Notes in Computer Science*, pp.195-207, Springer-Verlag, Berlin, Heidelberg, 2010.

3.2 サイドチャネル攻撃耐性

本章では、軽量暗号技術に関する現状調査のうち、サイドチャネル攻撃耐性に関する文献調査結果を記載する。

3.2.1 調査対象

サイドチャネル攻撃耐性に関して、2012 年度まで CRYPTREC 暗号実装委員会にて活動していたサイドチャネルワーキンググループ活動の報告書 [1]、ならびにセキュリティ認証に関する規格 ISO/IEC15408 のコモンクライテリア承認アレンジメント (Common Criteria Recognition Arrangement) の web サイトに登録されている攻撃手法 [2] を参考に、以下 (i)(ii) を調査対象とし、調査結果を以降に記す。

(i) サイドチャネル攻撃 (リーク解析、電流解析。電磁波解析も含む)
(ii) 故障利用攻撃

物理攻撃、例えば文献 [2] には IC へのアクセスもしくは加工をおこなう物理解析などの記載はあるが、暗号アルゴリズムによる対策等の記載がなかったため、各軽量暗号アルゴリズムにおける物理攻撃耐性の評価は調査対象から除外した。

CRYPTREC Report 2012 暗号実装委員会報告ならびに文献 [2] に記載されていない攻撃手法、例えば文献 [3] は AES を攻撃対象として鍵抽出を試みているが、これらも調査対象外とした。調査対象とする暗号技術は、ブロック暗号のうち CRYPTREC 電子政府推奨暗号の AES、 TDES、 Camellia、ISO/IEC 29192-2 記載の PRESENT[4]、CLEFIA、ならびに LED[5]、 Piccolo[6]、 TWINE[7]、 PRINCE[8] とした。

3.2.2 軽量暗号アルゴリズムにおけるサイドチャネル攻撃 (リーク解析) の耐性調査

現状調査として、リーク解析 [9] における各種解析手法に関する文献、リーク解析に関する測定手法に関する文献、軽量暗号に関するリーク解析ならびに耐性を題目とした文献、リーク解析対策の最新手法、リーク耐性全般に関する文献について順に報告する。

3.2.2.1 リーク解析における各種解析手法の現状調査

ブロック暗号を対象としたリーク解析において、差分電力解析 (DPA) ならびにその派生の解析方法 [10] を示す。

1. DPA。演算途中の特定の 1 ビット (選択関数) に着目。入力を変化させたときの各候補鍵で計算した値とリークとの相関を算出し、鍵を推測する手法 [11]
2. CPA。演算途中の特定の値 (複数ビット) に着目。入力を変化させたときの各候補鍵で計算したハミングウエイト、ハミングディスタンス等とリークとの相関を算出し、鍵を推測する手法 [12]
3. High-order 型。演算途中に着目する箇所を複数個所とし、1.、 2. と同様に鍵を推測する手法 [13]
4. 相互情報量を用いた手法 [14]
5. template を用いた攻撃 [10][15]。鍵と入力を変化させて事前に各鍵の電力 (電磁波) のプロファイルを作成し、攻撃時には固定した鍵に対して入力を変化させ、プロファイルとリークとの比較により鍵を推測。
6. シミュレーション結果をリーク結果との相関の入力に与える手法 [16]。攻撃対象となる選択関数の値と、例えば論理シミュレーションでトグル回数を入手しておき、各候補鍵において相関を求めて鍵を推測する手法。

文献 [16] が顕著な例だが、ファンクションから回路を起こした時に発生した AES SBOX での過渡遷移を含んだ消費電力において、SBOX への DPA では 90 万サンプルなのに対して、シミュレーションの結果を相関関数の入力に適用した場合では 13 万サンプルと大幅に減ったとしている。以上から、実装時における過渡遷移の程度など消費電力モデルの精度にばらつきが発生し、プロセスならびに論理合成のコンフィグファイル等で過渡遷移の発生頻度も変わることが文献 [16] から容易に想定できるため、実装結果に関する論文間での厳密な比較は困難である。無対策の軽量暗号アルゴリズムにおいてデータに依存したリークの発生源となり得る演算回路の規模以外の観点からリーク耐性の優劣をつけるのは困難と推測する[*1] 。

3.2.2.2 リーク解析における測定手法の現状調査

リーク解析において電磁波観測を利用した手法 [17] が提案されてから久しいが、2013 年の国際ワークショップ CHES では下記の文献で 2NAND セルに関するリークの違いが報告されており、ゲートレベルですら無対策のものは攻撃されつつあることから、無対策の暗号アルゴリズムでは方式に依存せずに攻撃できるものと類推する。

・On Measurable Side-Channel Leaks inside ASIC Design Primitives[18]

本文献では電磁波リークを観測することでチップ動作を識別する研究がされており、以下の識別が可能とのこと。

- 2NAND セルに対して、入力 (1,1) の状態から入力 (0,0) への変化と入力 (0,1) の変化の区別が可能である (各 1 万波形取得後の平均での比較において)
- メモリのカラム線のアクセスの違いも識別可能

文献 [18] での環境にて鍵抽出評価を実施した場合は、既存の研究結果よりも大幅にサンプル数を減らすことが期待される。

評価環境については評価ボード SASEBO[19] あるいは ZUIHO をキャリブレーションとして使用することで一定の能力の担保はできているものと思われるが、電磁波解析などはコイルから測定場所の選定までパラメータが多く、評価結果に関する論文間の比較は困難である。

3.2.2.3 軽量暗号に関するリーク解析を題目とした文献調査

軽量暗号に関するリーク解析を題目とした発表を文献 [20] にて確認したため、その内容を報告する。本件は特定アルゴリズムに呼応した対策ではない。

文献 [20] においては Adiabatic logics(断熱的回路) を用いた手法でのサイドチャネル攻撃対策がメインである。面積のオーバーヘッドは存在するが、いわゆるグリッチタイプの瞬間的な消費電力の抑制によりサイドチャネル攻撃の耐性が急激に上昇しており、RFID などの低消費電力用途での対策において既存の MDPL[22] や RSL[23] [24] の同じセルレベルでのリーク対策方式と比較して向いているとしている。実チップ評価なし。

その消費電力抑制の効果から軽量暗号のことが触れられている。軽量暗号モジュールは消費電力が比較的小さいことから S/N 比が小さいことが強みである一方で、省電力技術がサイドチャネル攻撃への抵抗を弱めており、まとめとしてサイドチャネル攻撃の成功の可能性を大きくあげており、その実例としてブロック暗号である Keeloq を用いたアプリケーションへの攻撃 [25] を挙げている。

[*1] モジュール内において暗号演算と無関係な回路の動作が多いほど S/N 比が下がるので、そのような暗号アルゴリズムはリーク解析には有利に働く可能性はあると考える。

3.2.2.4　リーク解析対策の最新手法

リーク解析の対策においては秘密情報と秘密情報に依存した消費電力との相関をなくすというのが一般的な手法だが、リーク解析していることを検知することで秘密情報の流出を防ぐ新しいタイプの対策が最近提案されている。

文献 [21] によると、リーク解析のひとつである電磁波解析攻撃の対抗策として EM attack sensor と命名したセンサを暗号モジュールを搭載したチップに実装、実チップによる評価を実施している。EM attack sensor はコイルの形状をしている配線を有しており、その配線に一定の周波数の信号を流しておく。電磁波解析攻撃のため観測用のプローブを近づけると相互インダクタンスが発生し、上記信号の周波数がシフト。この周波数のシフトを観測することで攻撃を受けているかどうかを判別することでリークを防ぐ手法である。

3.2.2.5　リーク解析耐性の文献調査ならびにまとめ

厳密にリーク対策を実施しようとするとセルレベルでの対策、例えば MDPL[22] や RSL[23] [24] などといった手法の採用が必要と考える。それ故、対策の対象となる SBOX などの暗号演算処理部、具体的には NAND、 NOR セル使用部が小さいほど低面積、低消費電力の耐リークモジュールを実現できると考える。文献 [2] ではリーク解析を実装した各種暗号方式の電力解析の評価結果が記載されており、対策効果を確認したと結論づけている。ただし、対策セルを使用して実装した場合においても文献 [18] までを想定すると、論理的には同じでも実装した際の配線などの容量に依存してマスクの値が区別できると指摘している文献 [26] もあることから、レイアウトにおける対策も必要となることが想定される。これは面積だけではなく、設計工数にも大きく影響することを意味している。対策箇所が少ないほど設計工数の面からも優秀であり、これらは一般的に AES よりも軽量暗号のほうが優位に働くものと思われる。

最新リーク対策手法である EM attack sensor について暗号モジュールを搭載したチップに適用させた場合、電磁波攻撃をするためにはセンサを回避しなければならず、十分な起電力が得られない状況に陥ると推測される。この条件下において SBOX 単体への電磁波解析による鍵抽出を考えた場合、テーブルルックアップ方式で実装された 8 ビットの AES SBOX と多くの軽量暗号で採用されている 4 ビットの SBOX では、SBOX の回路規模に起因する消費電力の少なさから軽量暗号への攻撃のほうが困難になることが推測される。SBOX が小型化になることで、SBOX 以外の回路から発生されるノイズの比率が高くなる以外に、電磁波攻撃するためのコイルの最適なポジジョンの選定も SBOX の消費電力の少なさから見つけにくくなることが想定される。

3.2.2.6　リーク解析の現状調査に関する今後の課題

リーク解析への耐性の優劣に関する暗号アルゴリズム間の比較は文献調査だけでは限界があると考える。対策回路を実装した各種暗号方式に対し、文献 [18] 相当のリーク解析の実施が今後の課題である。

3.2.3　軽量暗号アルゴリズムにおける故障利用攻撃の耐性調査

3.2.3.1　故障利用攻撃の調査概要

文献 [27] をはじめとした、故障注入による鍵の抽出攻撃 DFA(Differential Fault Analysis) の容易性は暗号方式に依存する。DFA の攻撃に関する論文の多くが効率的な攻撃手法をシミュレーションなどを用い理論的に研究しているものであり、例えば実際にレーザを注入して特定段の一つ、あるいは複数の SBOX 等を攻撃して Differential Fault Analysis が可能かどうか評価した論文は皆無である。但し、レーザ装置とステージ装置の自動スキャンにより AES 暗号などを対象として DFA ができるツールは市販されており [28]、特に 1 か所への攻撃を想定しているものについて故障対策なく実装された場合は再現可能と考える。本ツールは対象暗号方式以外の他の暗号方式への応用も可能なものと

思われる。以降、各ブロック暗号に関して理論的な DFA 攻撃の研究事例を挙げる。

攻撃を受けることで想定される故障の種類として、演算器の出力などが一時的に誤り、その値を取り込んでしまうことで故障が発生するテンポラリなものと、中間値を格納するフリップフロップが反転するなど恒久的に値が変わってしまうパーマネントなものが考えられるが、ここでは両方とも実チップにおいて攻撃可能と判断する。前者は演算器の入力となる格納された値には故障が含まれていないことになる。

3.2.3.2 AES への故障利用攻撃の文献調査

鍵長 128 ビット使用時の AES への DFA について文献 [29] によると 8 段目の拡大鍵がストアされた領域への 1 ブロックに対してのフォルト注入攻撃において、1 ペアの結果で 2^8 の空間まで絞り込みが可能とのこと。鍵長 192 ビット使用時ならびに 256 ビット使用時の AES への DFA については文献 [30] によるとそれぞれ 3 ペア、4 ペアの結果で 2^{32} の空間まで絞り込むことが可能とのこと。

3.2.3.3 CLEFIA への故障利用攻撃の文献調査

鍵長 128 ビット使用時の CLEFIA への DFA について文献 [31] によると 2 か所への攻撃、2 ペアで平均 $2^{19.02}$ の探索空間まで絞り込むことが可能としている。文献 [32] によると、CLEFIA への DFA について、鍵長 128 ビット使用時は 2 ペアの攻撃結果のみ、鍵長 192 ビットならびに鍵長 256 ビット使用時では 2 ペアの攻撃結果で平均 $2^{10.78}$ の探索空間まで絞り込むことが可能としている。

鍵長 192 ビットならびに鍵長 256 ビット使用時の CLEFIA への DFA について文献 [33] によると、いずれも 8 ペアの攻撃結果で鍵が判明するとしている。

3.2.3.4 TDES への故障利用攻撃の文献調査

TDES ではないが、Single DES への DFA について文献 [34] によると、特定された single ビットへの攻撃を 12 段目で実施していき 7 ペアを入手すると、ランダムな場所への single ビットの故障注入の場合は 9 ペアを入手すると、それぞれ 99% 以上の確率で 16 段目の鍵が回復できるとしている。

3.2.3.5 PRESENT への故障利用攻撃の文献調査

PRESENT-80/128 への DFA に関して文献 [35] によると、2 バイトのランダムフォルトを 28 段目に注入することで、PRESENT-80 であれば 2 ペア、PRESENT-128 であれば 3 ペアで鍵を回復できるとしている。

3.2.3.6 LED への故障利用攻撃の文献調査ならびに対策に関する特記事項

64 ビットブロック暗号、64 ビット鍵である LED-64 への DFA に関して文献 [36] によると、29 段目に対して故障を注入することで、1 ペアで鍵探索空間を平均で $2^{4.03}$ まで絞り込むことができるとしている (鍵探索空間の調査においてはランダムに生成した誤り暗号文ペア 50 組に対して、実際に攻撃を適用後の鍵候補数から算出)。

LED-64 は拡大鍵として使用する 64 ビットの鍵を全て同じ鍵としており、LED-128 は 64 ビット長 2 組の拡大鍵を交互に使用するため、演算中での拡大鍵の演算は不要である。故に、故障攻撃可能な範囲が狭くなる、対策回路を実装したときの負担低減などのメリットが考えられる (但し、文献 [36] は鍵スケジュール部ではなく、暗号処理中の中間値への攻撃)。

3.2.3.7 Piccolo、 TWINE への故障利用攻撃

研究が開始されたところである。暗号演算部分の 1 ビットあるいは 1 ニブルのレーザ攻撃ではないが、ソフトウェアによる暗号実装において命令への故障攻撃を想定したものとしては、64 ビットブロック暗号で 80 ビット鍵の Piccolo-80、 同じく 64 ビットブロック暗号で 80 ビット鍵の TWINE-80 に対して、正しい暗号文と故障注入により誤った二つの暗号文の組で鍵を抽出できるとしており、128 ビット鍵の CLEFIA-128 より容易という報告は出ている [37]。

3.2.3.8 PRINCE への故障利用攻撃ならびに対策に関する特記事項

64 ビットブロック暗号、128 ビット鍵である PRINCE の 10 段目に対して 1 ニブルの攻撃を実施。1000 例による PC での探索空間調査の結果、4 回の故障注入で 2^{18} 未満の探索空間まで絞り込むことができるとしている [38]。

PRINCE は拡大鍵として使用する 64 ビットの鍵を全て同じ鍵としており、拡大鍵の演算は実装不要である。故に、故障攻撃可能な範囲が狭くなる、対策回路を実装したときの負担低減などのメリットが考えられる (但し、文献 [38] は鍵スケジュール部ではなく、暗号処理中の中間値への攻撃)。

3.2.3.9 複数の暗号方式を対象とした故障利用攻撃の文献調査

多数の暗号方式への故障利用攻撃の最近の調査として文献 [39] が挙げられる。本文献では一般型 Feistel 構造への故障利用攻撃を比較しており、対象は DES(single)、 TWINE、CLEFIA 等。解析のしかたはオーソドックスで、ラウンドの前後でフォルトが伝搬するブロック関係を行列で表記。各段において single ビットの故障を与えたとき、Subkey ブロックのうちアタックされた個数、故障利用攻撃の際に中間値を推測した候補の数をまとめており、過去に発表された論文、例えば文献 [31] との比較を行いながら、本解析手法における故障利用攻撃の最適な攻撃の段数をまとめている。

3.2.3.10 故障利用攻撃耐性のまとめ

鍵長 128 ビット使用時の AES、 LED-64 が 1 ペアで鍵探索空間を 2^8 以下まで絞りこみ可能となっており、耐性が比較的低い。一方、TDES は鍵を 56 ビット毎 3 回に分けて使用するため、故障利用攻撃の耐性が比較的高いと考える。

また、今回調査した軽量暗号への故障利用攻撃の多くが 2012 年から 2014 年に発表されたものであるため、今後の研究により更なる故障注入回数の低減の可能性があると考える。

実チップへの攻撃については、拡大鍵演算部がないなど演算回路規模の小さいもののほうが攻撃範囲が狭いなどの可能性がある。更に、上記にも記載した文献 [29] の AES の攻撃に関しては拡大鍵の演算結果のブロックの一つにパーマネントのエラーを注入することで、中間値だけではなく拡大鍵計算時に故障が伝搬することも利用しており、特にオンザフライによる実装の脆弱性を確認しているが、上記軽量暗号の中には拡大鍵演算実行不要のものが提案されており、拡大鍵の故障伝搬による攻撃が利用できないという点で従来より故障耐性が高いと考えることが出来る。

次に、二回演算ならびに逆算による対策、冗長回路の実装、各種センサの実装による 3 つの主な対策手法において、それぞれ軽量暗号に適用した際の AES と比較しての優劣を記述する。

■二回演算ならびに逆算による対策 対策方法のひとつに文献 [40] に記載されている二回計算 (Doubling)、逆算などが考えられる。文献 [40] では DES を例にとっているが、他の共通鍵暗号方式においても適用可能と考える。但し、文献 [40] ではレーザによる故障利用攻撃において同じ場所に複数回照射する攻撃例や、複数の箇所にレーザを照射させる攻撃でこれらの対策を無効にすることが出来るとしており、攻撃者の能力や攻撃費用を想定して必要相当の対策を講

じることを DES と同様、他の暗号を実装した場合にも求められる。Doubling 対策を実装した実チップへのレーザ攻撃成功例については文献 [41] が挙げられる。複数回演算による対策を施す場合、一般的に暗号処理時間が高速である軽量暗号のほうが AES と比較して追加対策によるレイテンシ増加を抑えることが期待できる。

■冗長回路の実装による対策　冗長化、二重化など追加回路の実装による故障対策も考えられる。例えば文献 [42] で、冗長の程度と検出率を比較している。上記テンポラリーエラーが発生することで故障が注入された場合、単に中間値が格納されているフリップフロップ等に冗長ビットを持たせただけでは検出できない可能性がある。以上から冗長化等による対策の場合、演算器等を含めた暗号実装本体の面積に比例するものと思われ、一般的に軽量暗号が AES などと比較して面積コストの観点から優位に働くものと想定される。なお、上記二回演算等と同様に、冗長回路あるいは多重化された回路と元の回路の双方に攻撃される可能性についての脅威分析は必要であり、分析結果に応じて両方の回路が攻撃された場合の追加の対策が必要となるが、分析の必要性、対策実施の有無は暗号方式には依存しないものと思われる。

■各種センサによる対策　各種故障攻撃を各センサで対処する方法も考えられる。例えば、レーザなどの光源をチップ表面、あるいは裏面から局所的に照射することで故障利用攻撃を試みる手法に対して、光センサをチップ内にちりばめるように実装することで故障を防ぐ方法も提案されている [43]。本方式による対策の場合、光センサ実装による面積増は暗号実装本体の面積に比例するものと想定できることから、一般的に軽量暗号が AES などと比較して面積コストの観点から優位に働くものと想定される。電磁波注入によるチップへの局所攻撃 [44] も出てきているが、暗号アルゴリズムへの故障利用攻撃に使用された場合のセンサ複数配置による対策についても光センサと同様、面積コストの観点から一般的に軽量暗号が優位と考える。電源グリッチ [28] による故障利用解析をセンサ等で防御する場合は、チップ全体の電源回りの設計に大きく依存することになるため、暗号方式による面積コストの優位不利は少ないものと思われる。

3.2.3.11　故障利用攻撃手法の応用

故障利用攻撃の応用として、AES 演算における鍵長 128 ビット使用時の攻撃において Differential ではなく、攻撃により誤った暗号文のみを集めて鍵を復元する試みも文献 [45] でおこなわれている。故障注入の成功率が 50% から 100% それぞれにおいて、ラウンド 7 への攻撃において 4 から 10 の誤ったメッセージで 2^0 から $2^{39.7}$ の鍵候補の絞り込みが 62 から 100% の確率で出来ると調査されている。

3.2.3.12　故障利用攻撃の現状調査に関する今後の課題

故障利用攻撃に関しても文献調査のみならず、厳密には実チップによる各暗号アルゴリズムでの比較対象が望ましい。実チップによる故障利用攻撃、耐性評価は今後の課題である。

参考文献

[1] CRYPTREC Report 2012 暗号実装委員会報告

[2] CCRA. Application of Attack Potential to Smartcards CCDB-2013-05-002, `http://www.commoncriteriaportal.org/cc/`

[3] Pascal Manet, and Bruno Robisson. Differential Behavioral Analysis. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems — CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 413–426. Springer-Verlag, Berlin, Heidelberg, New York, 2007.

[4] Andrey Bogdanov, Lars Ramkilde Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and Charlotte H. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems — CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer-Verlag, Berlin, Heidelberg, New York, 2007.

[5] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED block cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems — CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 326–341. Springer-Verlag, Berlin, Heidelberg, New York, 2011.

[6] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: An ultra-lightweight blockcipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems — CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 342–357. Springer-Verlag, Berlin, Heidelberg, New York, 2011.

[7] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE: A lightweight, versatile block cipher. In Gregor Leander and François-Xavier Standaert, editors, *ECRYPT Workshop on Lightweight Cryptography*, pages 146–169. ECRYPT II, 2011.

[8] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, Tolga Yalçn, “PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications”, In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225. Springer, 2012.

[9] Paul Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Neal Koblitz , editor, *Advances in Cryptology - CRYPTO 1996 - 16th Annual International Cryptology Conference Santa Barbara, California, USA, August 18-22, 1996. Proceedings*, volume 1109 of *Lecture Notes*

in Computer Science, pages 104–113. Springer-Verlag, Berlin, Heidelberg, New York, 1996. `http://www.cryptography.com/public/pdf/TimingAttacks.pdf`

[10] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. Power Analysis Attacks Revealing the Secrets of Smart Cards. 2007 Springer.

[11] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. `http://www.cryptography.com/public/pdf/DPA.pdf`

[12] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In Marc Joye, and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems — CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29. Springer-Verlag, Berlin, Heidelberg, New York, 2004.

[13] Thomas S. Messerges. Using Second-Order Power Analysis to Attack DPA Resistant Software. In Çetin K. Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2000*, volume 1965 of *Lecture Notes in Computer Science*, pages 238–251. Springer-Verlag, Berlin, Heidelberg, New York, 2000.

[14] Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual Information Analysis. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems — CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442. Springer-Verlag, Berlin, Heidelberg, New York, 2008.

[15] S. Chari, J.R. Rao, and P. Rohatgi. Template Attacks. In Burton S. Kaliski, Çetin K. Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 13–28. Springer-Verlag, Berlin, Heidelberg, New York, 2002.

[16] Stefan Mangard, Norbert Pramstaller, and Elisabeth Oswald. Successfully Attacking Masked AES Hardware Implementations. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2005*, volume 3659 of *Lecture Notes in Computer Science*, pages 157–171. Springer-Verlag, Berlin, Heidelberg, New York, 2005.

[17] D. Agrawal, B. Archambeault, J.R. Rao, and P. Rohatgi. The EM Side-channel(s). In Burton S. Kaliski, Çetin K. Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 29–45. Springer-Verlag, Berlin, Heidelberg, New York, 2002

[18] Takeshi Sugawara, Daisuke Suzuki, Minoru Saeki, Mitsuru Shiozaki, and Takeshi Fujino. On Measurable Side-Channel Leaks inside ASIC Design Primitives. In Guido Bertoni, and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems — CHES 2013*, volume 8086 of *Lecture Notes in Computer Science*, pages 159–178. Springer-Verlag, Berlin, Heidelberg, New York, 2013

[19] `http://www.risec.aist.go.jp/project/sasebo/`

[20] Amir Moradi and Axel Poschmann. Lightweight Cryptography and DPA Countermeasures: A Survey. `http://emsec.rub.de/media/crypto/veroeffentlichungen/2010/09/05/wlc.pdf`

[21] Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Daichi Tanaka, Makoto Nagata, and Takafumi Aoki. EM Attack Is Non-invasive? - Design Methodology and Validity Verification of EM Attack Sensor. In Lejla Batina, and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems — CHES 2014*, volume 8731 of *Lecture Notes in Computer Science*, pages 1–16. Springer-Verlag, Berlin,

Heidelberg, New York, 2014

[22] T. Popp and S. Mangard. Masked Dual-Rail Pre-charge Logic: DPA-Resistance without Routing Constraints. In Josyula R. Rao and Berk Sunar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2005*, volume 3659 of *Lecture Notes in Computer Science*, pages 172–186. Springer-Verlag, Berlin, Heidelberg, New York, 2005.

[23] D. Suzuki, M. Saeki, and T. Ichikawa. Random Switching Logic: A Countermeasure against DPA based on Transition Probability. Cryptology ePrint Archive, Report 2004/346, 2004. `http://eprint.iacr.org/`

[24] D. Suzuki, M. Saeki, and T. Ichikawa. Random Switching Logic: A New Countermeasure against DPA and Second-Order DPA at the Logic Level. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E90-A(1): pages 160–168. IEICE, 2007.

[25] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoqCode Hopping Scheme. In Wagner David, editors *Advances in Cryptology - CRYPTO 2008 - 28th Annual International Cryptology Conference Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*, pages 203–220. Springer-Verlag, Berlin, Heidelberg, New York, 2008.

[26] Patrick Schaumont and Kris Tiri. Masking and Dual-Rail Logic Don't Add Up. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems — CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 95–106. Springer-Verlag, Berlin, Heidelberg, New York, 2007.

[27] D. Boneh, R. A. DeMillo, and R. J. Lipton. A New Breed of Crypto Attack on "Tamperproof" Tokens Cracks Even the Strongest RSA Code. 1996.

[28] RISCURE 社. `https://www.riscure.com/`

[29] Sk Subidh Ali and Debdeep Mukhopadhyay. A Differential Fault Analysis on AES Key Schedule using Single Fault. In Luca Breveglieri, Sylvain Guilley, Israel Koren, David Naccache, and Junko Takahashi, editors, *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on Date 28-28 Sept. 2011 IEEE computer society*, pages 54–64, IEEE, 2011.

[30] 高橋 順子、福永 利徳Differential Fault Analysis on AES with 192 and 256-bit keys. *2010*年 暗号と情報セキュリティシンポジウム — *SCIS 2010*. 2010.

[31] Junko Takahashi, and Toshinori Fukunaga. Improved Differential Fault Analysis on CLEFIA. In Luca Breveglieri, Shay Gueron, Israel Koren, David Naccache, and Jean-Pieere Seifert, editors, *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2008 Workshop on Date 10-10 Aug. 2008 IEEE computer society*, pages 25–34. IEEE, 2008.

[32] Junko Takahashi, Toshinori Fukunaga. Differential Fault Analysis on CLEFIA with 128, 192, and 256-Bit Keys. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, Vol.E93-A No.1 pages 136–143. IEICE, 2010

[33] S Ali, and D Mukhopadhyay. Improved Differential Fault Analysis of CLEFIA. In Wieland Fischer, and Jorn-Marc Schmidt, editors, *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on Date 20-20 Aug. 2013 IEEE computer society*, pages 60–72. IEEE, 2013.

[34] Matthieu Rivain, Emmanuel Prouff, Julien Doget. Differential Fault Analysis on DES Middle Rounds. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems — CHES 2009*, volume 5747 of *Lecture Notes in Computer Science*, pages 457–470. Springer-Verlag, Berlin, Heidelberg, New

York, 2009.

[35] Kitae Jeonga, Yuseop Leea, Jaechul Sungb, and Seokhie Honga. Improved differential fault analysis on PRESENT-80/128. *International Journal of Computer Mathematics, Volume 90, Issue 12*, pages 2553-2563. 2013.

[36] 上野 嶺、 本間 尚文、 青木 孝文. LED 暗号への単一の故障注入を用いた差分故障解析とその評価. *2014* 年 暗号と情報セキュリティシンポジウム — *SCIS 2014*. 2014.

[37] Hideki YOSHIKAWA, Masahiro KAMINAGA, Arimitsu SHIKODA, and Toshinori SUZUKI. Round Addition DFA on 80-bit Piccolo and TWINE. *IEICE Transactions on Information and Systems*, Vol.E96-D No.9 pages 2031–2035. IEICE, 2013.

[38] Ling Song, Lei Hu. Differential Fault Attack on the PRINCE Block Cipher. `http://eprint.iacr.org/2013/043.pdf`

[39] Helene Le Bouder, Gael Thomas, Yanis Linge and Assia Tria. On Fault Injections in Generalized Feistel Networks. *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2014 Workshop on Date 23-23 Sept. 2014 IEEE computer society*, pages 83–93. IEEE, 2014.

[40] Rob Bekkers and Hans König "Fault Injection, a Fast Moving Target in Evaluations", FDTC2011, IEEE computer society, p.65, IEEE. `http://conferenze.dei.polimi.it/FDTC11/shared/FDTC-2011-keynote-2.pdf`

[41] 大野 仁、土屋 遊、 中田 量子、松本 勉. IC カードへのレーザー照射フォールト攻撃は単純な冗長実装では防げない. *2014* 年 暗号と情報セキュリティシンポジウム — *SCIS 2014*. 2014.

[42] Tal G. Malkin, François-Xavier Standaert, Moti Yung. A Comparative Cost/Security Analysis of Fault Attack Countermeasures. In Luca Breveglieri, Israel Koren, David Naccache, and Jean-Pierrei Seifert, editors, *Fault Diagnosis and Tolerance in Cryptography: Third International Workshop, FDTC 2006*, volume 4236 of *Lecture Notes in Computer Science*, pages 159–172. Springer-Verlag, Berlin, Heidelberg, New York, 2006.

[43] Odile Derouet. Secure Smartcard Design against Laser Fault Injection Attacks (invited), FDTC2007, `http://conferenze.dei.polimi.it/FDTC07/Derouet_remaster.pdf`

[44] F. Poucheret, K. Tobich, M. Lisarty, L. Chusseauz, B. Robissonx, and P. Maurine. Local and Direct EM Injection of Power Into CMOS Integrated Circuits. In Luca Breveglieri, Sylvain Guilley, Israel Koren, David Naccache, and Junko Takahashi, editors, *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on Date 28-28 Sept. 2011 IEEE computer society*, pages 100–104, IEEE, 2011.

[45] Thomas Fuhr, Eliane Jaulmes, Victor Lomné and Adrian Thillard. Fault Attacks on AES with Faulty Ciphertexts Only. In Wieland Fischer, and Jorn-Marc Schmidt, editors, *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on Date 20-20 Aug. 2013 IEEE computer society*, pages 108–118. IEEE, 2013.

3.3 CAESAR プロジェクト

本章では、暗号技術調査 WG (軽量暗号 WG) の外部動向調査として、CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) プロジェクトについてまとめる。本プロジェクトのウェブサイトは `http://competitions.cr.yp.to/caesar.html` である。

3.3.1 CAESAR プロジェクト

■プロジェクト発足の背景　認証暗号は、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である。AES-CCM や AES-GCM など、すでに標準化され実用化されている認証暗号では、オンラインではない (あらかじめ入力データ長を決めないと処理を開始できない)、計算効率を改善させる余地がある、証明可能安全性に不備がある、弱鍵が存在する、といった様々な問題点が指摘されている。

また、OpenSSH や TLS、802.11 ネットワークにおける WEP などで安全性の問題点が指摘されており、認証暗号はこれらの問題の解決策として期待されている。一方、これらにおいて認証暗号の普及は遅れており、現状の認証暗号の計算効率が、たとえば RC4 などより劣る点にその原因の一つがあると考えられる。

■プロジェクトの目標　本プロジェクトの目標は、(1) AES-GCM より (安全性、計算効率、実装効率、あるいはその他何らかの点において) 優れていて、なおかつ (2) 広範に実用化されることに適した認証暗号のポートフォリオを選定することにある。

■プロジェクトの概要　本プロジェクトでは認証暗号アルゴリズムの公募を行う。応募締め切りは 2014 年 3 月であり、誰でも応募が可能である。公募されたアルゴリズムは第一ラウンドアルゴリズムであり、おおよそ 1 年の評価期間を経て 2015 年 1 月に第二ラウンド進出アルゴリズムを決定する。その後さらに 1 年の評価期間を経て 2015 年 12 月に第三ラウンド進出アルゴリズムを決定し、さらに 1 年の評価期間を経て 2016 年 12 月に最終候補アルゴリズムを決定する。ポートフォリオのアナウンスは 2017 年 12 月を予定している。

本プロジェクトは研究者主体で進められるものであり、ポートフォリオは標準を意味するものではない (ただし、本プロジェクトは NIST によるスポンサーシップを受けている)。また、各ラウンドに進出するアルゴリズムの決定では、選定委員による投票が行われる予定である。

本プロジェクトでは各提案者の設計指針に応じて安全性、機能、実装性能、計算効率など様々な評価要素が考えられ、「軽量」性についても評価要素に入ることが予想される。

■スケジュール詳細　下記スケジュールを予定している[*2]。

- M-20, 2012.07.05–06: DIAC: Directions in Authenticated Ciphers. Stockholm.
- M-14, 2013.01.15: Competition announced at the Early Symmetric Crypto workshop in Mondorf-les-Bains; also announced online.
- M-7, 2013.08.11–13: DIAC 2013: Directions in Authenticated Ciphers 2013. Chicago.
- M0, 2014.03.15: Deadline for first-round submissions.
- M1, 2014.05.15: Deadline for first-round software.

[*2] 2015 年 2 月 20 日現在。頻繁に更新されており、最新情報はプロジェクトのウェブサイト `http://competitions.cr.yp.to/caesar.html` より確認できる。

- M5 2014.08.23–24: DIAC 2014: Directions in Authenticated Ciphers 2014. Santa Barbara.
- M12 (tentative), 2015.03.15: Announcement of second-round candidates.
- M13 (tentative), 2015.04.15: Deadline for second-round tweaks.
- M14 (tentative), 2015.05.15: Deadline for second-round software.
- M15 (tentative), 2015.06.15: Deadline for second-round Verilog/VHDL.
- 2015 summer (tentative): DIAC 2015.
- M21 (tentative), 2015.12.15: Announcement of third-round candidates.
- M22 (tentative), 2016.01.15: Deadline for third-round tweaks.
- M23 (tentative), 2016.02.15: Deadline for third-round software.
- M24 (tentative), 2016.03.15: Deadline for third-round Verilog/VHDL.
- 2016 summer (tentative): DIAC 2016.
- M33 (tentative), 2016.12.15: Announcement of finalists.
- M34 (tentative), 2017.01.15: Deadline for finalist tweaks.
- M35 (tentative), 2017.02.15: Deadline for finalist software.
- M36 (tentative), 2017.03.15: Deadline for finalist Verilog/VHDL.
- 2017 summer (tentative): DIAC 2017.
- M45 (tentative), 2017.12.15: Announcement of final portfolio.

■公募要領　2014 年 1 月 27 日に公募要領の最終版が公表された。2014 年 3 月の応募時点では下記情報を含めたドキュメントを提出する。

- 方式の名称、設計者、応募者、連絡用メールアドレス
- 仕様
- 安全性のゴール
- 安全性解析
- 特筆すべき事項、特徴
- 設計の合理性
- 知的財産に関する事項
- 応募に際して合意する事項

その後 2014 年 5 月 15 日までにソフトウェアでのレファレンスコードを提出する。また、第二ラウンド進出アルゴリズムについては、応募者は 2015 年 4 月までにハードウェアでのレファレンス実装を提出する。

■選定委員　選定委員は下記 22 名のメンバーからなる。

1. Steve Babbage (Vodafone Group, UK)
2. Daniel J. Bernstein (University of Illinois at Chicago, USA, and Technische Universiteit Eindhoven, Netherlands); secretary, non-voting
3. Alex Biryukov (University of Luxembourg, Luxembourg)
4. Anne Canteaut (Inria Paris-Rocquencourt, France)
5. Carlos Cid (Royal Holloway, University of London, UK)
6. Joan Daemen (STMicroelectronics, Belgium)

7. Christophe De Cannière (Google, Switzerland)
8. Orr Dunkelman (University of Haifa, Israel)
9. Henri Gilbert (ANSSI, France)
10. Tetsu Iwata (Nagoya University, Japan)
11. Lars R. Knudsen (Technical University of Denmark, Denmark)
12. Stefan Lucks (Bauhaus-Universität Weimar, Germany)
13. David McGrew (Cisco Systems, USA)
14. Willi Meier (FHNW, Switzerland)
15. Kaisa Nyberg (Aalto University School of Science, Finland)
16. Bart Preneel (COSIC, KU Leuven, Belgium)
17. Vincent Rijmen (KU Leuven, Belgium)
18. Matt Robshaw (Impinj, USA)
19. Phillip Rogaway (University of California at Davis, USA)
20. Greg Rose (Qualcomm Technologies Inc., USA)
21. Serge Vaudenay (EPFL, Switzerland)
22. Hongjun Wu (Nanyang Technological University, Singapore)

■応募方式一覧　下記の 57 方式が提案された。方式の名称と設計者を記載している。冒頭の (L) は、軽量性を特徴として挙げている方式を示している[*3]。

1. (L) ACORN: v1 (Hongjun Wu)
2. (L) ++AE: v1.0 (Francisco Recacha)
3. AEGIS: v1 (Hongjun Wu, Bart Preneel)
4. AES-CMCC: v1, v1.1 (Jonathan Trostle)
5. AES-COBRA: v1, withdrawn, (Elena Andreeva, Andrey Bogdanov, Martin M. Lauridsen, Atul Luykx, Bart Mennink, Elmar Tischhauser, Kan Yasuda)
6. AES-COPA: v1 (Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, Kan Yasuda)
7. AES-CPFB: v1 (Miguel Montes, Daniel Penazzi)
8. (L) AES-JAMBU: v1 (Hongjun Wu, Tao Huang)
9. AES-OTR: v1 (Kazuhiko Minematsu)
10. AEZ: v1 (Viet Tung Hoang, Ted Krovetz, Phillip Rogaway)
11. Artemia: v1 (Javad Alizadeh, Mohammad Reza Aref, Nasour Bagheri)
12. (L) Ascon: v1 (Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer)
13. AVALANCHE: v1 (Basel Alomair)
14. (L) Calico: v8, withdrawn, (Christopher Taylor)
15. CBA: v1 v1-1 (Hossein Hosseini, Shahram Khazaei)
16. (L) CBEAM: r1, withdrawn, (Markku-Juhani O. Saarinen)

[*3] “lightweight” をキーワードとして応募ドキュメントを検索し、軽量性を方式の特徴として挙げているか、あるいは使用している演算や構成要素を軽量性を考慮して選定している方式をピックアップした。

17. CLOC: v1 (Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka)
18. (L) Deoxys: v1 (Jérémy Jean, Ivica Nikolić, Thomas Peyrin)
19. (L) ELmD: v1 (Nilanjan Datta, Mridul Nandi)
20. Enchilada: v1 v1.1 (Sandy Harris)
21. (L) FASER: v1, withdrawn, (Faith Chaza, Cameron McDonald, Roberto Avanzi)
22. HKC: v1, withdrawn, (Matt Henricksen, Shinsaku Kiyomoto, Jiqiang Lu)
23. HS1-SIV: v1 (Ted Krovetz)
24. ICEPOLE: v1 (PawełMorawiecki, Kris Gaj, Ekawat Homsirikamol, Krystian Matusiewicz, Josef Pieprzyk, Marcin Rogawski, Marian Srebrny, Marcin Wojcik)
25. iFeed[AES]: v1 (Liting Zhang, Wenling Wu, Han Sui, Peng Wang)
26. (L) Joltik: v1 (Jérémy Jean, Ivica Nikolić, Thomas Peyrin)
27. Julius: v1.0 (Lear Bahack)
28. (L) Ketje: v1 (Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche, Ronny Van Keer)
29. Keyak: v1 (Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche, Ronny Van Keer)
30. (L) KIASU: v1 (Jérémy Jean, Ivica Nikolić, Thomas Peyrin)
31. (L) LAC: v1 (Lei Zhang, Wenling Wu, Yanfeng Wang, Shengbao Wu, Jian Zhang)
32. Marble: v1.0 (Jian Guo)
33. McMambo: v1, withdrawn, (Watson Ladd)
34. (L) Minalpher: v1 (Yu Sasaki, Yosuke Todo, Kazumaro Aoki, Yusuke Naito, Takeshi Sugawara, Yumiko Murakami, Mitsuru Matsui, Shoichi Hirose)
35. MORUS: v1 (Hongjun Wu, Tao Huang)
36. NORX: v1 (Jean-Philippe Aumasson, Philipp Jovanovic, Samuel Neves)
37. OCB: v1 (Ted Krovetz, Phillip Rogaway)
38. OMD: v1.0 (Simon Cogliani, Diana-Ştefania Maimuţ, David Naccache, Rodrigo Portella do Canto, Reza Reyhanitabar, Serge Vaudenay, Damian Vizár)
39. PAEQ: v1 (Alex Biryukov, Dmitry Khovratovich)
40. PAES: v1, withdrawn, (Dingfeng Ye, Peng Wang, Lei Hu, Liping Wang, Yonghong Xie, Siwei Sun, Ping Wang)
41. PANDA: v1, withdrawn, Dingfeng Ye, Peng Wang, Lei Hu, Liping Wang, Yonghong Xie, Siwei Sun, Ping Wang)
42. (L) π-Cipher: v1 (Danilo Gligoroski, Hristina Mihajloska, Simona Samardjiska, Håkon Jacobsen, Mohamed El-Hadedy, Rune Erlend Jensen)
43. POET: v1 (Farzaneh Abed, Scott Fluhrer, John Foley, Christian Forler, Eik List, Stefan Lucks, David McGrew, Jakob Wenzel)
44. POLAWIS: v1 (Arkadiusz Wysokinski, Ireneusz Sikora)
45. (L) PRIMATEs: v1 (Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Florian Mendel, Bart Mennink, Nicky Mouha, Qingju Wang, Kan Yasuda)
46. (L) Prøst: v1 (Elif Bilge Kavun, Martin M. Lauridsen, Gregor Leander, Christian Rechberger, Peter Schwabe, Tolga Yalçın)
47. Raviyoyla: v1 (Rade Vuckovac)

48. (L) Sablier: v1 (Bin Zhang, Zhenqing Shi, Chao Xu, Yuan Yao, Zhenqi Li)
49. (L) SCREAM: v1 (Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici, François Durvaux, Lubos Gaspar, Stéphanie Kerckhof)
50. SHELL: v1 (Lei Wang)
51. (L) SILC: v1 (Tetsu Iwata, Kazuhiko Minematsu, Jian Guo, Sumio Morioka, Eita Kobayashi)
52. Silver: v1 (Daniel Penazzi, Miguel Montes)
53. STRIBOB: v1 (Markku-Juhani O. Saarinen)
54. Tiaoxin: v1.0 (Ivica Nikolić)
55. TriviA-ck: v1 (Avik Chakraborti, Mridul Nandi)
56. Wheesht: v1 (Peter Maxwell)
57. YAES: v1 v2 (Antoon Bosselaers, Fre Vercauteren)

3.3.2 まとめ

本章では、暗号技術調査 WG (軽量暗号 WG) の外部動向調査として、CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) プロジェクトについてまとめた。AES コンペティション、NESSIE プロジェクト、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、継続的に注視していくことが求められる。

3.4 軽量暗号の活用事例および標準化動向調査

3.4.1 調査目的

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。

3.4.2 活用事例調査

3.4.2.1 調査方法

以下に示す軽量暗号が活用されると期待されている分野について公開されている情報を調査する。

- RFID
- センサーネットワーク（環境測定等）
- 医療センサ
- ITS、自動車
- 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）
- その他

3.4.2.2 調査報告

3.4.2.1 章に挙げたそれぞれの項目について調査を行った。現段階で実際に軽量暗号が使用されているという公開の情報はない。そこで、これらの項目について、暗号についてどのように利用されているか、その中で軽量暗号がどのような導入方法が考えられるかを考察する。

■RFID、センサーネットワーク（環境測定等）、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）　これらについては、一般論となる情報のみが公開されていた [1, 2, 3]。無線ネットワーク接続機能を持つ RFID がインターネットのようなオープンなネットワークに接続する際に暗号を利用する。ほとんどの RFID、センサー、携帯端末デバイスの CPU は低スペックであり、信号処理を行う能力に乏しいこと、またメモリサイズも小さい。さらに、低消費電力での実装をしなければならず、軽量暗号に対する期待は極めて大きい。

■医療センサ　Texas Instrument[4] では、血圧、体温、心拍数、ブトウ糖等の測定を行い、Bluetooth で通信を行い、低消費電力のポータブル機器用のデバイス、MSP430FR59xx ファミリーを提供している。このデバイスの記事では、“政府標準である”256-bit AES を用いた医療用センサと記載されている。MSP430FR59xx ファミリーのスペックでは、MSP430microcotroller（16bitRISC CPU）を使用、メモリサイズは 32KB-256KB、消費電力は不明である。また、Position Paper[5] での報告として遠隔健康ケアシステムでは、埋め込みデバイスが使われており、これらとのコミュニケーションをとる際にセキュリティ技術が必要。そして、これらを Ultra-low-power で行いたいとしている。この論文では、待機電力を減らす、置換を減らすなどによるアルゴリズムの簡素化が主体で低消費電力化を図っている。

■ITS、自動車　ITS（Intelligent Transport Systems:高速道路交通システム）は、人と道路と自動車の間で情報の共有を行い、交通の最適化を図るシステムとして作られたシステムである [6]。そして、”安全”が強調されたシステム造

りが目指されている。そして、その基本構成である自動車搭載機器について、装置機器間のデータの秘匿、認証のために暗号が利用されることが謳われている [7, 8, 9, 10]。これらについても、リソースが限られているとはわかっているものの、軽量暗号を使用する段階には至っておらず、軽量暗号を使うことを提案している段階 [11] である。

■記録メディア（HDD、SSD 等）　SandForce[12] ではセキュリティ機能を持つ SSD を提供している。Windows8 の PC やタブレットにおいても低消費電力の記録デバイス（SSD）が必要であった。このため、従来品が 20mA を利用していたのに対し、0.05mA で動作するようにしている。モバイル端末でも利用可能であるとのこと。

■その他　ICT 社会において、ETC システムにおいても暗号化が使われている。このシステムではプライバシ保護のため、認証、暗号化などが必要となる [13]。　その他、軽量暗号の一般的な利用可能性については、軽量暗号関係の多くの論文 [14, 15] で書かれている。

3.4.2.3　ヒアリング

メーカー数社にヒアリングを行い、軽量暗号に対する考え方を調査した。その結果を以下に示す。最近の測定器や家電はほぼ CPU が積まれ、ネットワーク接続が可能となっているが、使用目的によって要求条件が異なっている。大きくわけて以下の 2 つのケースがある。

1. 一つのハードウェアもしくはソフトウェアに入れる機能が確定している場合
2. 一つのハードウェアもしくはソフトウェアに入れる機能が確定しておらず、いろいろな機能を入れる場合

前者は医療センサのように使用用途が厳密に限られる場合、後者は PC やタブレットのように汎用の機器であり、使用目的が厳密に制限されていない場合である。

■ケース 1 について

- セキュリティが必要で AES を入れたければ、外部モジュールとして AES チップを使う、もしくは、ソフトウェアとして AES を入れられるスペックの CPU やメモリを搭載する。
- 軽量暗号をあえて導入する必要を感じていない。チップサイズ（消費電力を含む）が小さくなればよいという一般論があるが、どれほど小さいチップが必要であるかの指定はない。

■ケース 2 について

- CPU、メモリなどのリソースをそれぞれの機能でシェアして使用する。欠点として、機能が多くなりリソースを取り合うことが生じる。
- ハードウェア、ソフトウェアの構築段階でどの機能を必須として使うかを決める。これにより、リソースを分割する度合い（量、順位）が決まる。
- AES が使用困難であり、軽量暗号であれば使用可能、というアプリケーションは少ない。
- リソースを削られたとしても高速な動作が保障されるような暗号方式として軽量暗号が求められていることはある。

3.4.2.4　活用事例のまとめ

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。ただし、医療センサの項で紹介した Texas Instrument のように、標準として認められることで使用する業者があるということも事実で

ある。従って、CRYPTREC などの機関で調査・評価することは、軽量暗号の利用促進に供する情報を提供できると考えられる。

3.4.3 標準化動向調査

3.4.3.1 調査方法

軽量暗号の標準化について、ISO/IEC JTC 1/SC 27/WG 2 で進められてきた標準化内容を調査する。また、IETF Light-Weight Implementation Guidance(lwig) で行われている軽量暗号の実装に関するガイダンスについてまとめる。

3.4.3.2 ISO/IEC JTC 1/SC 27/WG 2 の活動

ISO/IEC 29192 は、チップサイズ、ハードウェアの消費電力、ソフトウェアのコードサイズ、RAM サイズ、伝送容量、実行時間などの制限がある場合の、データ秘匿、認証、本人識別、否認防止、鍵交換などを目的に適した軽量暗号の仕様を標準化している。ISO/IEC JTC 1/SC 27/WG 2 では技術カテゴリに対応し以下の 4 つのパートに分かれてこの標準化作業が行われた。これらの標準化作業はすべて 2013 年までに終了し、各パートの内容が ISO/IEC 29192-1，-2，-3，-4 として標準化されている。

■パート 1：総論　安全性要件、ハードウェア／ソフトウェア実装要件が規定された。

■安全性要件　80 ビットセキュリティ以上

■ハードウェア実装要件　ハードウェアチップ面積、実行サイクル数、1 サイクル当たりの処理ビット数、消費電力、消費電力量、1 ビット当たりの消費電力量、実装に用いられたルールが方式比較のための参考情報とされた。但し、これらの具体的な数値はアプリケーション依存であるため、規定しない。

■ソフトウェア実装要件　プログラムコードサイズ、RAM サイズ、実行速度が方式比較のための参考情報とされた。但し、これらの具体的な数値はアプリケーション依存であるため、規定しない。

■他の特性　　軽量暗号は、短い平文、暗号文に対する処理も重要な要素となる。可能であれば、その特性が示されるべきである。また、実装に伴う遅延についても重要な要素となる。

■パート２：ブロック暗号　２つのブロック暗号、PRESENT と CLEFIA が標準化された。

・PRESENT　ブロックサイズ 64 ビット、鍵サイズ　80、128 ビット
・CLEFIA　　ブロックサイズ 128 ビット、鍵サイズ　128、192、256 ビット

■パート３：ストリーム暗号　２つのストリーム暗号、Enocoro と Trivium が標準化された。

・Enocoro　鍵サイズ 80、128 ビット
・Trivium　鍵サイズ 80 ビット

■パート４：公開鍵暗号（非対称暗号）技術を用いたメカニズム　公開鍵暗号技術を用いた、楕円上の離散対数問題をベースにした認証方式（cryptGPS）と、公開鍵暗号をベースにしたセッション鍵生成・鍵交換方式 (ALIKE) と、Identity ベース署名方式の 3 つが標準化された。

3.4.3.3 IETF における軽量暗号の実装に関するガイダンス

建物、車、電化製品などで使われている多くのデバイスでコミュニケーションができるようになってきた。但し、これらのデバイスの能力は様々であり、能力の小さいデバイスもある。IETF Light-Weight Implementation Guidance (lwig) では、このような小さい能力のデバイスに焦点をあて、非常に制限された環境下で、最小限の IP 接続を可能とする軽量暗号の実装方法、について標準化することを目的とする [16]。現在、lwig で議論が開始された段階であり、インターネット上での鍵交換関連 [17]、モーバイルネットワークでの低消費電力デバイス関連 [18]、TLS のカスタマイズ関連 [19] などの寄与文書が WG に提出されてきているが、まだ RFC 化されたものはない。

なお、lwig とは独立であるが、CLEFIA の暗号アルゴリズムが RFC6114 となっている。

参考文献

[1] PRWeb,“IEC and ISO adopt lower power encryption standard Enocoro stream cipher,”http://www.prweb.com/releases/2012/11/prweb10132688.htm

[2] M. B. Abdelhalim, M.El-Mahallawy, and A. Elhennawy,“Design & Implementation of an Encryption Algorithm for use in RFID System,”International Journal of RFID Security and Cryptography, Vol.1, Issues1-4, Mar-Dec. 2012.

[3] TechRepublic, “Is wireless RFID sensor authentication / encryption possible? Maybe.” http://www.techrepublic.com/blog/it-security/is-wireless-rfid-sensor-authentication-encryption-possible-maybe/

[4] TEXAS INSTRUMENT, “Ultra-low Power Microcontrollers for Portable Medical Device Designs,” http://www.engineering.com/ElectronicsDesign/ElectronicsDesignArticles/ArticleID/6222/ Ultra-low-Power-Microcontrollers-for-Portable-Medical-Device-Designs.aspx

[5] F. H. Qi Hao, and M. Lukowiak, “Implantable Medical Device Communication Security: Pattern vs. Signal Encryption (Position Paper),” https://www.usenix.org/legacy/evnet/healthsec11/tech/final_files/hu-healthsec11.pdf

[6] ITS Japan,「ITS とは」, http://www.its-jp.org/about/

[7] IPA,「2012 年度自動車の情報セキュリティ動向に関する調査」, http://www.ipa.go.jp/files/000027274.pdf

[8] EVITA,“E-safety vehicle intrusion protected applications,” http://www.evita-project.org/

[9] PRESERVE,“PRESERVE preparing secure v2x communication systems,” http://www.evita-project.org/

[10] SAE,“Vehicle Electrical System Security Committee,” http://www.sae.org/works/committeeHome.do?comtID=TEVEES18

[11] 野島，盛合,「『シェア暗号』を自動車に」, http://techon.nikkeibp.co.jp/article/COLUMN/20140401/343501/?rt=nocnt

[12] The TECH REPORT, “SandForce Improves SSD encryption, power management,”http://techreport.com/news/24894/sandforce-improves-ssd-encryption-power-management

[13] 松井,「情報セキュリティ基盤技術暗号技術の最新動向- Cryptography:Technology and Applications -」, http://hiroshi1.hongo.wide.ad.jp/hiroshi/files/toku1/material/Matsui_Mitsubishi.pdf

[14] Axel Poschmann,“Lightweight Cryptography,” http://mathsci.ucd.ie/~gmg/ECC2007Talks/poschmann_LWC.pdf

[15] 鈴木，菅原，佐伯,「軽量／低遅延暗号のハードウェア実装性能について」, SCIS2014, 2A2-2

[16] IETF, “Light-Weight Implementation Guidance (lwig),”https://ietf.org/wg/lwig/charter/

[17] T. Kivinen, "Minimal IKEv2 draft-ietf-iwig-ikev2-minimal-01", https://ietf.org/doc/draft-ietf-lwig-ikev2-minimal/

[18] J. Arkko, A. Eriksson, and A. Keranen, "Minimal IKEv2 draft-ietf-iwig-ikev2-minimal-01," https://ietf.org/doc/draft-ietf-lwig-cellular/

[19] S. S. Kumar, S. Keoh, and H. Tschofenig, "Minimal IKEv2 draft-ietf-iwig-ikev2-minimal-01," https://ietf.org/doc/draft-ietf-lwig-tls-minimal/

第 4 章

軽量暗号のアプリケーションに関するヒアリング

2013 年度第 2 回軽量暗号 WG にて、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。

2013 年度第 2 回軽量暗号 WG での発表資料を、参考資料として本報告書の A.1 章に掲載している。

第 5 章

軽量ブロック暗号の実装詳細評価

第 2 章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、既存文献では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、情報通信研究機構にて、軽量ブロック暗号 (AES, Camellia, CLEFIA, PRESENT, LED, Piccolo, TWINE, PRINCE) 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調査を実施した。この評価結果が 2013 年度 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	512 B	1024 B
RAM	64 B	128 B

■評価結果概要　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 200 B 以下、RAM 32 B 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。

2013 年度 第 3 回軽量暗号 WG での発表資料を、参考資料として本報告書の A.2 章に掲載している。

付録 A

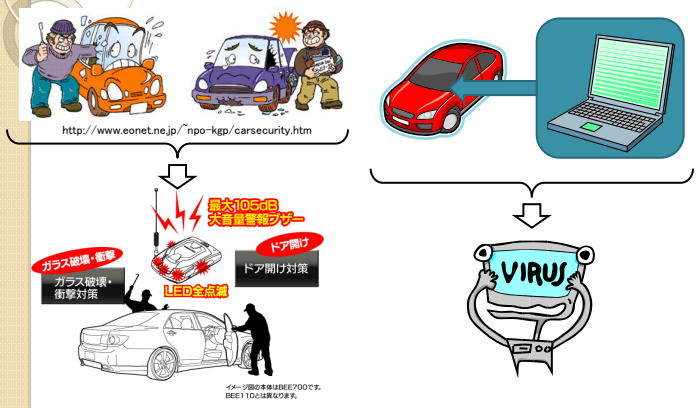
参考資料

A.1　軽量暗号のアプリケーションに関するヒアリング

A.1.1　自動車における IT セキュリティ

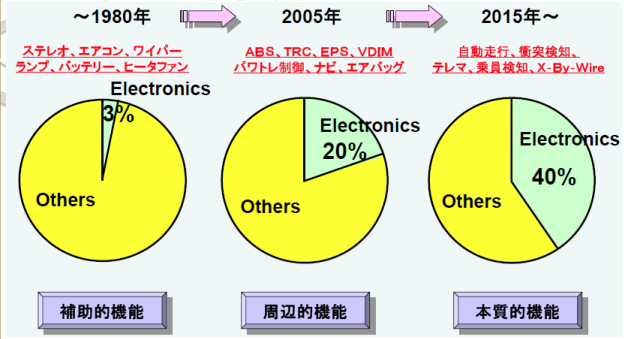
2013 年度 第 2 回軽量暗号 WG (2013 年 12 月 26 日) でのトヨタ IT 開発センター 小熊 寿氏による発表資料を示す。

「クルマ」×「セキュリティ」



http://www.kato-denki.com/products/bee/bee110/img/standard_sensor.png

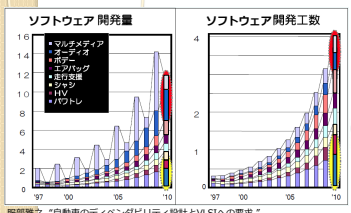
クルマの電子化

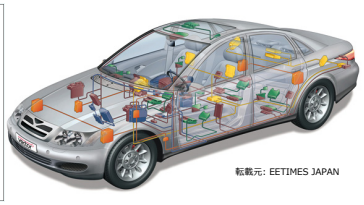


服部雅之, "自動車のディペンダビリティ設計とVLSIへの要求,"
JST CREST「ディペンダブルVLSIシステムの基盤技術」研究領域 平成19年度ワークショップ

- 1970年代の排ガス規制
  - エンジン状態を監視し、燃料噴射量と点火タイミングを制御
  - 電子部品導入のきっかけ

現在のクルマ





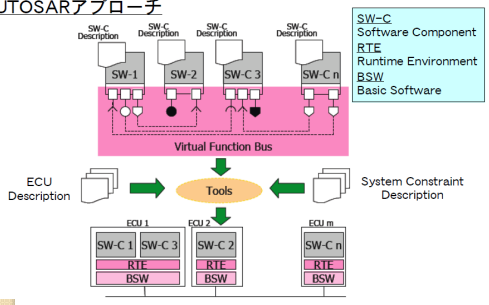
転載元: EETIMES JAPAN

服部雅之, "自動車のディペンダビリティ設計とVLSIへの要求,"
JST CREST「ディペンダブルVLSIシステムの基盤技術」研究領域 平成19年度ワークショップ

- 高級車の事例: LEXUS LS460
  - 100個以上の車載制御マイコン (ECU: Electronic Control Unit)
  - SWの総ライン数はカーナビなどを含めると17M行: 雑誌報道による数値
    - 2015年には100M行という予測も...
- ECUが連携してサービスを提供
  - e.g. 車体姿勢制御、プリクラッシュセーフティ
  - SWの大規模化と複雑化↑

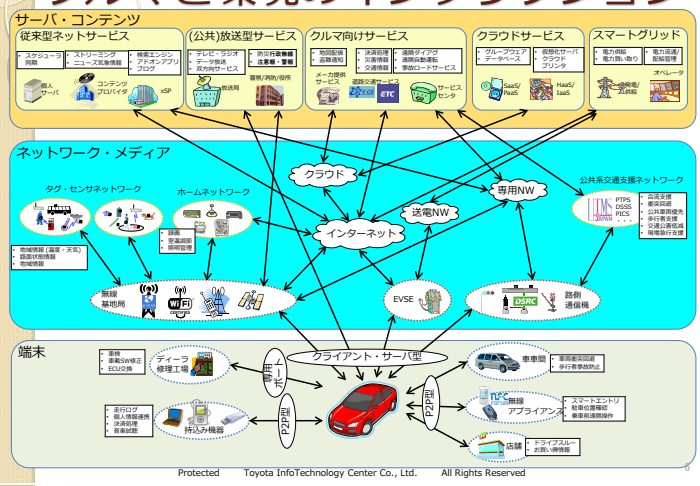
プラットフォームベース開発

AUTOSARアプローチ



- 基盤機能共通化による開発工数およびコストの削減
  - プラットフォームベースの開発へ移行
- AUTOSAR (Automobive Open System Architecture): 2003～
  - SW基盤の業界標準を作成
- JasPar (Japan Automotive Software Platform): 2004～
  - 国内メーカの要望を集約し、AUTOSARへのインプットなどを行う

クルマと環境のインタラクション



標準化とコンピュータ

- 攻撃者がクラック出来る環境
  - 仕様書が閲覧可能であり、セキュリティホールも確認出来る
- 全く同じ事象が起きる環境
  - 1台さえ解析できれば、他も同じアーキテクチャであるため同じ手法が適用可能
- 情報伝搬速度が早い
  - ほとんどのPCがネットワーク接続しているため、瞬時に広範囲に影響する

- アーキテクチャの変化：「機種毎」⇒「みんな同じ」
- 仕様書の公開

- 外部からの侵入口
- 情報発信

1980年代後半
機能の標準化

1990年代前半
インターネット接続

メインフレーム

PC/AT互換機

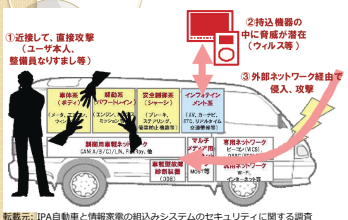
ワークステーション

- 「標準化」と「NW接続」する将来のクルマ
  - 同じサイクルにはまる可能性大

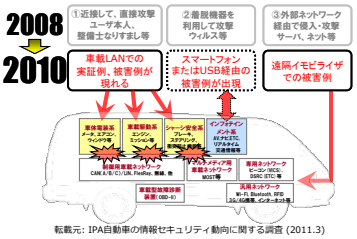
クルマの要求条件

- ハードリアルタイムとFail-Safe
  - 生命に直結するため時間制約が厳しい (即時応答性)
  - 不具合が起きたときに安全側に倒れる事
- 10年以上の耐用年数
  - 製造から廃車までの時間が長く、中古車市場にも転用
- 不具合発生を事前に防止
  - PC: ウイルス感染などの被害が現れてからの対応が多い (セキュリティSWメーカによる事前調査もある)
  - クルマ: 事故など具体的な被害が出る前に対応する必要あり
- 切断時動作
  - NW接続はモバイル機器と同様に無線: 生命に直結するサービスを常時接続前提で考えてはいけない
- 劣悪な環境での動作、信頼性
  - 電圧変動±50% 動作環境温度−40〜140℃

2010年に潮目が変化



転載元: IPA自動車と情報家電の組込みシステムのセキュリティに関する調査 (2009.3)



転載元: IPA自動車の情報セキュリティ動向に関する調査 (2011.3)

- 想定される脅威の列挙
  - 「机上の空論」: 〜のでは?
  - 想定ベースの議論であり、説得性に欠ける: Evidence 不足
- 攻撃結果の公開
  - 予想した脅威が現実化
  - 事例として対外発表が行われる
- 具体的な事故は未報告
  - 想定外の事象が起こる可能性は否定できない

周辺動向

- 海外
  - 国プロ関連
    - 欧州によるFramework Program: 製品化を見据えた研究・標準化活動
      - SeVeCom (FP6): 路車間・車車間通信のセキュリティ
      - EVITA (FP7): 車載システムのセキュリティ
  - 学会
    - Escar: Embedded Security in Cars Conference
  - 産業界
    - SAE Vehicle Electrical System Security Committee (2011〜): NHTSAによるCybersecurity Researchと連携
- 国内
  - 情報処理推進機構による研究会
    - 2006年、2008年〜2011年: クルマ向け情報セキュリティ動向と想定される脅威を調査
  - 産業界
    - 自動車技術会による情報セキュリティ小委員会 (2010〜)

escar: Embedded Security in Cars Conference

- 2003年から毎年ドイツ国内で開催
  - 2003年は20名程度、2008年からはCFP

	2009年	2010年	2011年	2012年	2013年
参加者	54	72	74	112	110
うち日本人	1	3	5	7	16

*参加者リストを参照

- 2013年からはUS、2014年からはアジアでも実施
  - 次回escar USAは7月、CFPの予定
  - 1st escar ASIAは4月

Trusted Assurance Levels

- C2C-CCにて検討中

TAL	Security Evaluation Requirements			Resulting Security Implications		
	Minimum Target of Evaluation (TOE)	Minimum Evaluation Assurance Level (EAL)	Minimum (Hardware) Security Functionality	Prevented (Internal) Attacker acc. to CC	Potential Security Implications	V2X Use Case Examples
0	None	None	None	None	Not reliable against security attacks	Some limited (e.g., using trusted V2I infrastructures)
1	+ V2X software	EAL 3	Only software security mechanisms	Basic	Not reliable against simple hardware attacks (e.g., offline flash manipulation)	Non-safety, but most privacy relevant use cases
2	+ V2X hardware	EAL 4	+ dedicated hardware security (i.e., secure memory & processing) + tamper evidence	Enhanced Basic	Not reliable against more sophisticated hardware attacks (e.g., side-channel attacks)	V2X day one use cases (e.g., passive warnings and helpers)
3	+ Private ECU & private network	EAL 4+ (AVA_VAN.4 vulnerability resistance)	+ basic tamper resistance	Moderate	V2X box secure as stand alone device, but w/o trustworthy in-vehicle inputs	Safety relevant relying not only on V2X inputs
4	+ Relevant in-vehicle sensors and ECUs	EAL 4+ (AVA_VAN.5 vulnerability resistance)	+ moderate – high tamper resistance	Moderate – High	V2X box is trustworthy also regarding all relevant in-vehicle inputs	All

- Marko Wolf, – Hardware Security Modules for Protecting Automotive IT Systems – The EVITA project and beyond, escar USA 2013

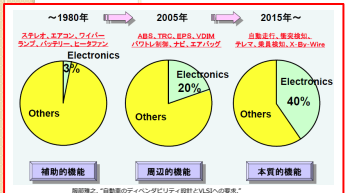
Vehicle Electrical System Security Committee

- SAEにて2011年から活動開始
  - 車載システムへの攻撃に関する研究発表などがトリガ
- 2つのタスクフォース
  - Automotive Security Guidelines and Risk Development
    - プロセスベースで車載システムのセキュリティレベルを策定
    - リスクを軽減するためのガイドラインおよび推奨デザインを作成
    - 2014年夏に初版リリースを目指す
  - Vehicle Electrical Hardware Security
    - ハードウェアベースのセキュリティ技術を利用
    - 「車載システムのセキュリティ」担保のための推奨デザインを作成
    - 2014年1月に作業完了予定

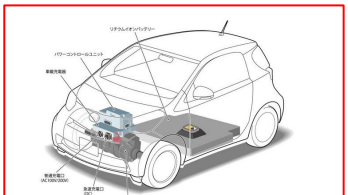
Battelle CyberAuto Challenge

- 自動車を中心とした交通システムに対する脅威と防御について学習
  - 高校/大学生向けサマーキャンプ: 1週間程度
  - USビッグ3やUS政府関係者などによる実地サポート
  - 実際に自動車をクラック
- 今年が第2回目

今後のクルマ



高度サービス・コスト削減のための電子化


電子部品比率が増えるEV

- 「計算機科学的アプローチ」によるセキュリティ技術が重要かつ必須
- 「EVならでは」も存在
  - EVは高トルク: エンジンチューンナップによる想定外の動き
  - 安価なサードパーティ製バッテリ: ただでさえEVは走行距離が短く、販売価格の30%を占めるバッテリ

まとめ

- クルマへの情報セキュリティ技術の必要性
  - 要因: 電子化比率の増加、標準化、EV化
- 気をつけること
  - ヒトの命を預かる耐久消費品
- 国内技術者の絶対的な不足

A.1.2　制御システム向け暗号の要件の考察

2013 年度 第 2 回軽量暗号 WG (2013 年 12 月 26 日) での日立製作所 大和田 徹氏による発表資料を示す。

HITACHI
Inspire the Next

CRYPTREC 軽量暗号WG

制御システム向け暗号の要件の考察

2013/12/26
(株)日立製作所 横浜研究所
大和田 徹

1　IT分野における情報セキュリティ

HITACHI
Inspire the Next

情報システムに対する様々なセキュリティ上の脅威が存在

■ 情報システムにおける主な脅威
- 情報漏えい、盗聴、なりすまし、不正アクセス
- データ/プログラムの改ざん、ウィルス感染
- DoS攻撃によるネットワーク/サーバのダウン、データ/プログラムの削除

■ 情報セキュリティ:
情報資産(保護資産)の定義 + 当該資産に対する3要素の維持

要素	定義	代表的な対策技術
機密性	認可されていない個人、エンティティまたはプロセスに対して、情報を使用不可または非公開にする特性	暗号、認証、アクセス制御
完全性	資産の正確さ、および完全さを保護する特性	改ざん検知、ログ管理、バックアップ
可用性	許可されたエンティティが要求したときに、アクセスおよび使用が可能である特性	ファイアウォール、リソースの多重化

情報システムでは各種対策技術を組合せて情報資産のセキュリティを確保

2 制御システム分野における情報セキュリティ優先事項

HITACHI Inspire the Next

制御システムにおける重要な保護資産とは

■ 制御システムと情報システムの比較(*)

比較項目	制御システム	情報システム
データ処理制約	リアルタイムかつ周期的な制御処理 ⇒遅延により制御不全に陥る可能性	処理集中による遅延は、 ある程度許容
システム更新頻度	10-20年	3-5年
稼動時間	24時間365日連続	一般には通常業務時間内
想定被害	システム不具合による人命影響の 可能性	金銭的損失、 プライバシー被害
優先保護資産	システムの連続稼動(可用性)	情報資産の漏洩防止(機密性)

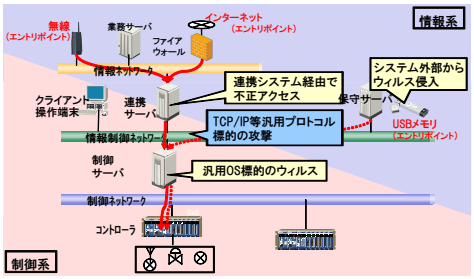
セキュリティ上の脅威に晒されても
制御システムが連続稼動すること(可用性)が最重要

＊IPA「重要インフラの制御システムセキュリティとITサービス継続に関する調査」を元に作成
http://www.ipa.go.jp/security/fy20/reports/ics-sec/

3 制御システムの一般的構成と脅威例

HITACHI Inspire the Next

昨今の制御システム～IT + CTのハイブリッド構成



物理アクセス性はシステム
によりまちまち
発電所、プラント～ビル
～スマートメータ

情報系部分は既存手法によるサイバー攻撃の対象となり得る
制御系部分への侵入で制御不全に

4 攻撃の顕在化と、それに対抗する動き

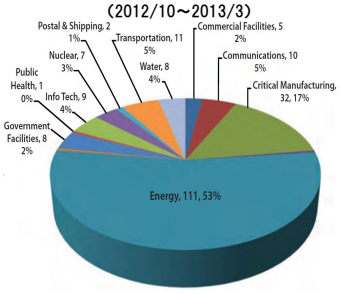
HITACHI Inspire the Next

制御システムへのサイバー攻撃が顕在化(12/下 200以上の報告),
制御システムに対するセキュリティ強化の要求が高まる

- WIB等, 業界レベルのセキュリティ規格策定段階から
  EDSA認証(CSSC)・CSMS認証(JIPDEC)等の
  国際的なセキュリティ認証制度整備段階へ進展
- ICS-CERTによる脆弱性公開が加速

コンポーネント/システムの
セキュリティ設計, セキュリティ運用
の重要性増大

重要インフラにおけるセキュリティ事故報告
(2012/10～2013/3)

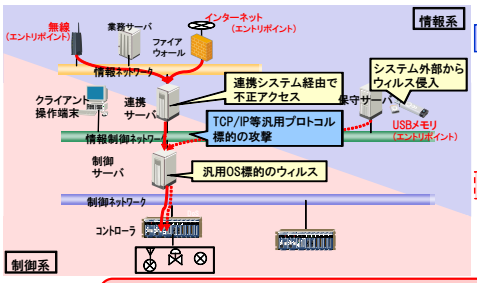


出典：米ICS-CERT,
http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf

5 制御システムにおけるセキュリティ対策

HITACHI Inspire the Next

**昨今の制御システム～IT + CTのハイブリッド構成
ITベース攻撃手法の対象となり得る**



対抗策
3要素を組合せた最新の
情報系セキュリティ対策技術

（大） （汎用・標準）
外部接続 採用技術
（小） （専用・独自）

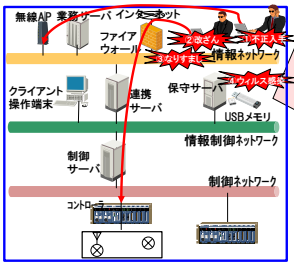
対抗策
制御系の特徴を考慮した
セキュリティ対策技術

制御系の特徴を考慮した対策技術の確立が急務

6 制御システムの可用性確保に向けた対策技術

HITACHI Inspire the Next

制御システムの可用性を損なう主要な脅威の洗い出し



可用性を損なう主要な脅威とその対策方針

#	脅威	対策方針
①	第三者がシステム内を流れるデータを不正に入手し、誤作動を引き起こすために悪用する(不正パケットの送信など)	パケットの内容が理解できないようにする
②	第三者がコントローラ宛のデータを改ざんし、コントローラが誤った制御指令をセンサに送信してしまう(誤動作、機能低下)	不正パケットを検知する
③	第三者が保守サーバになりすまして制御サーバを乗っ取り、コンローラの誤動作を引き起こす	通信相手が正しいことを確認する
④	保守員が保守サーバにアクセスする際、保守サーバに接続する可搬型記憶媒体(USBなど)がウィルスに感染していた為、ウィルスがシステム内に侵入し、プログラムやデータの改ざん/破壊、DoS攻撃を行う(システムを停止するため)	ウィルスを検知する

暗号技術が可用性確保に繋がる分野が存在

7 暗号適用時の課題

HITACHI Inspire the Next

制御系への暗号適用影響を分析し、課題を抽出

#	制御系の制約	暗号適用時に想定される影響	暗号適用時の課題	
1	周期的/リアルタイム処理	負荷増加により、周期的/リアルタイム処理の困難化	レイテンシ制約	性能
2	組込み機器のリソース制約(CPU性能、メモリ容量等)	高処理負荷暗号の実行によるシステム通常動作の困難化	暗号による処理負荷大	性能
3	全てがクリティカルな制御情報とは限らない	制御データ全てを暗号化対象とすると処理負荷大	不必要な暗号処理による不要な処理負荷の発生	性能/安全性
4	連続稼動	鍵管理/鍵更新処理がシステムの連続稼動に影響	連続稼動に影響しない鍵管理/鍵更新方式が確立されていない	運用
5	長期運用(10-20年)	暗号危殆化の可能性	暗号危殆化による安全性低下	運用

上記課題を解決する暗号機能の実現が求められている

＊ JPCERT/CC「重要社会インフラのためのプロセス制御システムのセキュリティ強化ガイド」を元に作成
www.jpcert.or.jp/research/2009/PCSSecGuide_20091120.pdf

8 制御システム向け暗号の要件

HITACHI Inspire the Next

課題から制御システム向け暗号の要件を抽出

#	【再掲】課題/課題の区分		制御システム向け暗号の要件
1	レイテンシ制約	性能	高速処理可能
2	暗号による処理負荷大	性能	低処理負荷
3	不必要な暗号処理による不要な処理負荷の発生	性能/安全性	柔軟な暗号化対象長
4	連続稼動に影響しない鍵管理/鍵更新方式が確立されていない	運用	低リソースな鍵管理/鍵更新機能
5	暗号危殆化による安全性低下	運用	複数鍵長/アルゴリズムの切替容易

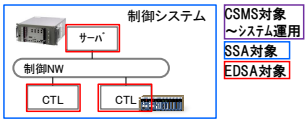
制御システム向けに上記要件を満たす「軽量暗号」が役立つ可能性はある

9 制御コンポーネントのセキュリティ認証

HITACHI Inspire the Next

動向

- IEC62443に則ったｾｷｭﾘﾃｨ評価認証ｽｷｰﾑ整備中
  - 事業・運用者向けCSMS認証(→IEC62443-2)
  - システムベンダ向けCSS認証(→IEC62443-3)
  - **装置ベンダ向けEDSA認証(→IEC62443-4)**
    - 将来的な調達要件化が想定
    - 総構造認証～システム認証は認証機器が前提



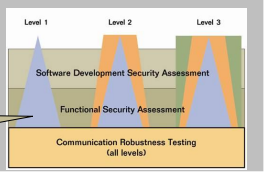
- CSSCがEDSA国際相互認証ｽｷｰﾑを準備中
  EDSA認証取得機器：2社4製品(‘13/12時点)

EDSA認証

ISAセキュリティ適合性協会(ISCI)が運営する制御機器のセキュリティ保証に関する認証制度

評価項目としては
1. 機能セキュリティアセスメント(FSA)
2. ソフトウェア開発セキュリティアセスメント(SDSA)
3. 通信ロバストネステスト(CRT)

の3項目が存在。



レベル1でのFSA要求は主にユーザ認証アクセスコントロール、データ完全性、機密性要求はレベル2以上で
→暗号化以前の課題が山積

出典：米ISA Secure
http://www.isasecure.org/ISASecure-Program.aspx

10 まとめ～制御システム向け暗号への期待

HITACHI Inspire the Next

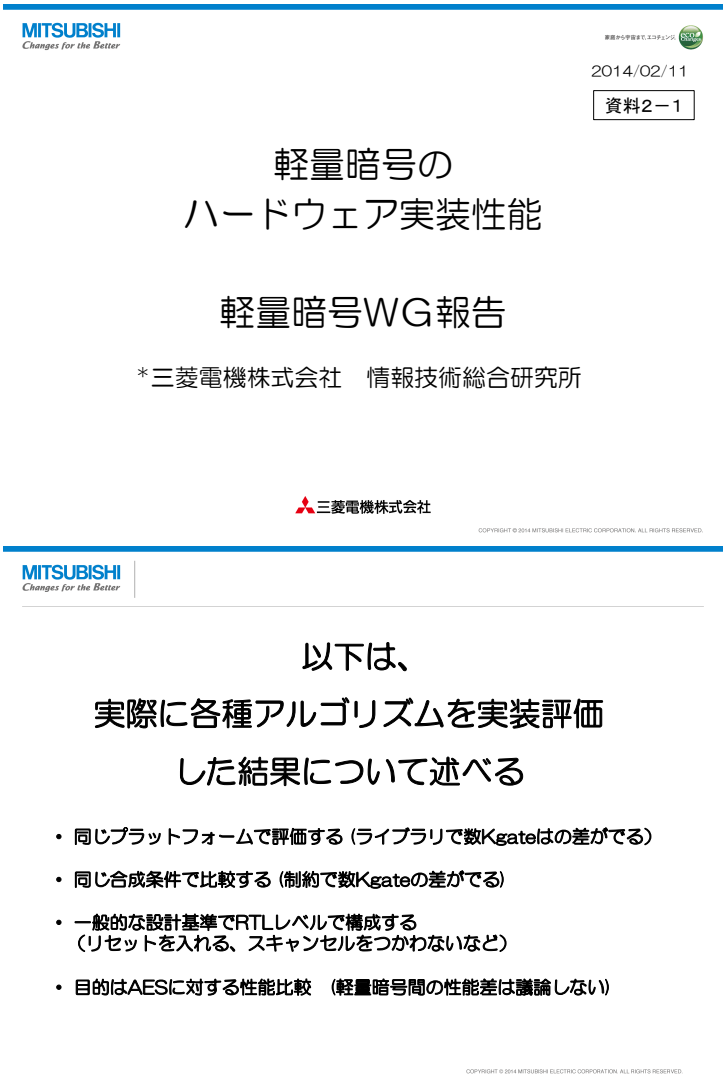
**実現したいシステムセキュリティからすると
暗号は数多くの要件のうちの一つ
～「グローバルで使い易い」暗号を期待**

- 暗号アルゴリズムだけ、では使いこなせない
  - 鍵管理手法等も含めたシステムパッケージを期待
  - 制御向けの暗号使い方ガイドを期待
- 制御コンポーネントは汎用技術活用の方向
  - 専用HWを必要としない組込みCPUに適した暗号を期待
- 評価認証スキームの確立と国際調達要件化
  - 国際標準でない暗号の採用困難化の方向→使える暗号の国際標準化推進を期待

A.2　軽量ブロック暗号の実装詳細評価

A.2.1　ハードウェア性能評価

2013 年度 第 3 回軽量暗号 WG (2014 年 2 月 20 日) での三菱電機 鈴木 大輔氏による発表資料を示す。



MITSUBISHI
Changes for the Better

2014/02/11

資料2－1

軽量暗号の
ハードウェア実装性能

軽量暗号WG報告

＊三菱電機株式会社　情報技術総合研究所

三菱電機株式会社

MITSUBISHI
Changes for the Better

以下は、
実際に各種アルゴリズムを実装評価
した結果について述べる

- 同じプラットフォームで評価する (ライブラリで数Kgateはの差がでる)
- 同じ合成条件で比較する (制約で数Kgateの差がでる)
- 一般的な設計基準でRTLレベルで構成する
  (リセットを入れる、スキャンセルをつかわないなど)
- 目的はAESに対する性能比較　(軽量暗号間の性能差は議論しない)

MITSUBISHI Changes for the Better

機能概略

F1. 鍵長は規定される最小のモードを想定する.

F2. 暗号化のみの実装とする.
(一部暗号化・復号も実装したので報告する)

F3. CPU のコプロセッサとしての利用を想定し，コンパクトで低電力とされるAPB バス接続が可能な設計とする.

MITSUBISHI Changes for the Better

設計方針概略

P1. 各アルゴリズムに対して3 種類の実装を行う:

(i) 典型的なround ベースの実装
(ii) 1 サイクルで処理が完了するunrolled 実装
(iii) データパスをS-box のサイズとするserial 実装

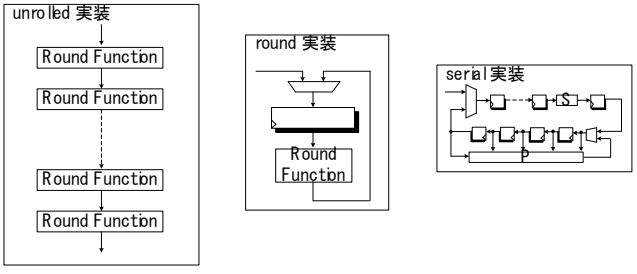
P2. 鍵スケジュールはon-the-yで実装する.

P3. CMOS セルライブラリを直接インスタンスするような最適化は行わず，ライブラリ非依存で合成可能な記述とする.

MITSUBISHI Changes for the Better

アーキテクチャ

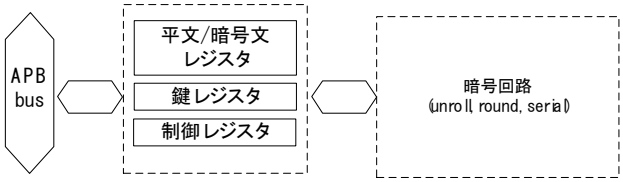
■実装方式



MITSUBISHI Changes for the Better

インターフェース

■インターフェース



MITSUBISHI Changes for the Better

評価環境

オープンセルライブラリと標準的なツールを使用.

論理合成ツール	Design Compiler (G-2012.06-SP5)
ライブラリ	NANGATE Open Cell Library(45nm CMOS)
合成制約	面積最小
遅延条件	NangateOpenCellLibrary slow (最悪条件の仮想遅延)
論理シミュレータ	NC-Verilog 10.20-s040
使用言語	Verilog-HDL

MITSUBISHI Changes for the Better

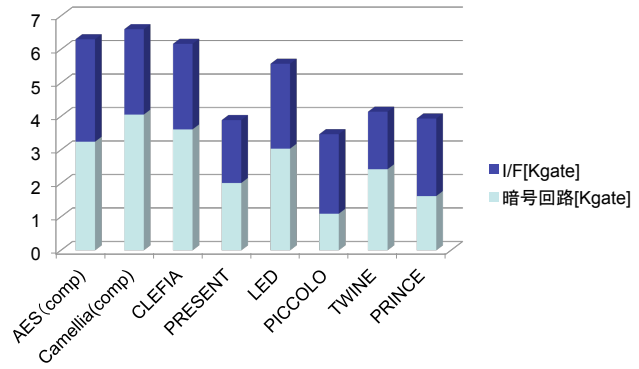
暗号化のみ

MITSUBISHI Changes for the Better

Serial

ゲートサイズ

AESに対して他のアルゴリズムは-2Kgateから+1Kgateの範囲

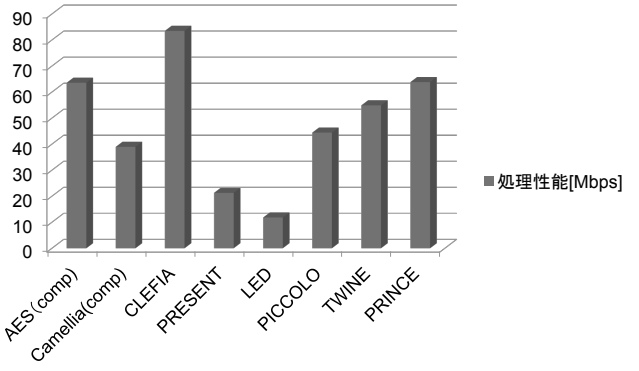


MITSUBISHI Changes for the Better

Serial

スループット

軽量暗号はSerial実装で高速化しにくい

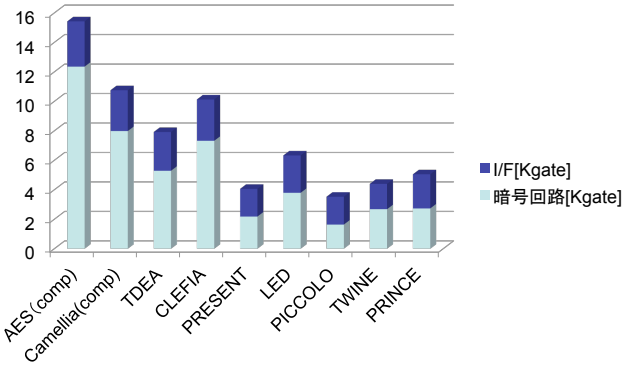


MITSUBISHI Changes for the Better

Round

ゲートサイズ

AESに対して軽量暗号はRound実装とSerial実装の回路規模に差がほとんどなく、4Kgate以下で実装できる

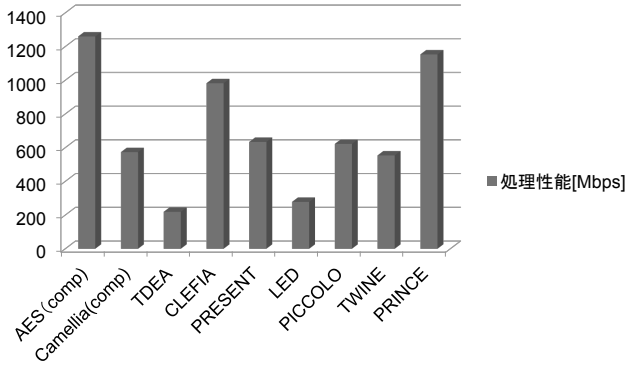


MITSUBISHI Changes for the Better

Round

スループット

軽量暗号はRound実装の軽量暗号はSerial実装のAESに対して速度性能約10倍

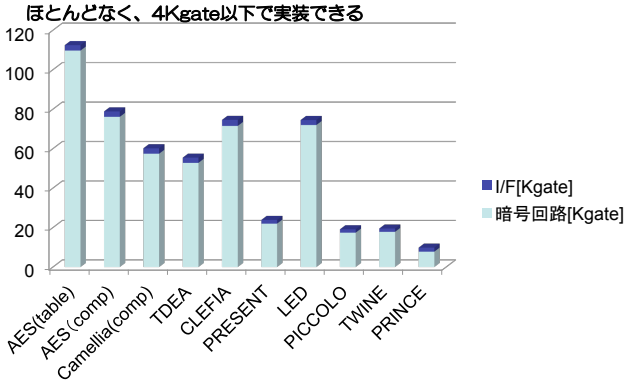


MITSUBISHI Changes for the Better

Unrolled

ゲートサイズ

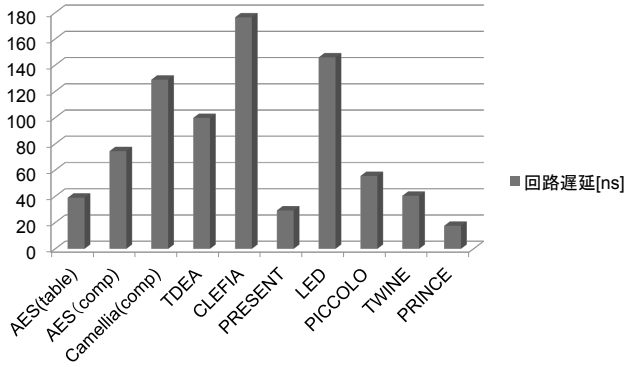
AESに対して軽量暗号はRound実装とSerial実装の回路規模に差がほとんどなく、4Kgate以下で実装できる



MITSUBISHI Changes for the Better

Unrolled

回路遅延



MITSUBISHI Changes for the Better

差分のまとめ

- 「論理回路性能の視点から」　軽量暗号とAESの違い

  ① 回路規模は１～2Kgate軽量暗号の方が小さい

  ② 約3Kgate以内でつくるなら軽量暗号の方がサイクル数が1/10

  ③ ②と同じサイクル数を達成するためにはAESは約10Kgate必要

  ④ 「1サイクル暗号化」に必要な回路規模が2ケタ違う。

  ⑤ 1サイクルとしてとれる周波数が2～3倍低遅延暗号が高速

MITSUBISHI Changes for the Better

RFIDをメインアプリと想定した場合

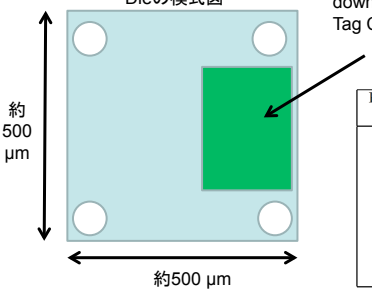
軽量暗号のハードウエア実装のアプリケーションと言えば「RFID」

この領域のアプリケーションでは処理時間は通信時間の方が支配的であることが多い

（②、③よりも）①の視点が産業上の有用性を見出せるか？

MITSUBISHI Changes for the Better

RFIDにおける実装制約



http://www.impinj.com/support/downloadable_documents.aspx#Monza 5 Tag Chips

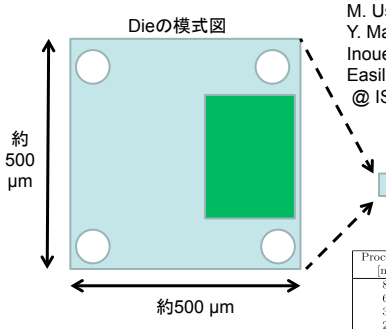
ロジック部は全体の3割程度

Process [nm]	Gate dencity [gate/mm^2]	500um 角の 30% 領域利用時 [gate]
800	1.2K	90
600	3K	225
350	18K	1.4K
250	35K	2.6K
180	80K	6K
130	180K	13.5K
90	400K	30K
65	800K	60K
40	1600K	120K

１～2Kgateの違いによって、実装の可否が変わるのは0.18 umくらいまで

MITSUBISHI Changes for the Better

RFIDにおける実装制約



M. Usami, H. Tanabe, A. Sato, I. Sakama, Y. Maki, T. Iwamatsu,T.Ipposhi and Y. Inoue:A 0.05 × 0.05 mm² RFID Chip with Easily Scaled-Down ID-Memory. @ ISSCC 2007

μ-chipくらいのRFIDであれば･･･

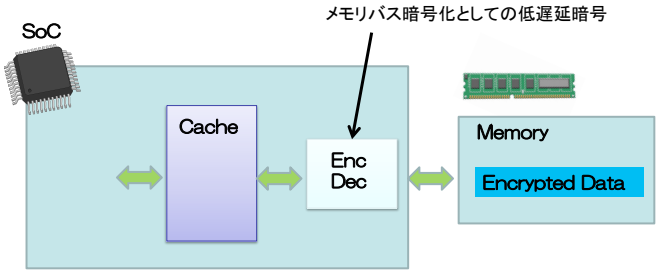
Process [nm]	Gate dencity [gate/mm²]	500um 角の 30% 領域利用時 [gate]	50um 角領域 利用時 [gate]
800	1.2K	90	3
600	3K	225	7.5
350	18K	1.4K	45
250	35K	2.6K	76
180	80K	6K	200
130	180K	13.5K	450
90	400K	30K	1K
65	800K	60K	2K
40	1600K	120K	4K

40nmでも1～2Kgateの差によって、実装の可否が変わる可能性あり

MITSUBISHI Changes for the Better

XOM, AEGIS

- 耐タンパプロセッサ
- 主記憶をOSや他のプロセス、あるいはプロービング攻撃などから秘匿することを目的として暗号化
- 読み出し速度がクリティカル



MITSUBISHI Changes for the Better

リアルタイム性能

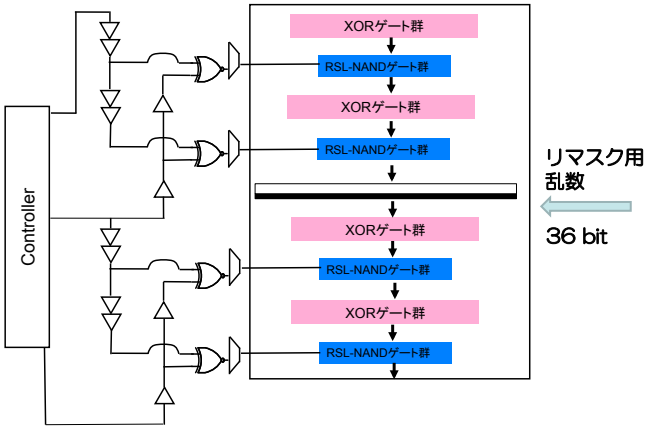
App.	Time region
Man-machine interface	数秒
Motor control	数 ms～数十 ms
I/O device control	数 μs
フラッシュ, EEPROM 読み出し	数 10～100ns
低電力 SRAM	数 10ns
高速 SRAM	～10ns

MITSUBISHI
Changes for the Better

＋　サイドチャネル対策

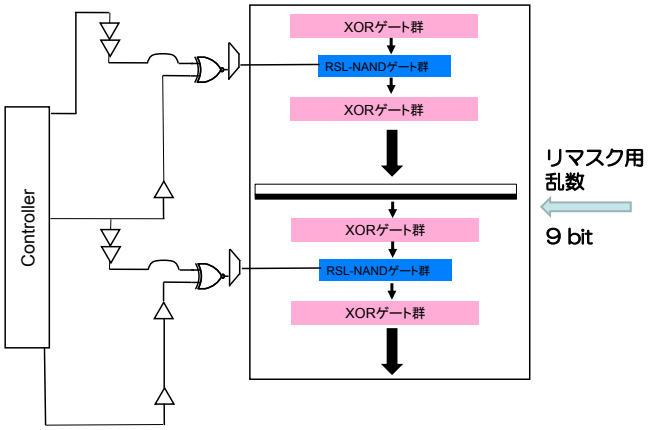
MITSUBISHI
Changes for the Better

8bit S-boxでのRSL



MITSUBISHI
Changes for the Better

4bit S-boxでのRSL



MITSUBISHI Changes for the Better

考察

■「軽量暗号」たる特徴は
- ✓ブロック長が64bit
- ✓鍵スケジュールが軽い（ラウンド定数のみ、レジスタ不要）
- ✓4bit S-box

これらがAESより1～2Kgate小さくなる主要因
(逆にいえば、これでほぼ特徴付けられる)

■ 改良は

暗号化のみ(PRESENT)
→復号もほぼ同じサイズでできる(Piccolo,TWINE)
→そもそも速い(低遅延 PRINCE)
→(認証暗号（FIDES）) という流れ？

MITSUBISHI Changes for the Better

まとめ

■ハードウェア実装からの視点としては軽量暗号は、
- ・マチュアなプロセスでの回路規模
- ・(リアルタイム)メモリ暗号化
- ・μ秒クラスのリアルタイム通信

などのアプリにおいて、AES に対してアドバンテージがある。

■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。小さく、速く（低遅延)、サイドチャネル対策しやすい、のが良い軽量暗号、という考え方は？

■ファームウェア実装を考慮すれば、また違った視点
軽量暗号のアドバンテージが考えられる。

MITSUBISHI Changes for the Better

以下付録

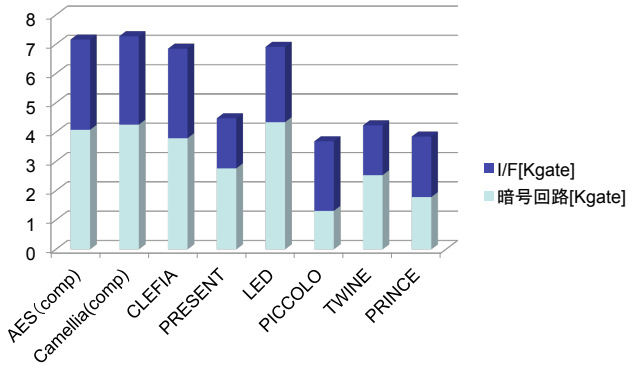
MITSUBISHI
Changes for the Better

暗号化・復号

MITSUBISHI
Changes for the Better

Serial

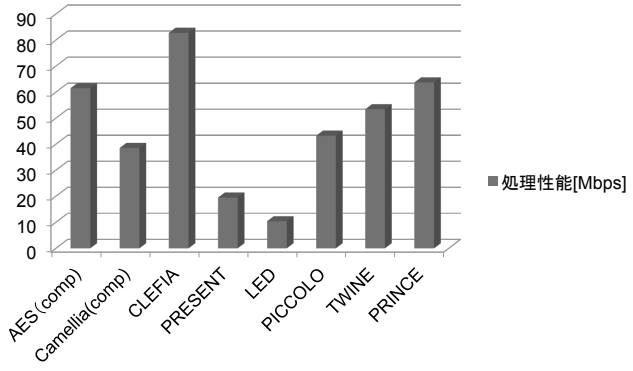
ゲートサイズ



MITSUBISHI
Changes for the Better

Serial

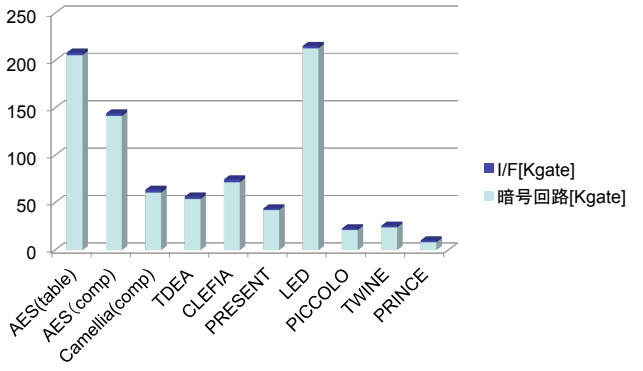
スループット



MITSUBISHI Changes for the Better

Unrolled

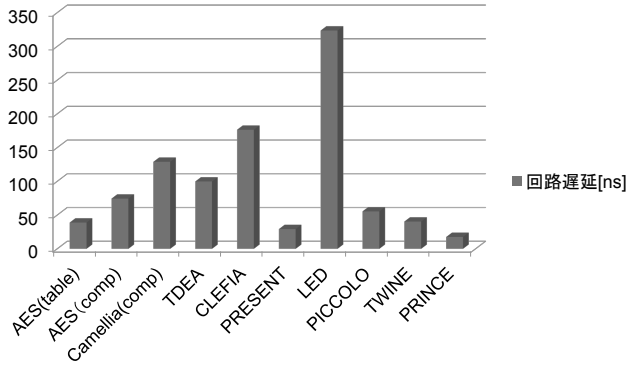
ゲートサイズ



MITSUBISHI Changes for the Better

Unrolled

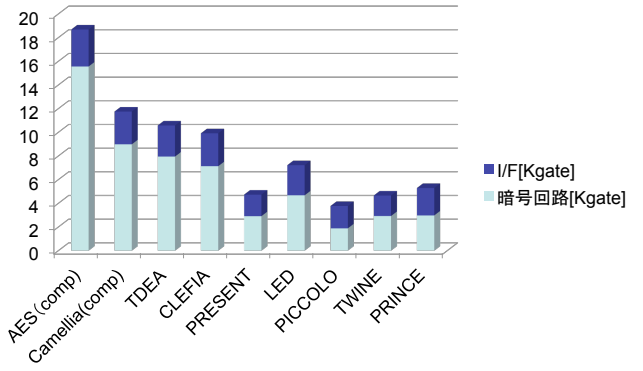
回路遅延



MITSUBISHI Changes for the Better

Round

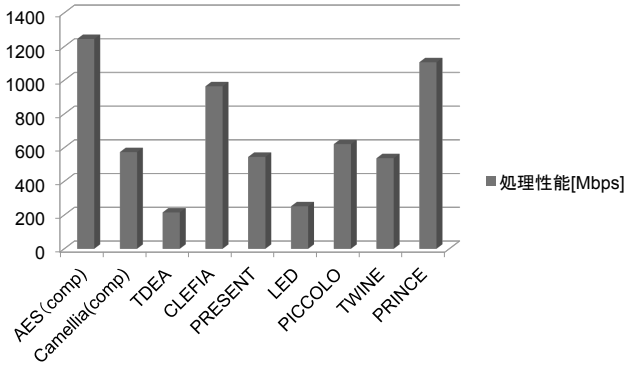
ゲートサイズ



MITSUBISHI Changes for the Better

Round

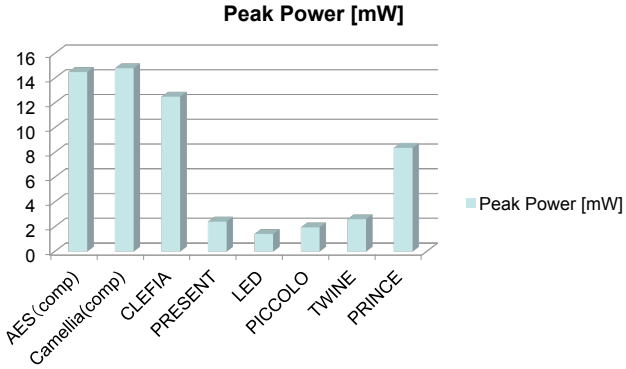
スループット



MITSUBISHI Changes for the Better

Serial

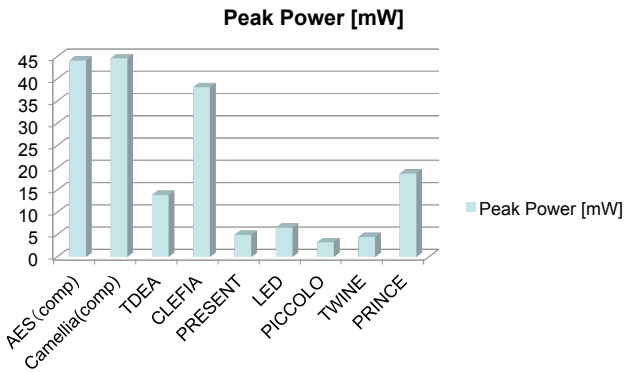
ピーク電流



MITSUBISHI Changes for the Better

Round

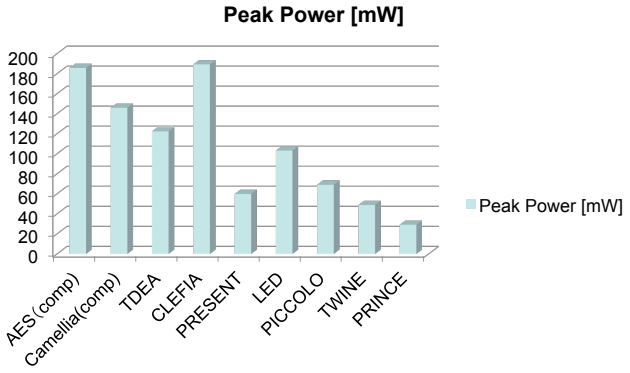
ピーク電流



MITSUBISHI Changes for the Better

Unrolled

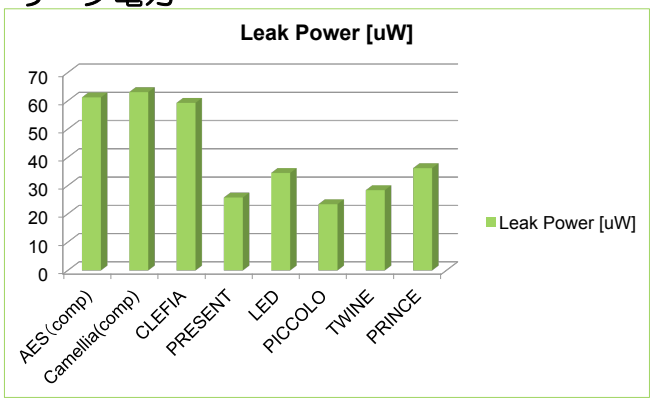
ピーク電流



MITSUBISHI Changes for the Better

Serial

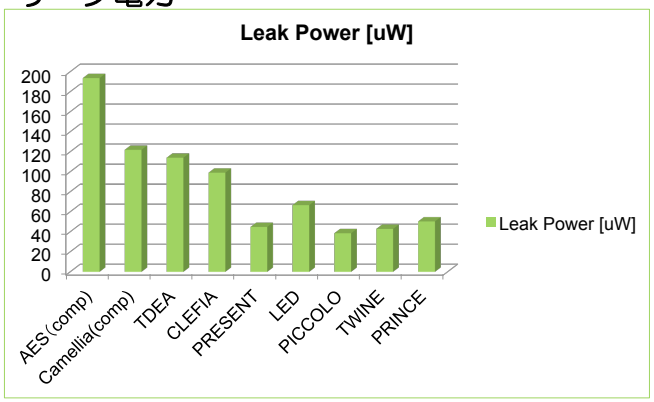
リーク電力



MITSUBISHI Changes for the Better

Round

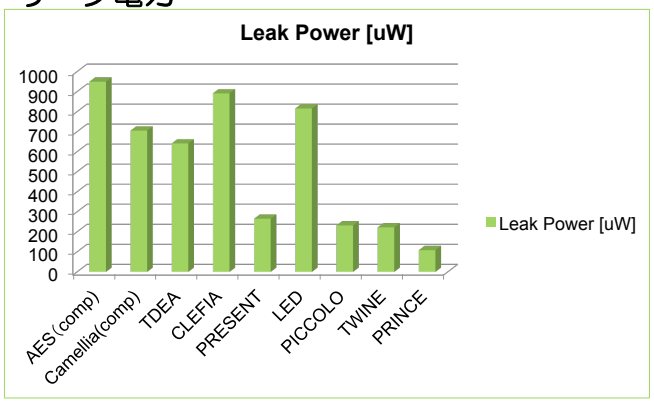
リーク電力



MITSUBISHI Changes for the Better

Unrolled

リーク電力



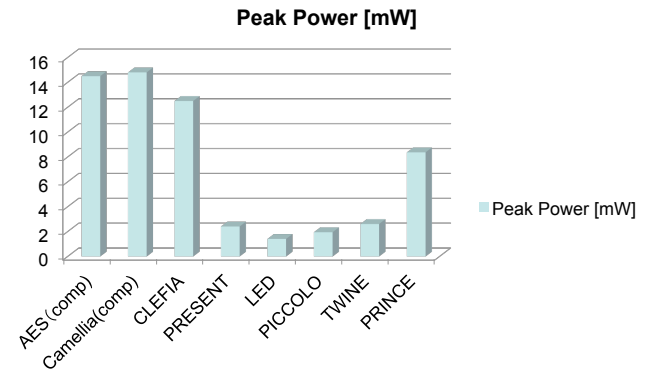
MITSUBISHI Changes for the Better

暗号化のみ(残りのデータ)

MITSUBISHI Changes for the Better

Serial

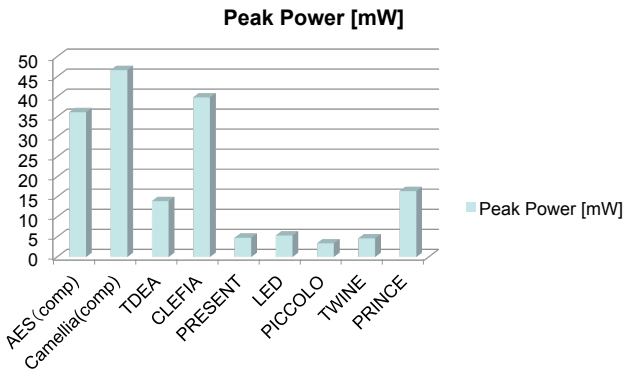
ピーク電流



MITSUBISHI Changes for the Better

Round

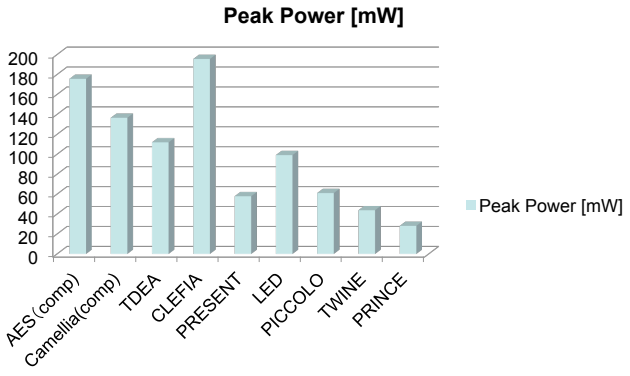
ピーク電流



MITSUBISHI Changes for the Better

Unrolled

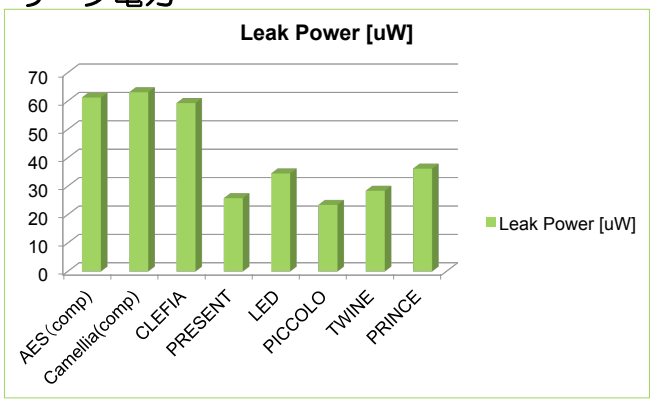
ピーク電流



MITSUBISHI Changes for the Better

Serial

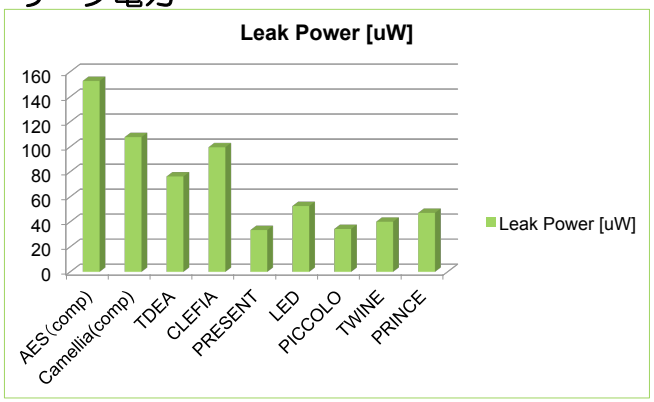
リーク電力



MITSUBISHI Changes for the Better

Round

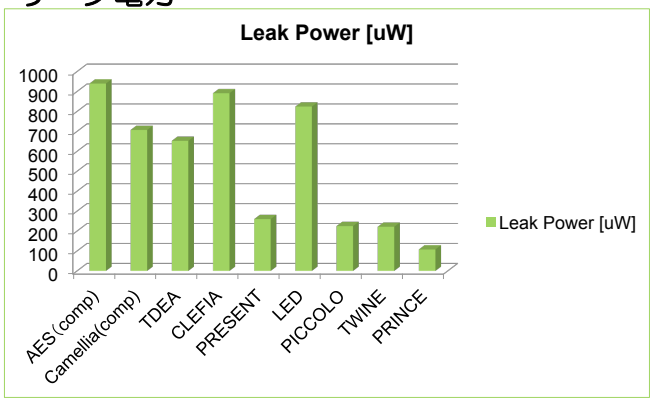
リーク電力



MITSUBISHI Changes for the Better

Unrolled

リーク電力



124

A.2.2　ソフトウェア性能評価

2013 年度 第 3 回軽量暗号 WG (2014 年 2 月 20 日) での三菱電機 松井 充氏による発表資料を示す。

資料2－2

軽量暗号のソフトウエア性能評価

(CRYPTREC軽量暗号WG資料)

2014年2月20日
三菱電機情報技術総合研究所　松井充

1

評価の目的

- Lightweight と呼ばれるブロック暗号がマイコン上のソフトウエアでどの程度 Lightweight であるかを調べる
  - Lightweight はハードウエアで語られることが多い
- マイコン上で小型を目指した暗号実装評価結果は数少ない
  - ソフトウエアでの暗号評価はほとんどの場合高速化が目標
  - しかも評価方法のコンセンサスがない
- 評価方法を提案
  - 実用的な観点からのインターフェースと評価方法を定義
  - ROM, RAM サイズを指定して、その範囲内で実装し速度を計測
  - 速度は無視してROMサイズがどこまで小さくなるかもみる

2

どの程度小さければLightweightか

- Renesas社マイコンRL78の場合
  - 汎用品（G1xシリーズ）： ROM 1KB, RAM 128B から
  - 車載品（F1xシリーズ）： ROM 8KB, RAM 512B から
- Atmel社マイコンAVRの場合
  - ATtiny: ROM 0.5KB, RAM 32B から ROM 16KB, RAM 1KB まで
  - ATtiny24/44/84 Automotive: ROM 2/4/8KB, RAM 128/256/512B
- 暗号機能はアプリケーションの一部
  - 暗号アルゴリズムが占有できるメモリ量は、通常全体のごく一部
  - 小さければ小さいほど暗号を使える品種が増える
- Lightweight というからには…
  - ROM 512B, RAM 64B 程度はめざしたいところ
  - この範囲の ROM, RAM サイズが議論されることは少ない

3

既存の評価事例 AES-128

独自インターフェース。C言語から呼び出し可能にするためは()内に示す追加メモリが必要

Algorithm	Processor	ROM	RAM static	RAM stack	Enc Speed	Dec Speed
AES (ED)	ATtiny	1659(+72)	33	0(+24)	4557n	7015n

http://perso.uclouvain.be/fstandae/lightweight_ciphers/ から作成

C言語から呼び出し可能。但し()内に示す平文・鍵領域やスタックがカウントされていない

Algorithm	Processor	ROM	RAM static	RAM stack	Enc Speed	Dec Speed
AES (ED)	ATmega	2070	176(+32)	0(+22)	2039+2555n	2039+6764n
AES (ED)	ATmega	2580	176(+32)	0(+22)	2039+2555n	2039+3193n

http://www.das-labor.org/wiki/AVR-Crypto-Lib/en から作成

C言語から呼び出し可能。RAMサイズには平文、鍵、スタックすべてを含む

Algorithm	Processor	ROM	RAM	Enc Speed	Dec Speed
AES (E)	RL78	486	78	7288n	-
AES (E)	RL78	1021	60	3855n	-
AES (ED)	RL78	970	84	7743n	1821+10862n
AES (ED)	RL78	1989	64	3917n	893+5911n

(E) Enc only
(ED) Enc+Dec
n: blocks
Size: bytes
Speed: cycles

Matsui, Murakami: FSE2013

4

既存の評価事例 Present-80

独自インターフェース。C言語から呼び出し可能にするためは()内に示す追加メモリが必要

Algorithm	Processor	ROM	RAM static	RAM stack	Enc Speed	Dec Speed
Present (ED)	ATtiny	1000(+72)	18	0(+24)	11342n	13599n

http://perso.uclouvain.be/fstandae/lightweight_ciphers/ から作成

上と同様の独自インターフェース。さらにカウントされていないスタックを加算

Algorithm	Processor	ROM	RAM static	RAM stack	Enc Speed	Dec Speed
Present (E)	ATtiny	204(+72)	18	0(+28)	190048n	-
Present (ED)	ATtiny	272(+72)	18	0(+30)	190048n	253384n
Present (E)	ATtiny	210(+72)	18	0(+28)	55784n	-
Present (ED)	ATtiny	278(+72)	18	0(+30)	55784n	77304n

http://rfidsec2013.iaik.tugraz.at/res/slides/Session4_Talk2_Verstegen.pdf から作成

C言語から呼び出し可能。RAMサイズには平文、鍵、スタックすべてを含む

Algorithm	Processor	ROM	RAM	Enc Speed	Dec Speed
Present (E)	RL78	210	54	144879n	-
Present (E)	RL78	897	42	9007n	-
Present (ED)	RL78	512	62	61634n	44068+60834n
Present (ED)	RL78	1855	48	9007n	1903+8920n

(E) Enc only
(ED) Enc+Dec
n: blocks
Size: bytes
Speed: cycles

Matsui, Murakami: FSE2013

5

評価方法

- インターフェースの統一が必要
  - 小型実装では、インターフェースの違いによるサイズ差は無視できない
  - 暗号を利用することによるすべてのオーバーヘッドを数値化すべき
- 実用性の観点から
  - 評価対象は高級言語から呼び出し可能なサブルーチンとして記述する
  - RAM サイズには平文や鍵の領域、スタックをすべて含める
  - アプリケーションプログラムの範囲をこえる特殊なことはしない
- 評価対象のソフトウエア仕様
  - 1ブロックを暗号化／復号する機能をもつ
  - 平文領域と暗号文領域は共通化する
  - 鍵領域は終了時に元の状態を復帰（一時的に変更してもよい）

6

評価対象と評価項目

- 評価対象

	AES	Camellia	Clefia	TDES	LED	Prince	Present	Piccolo	Twine
ブロックサイズ	128	128	128	64	64	64	64	64	64
鍵サイズ	128	128	128	168	128	128	80	80	80

- 評価環境
  - ルネサスマイコンRL78　CISCプロセッサで小型化に向いている
- 評価項目
  1. ROM 512B/1024B, RAM 64B/128B の4通り制約条件のもとで、暗号化のみの実装と、暗号化＋復号の実装をおこなう
  2. 暗号化のみで、ROM サイズを最小化する実装をおこなう
  3. ROM 2KB程度で、暗号化がどこまで高速になるかを調べる

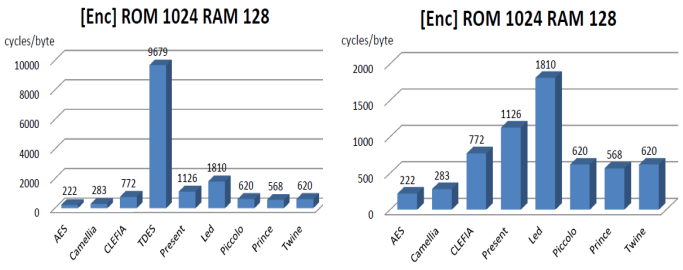
7

RL78 v.s. ATtiny

		RL78	ATtiny
ハードウエアレジスタ	レジスタ長	8, 16	8
	レジスタ数	8	32
アドレッシングモード	Read-Modify	Yes	No
	Post-Increment	No	Yes
命令長（bytes）	xor reg, [mem]	1-3	4
	call	3	2
	push / pop	1	2
実行時間（cycles）	read from RAM/ROM	1/4	2/3
	xor reg, [mem]	1	2
	taken/not-taken jump	4/2	2/1
	call + return	9	7

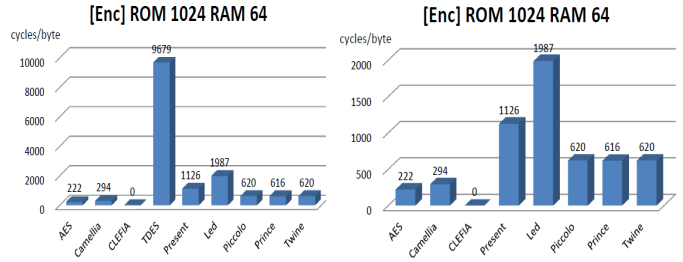
8

評価結果1: (E) ROM 1024B, RAM 128B



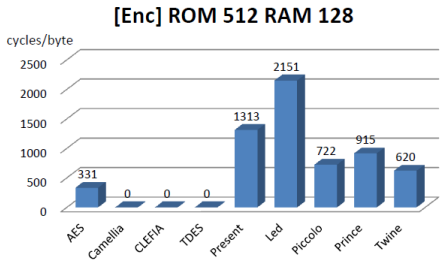
9

評価結果2: (E) ROM 1024B, RAM 64B



10

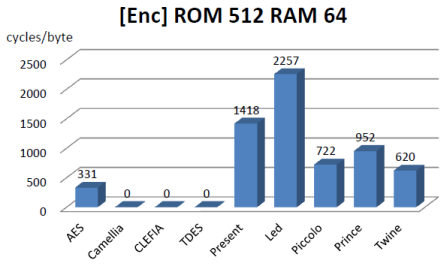
評価結果3: (E) ROM 512B, RAM 128B



11

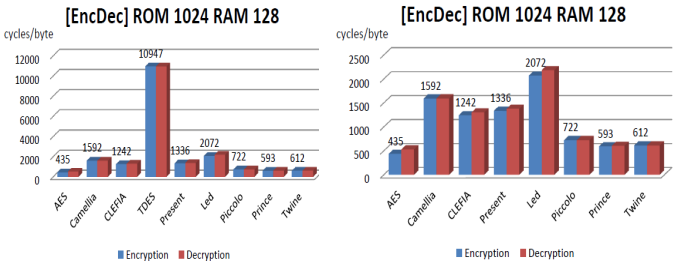
128

評価結果4：(E) ROM 512B, RAM 64B



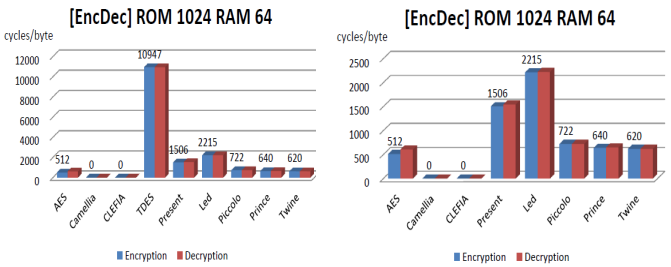
12

評価結果5：(ED) ROM 1024B, RAM 128B



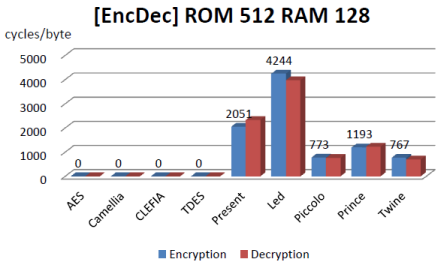
13

評価結果6：(ED) ROM 1024B, RAM 64B



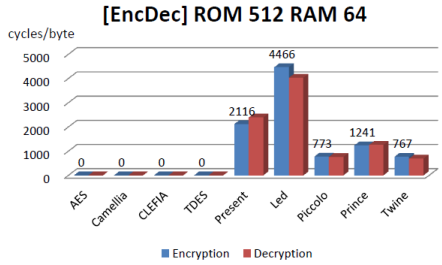
14

評価結果7: (ED) ROM 512B, RAM 128B

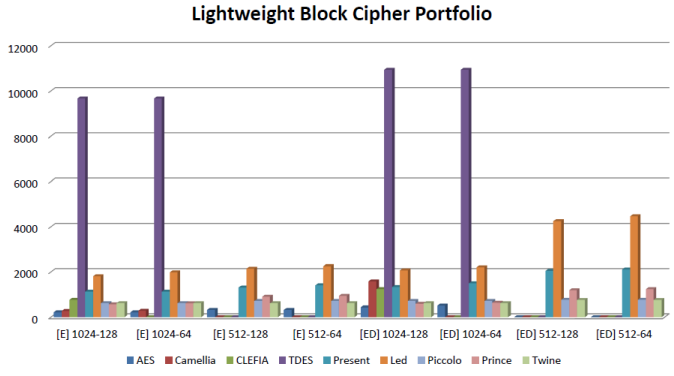


15

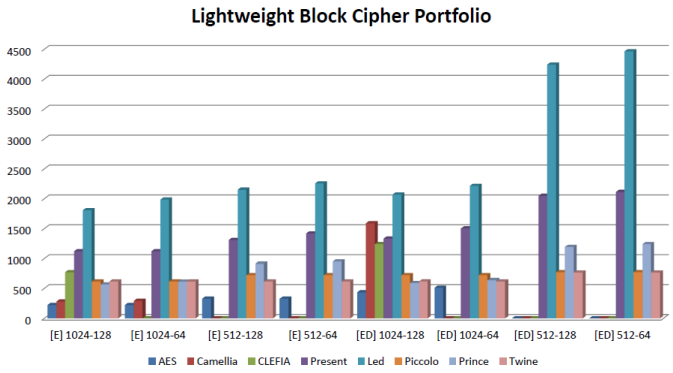
評価結果8: (ED) ROM 512B, RAM 64B



16

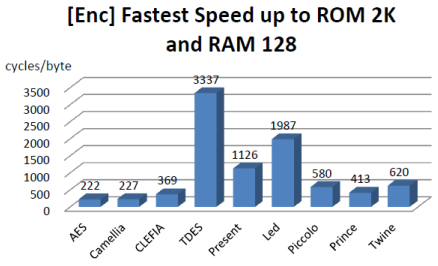


17



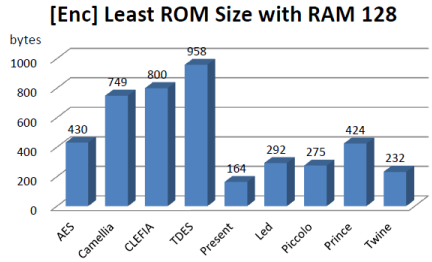
18

評価結果9：(E) Fastest Speed

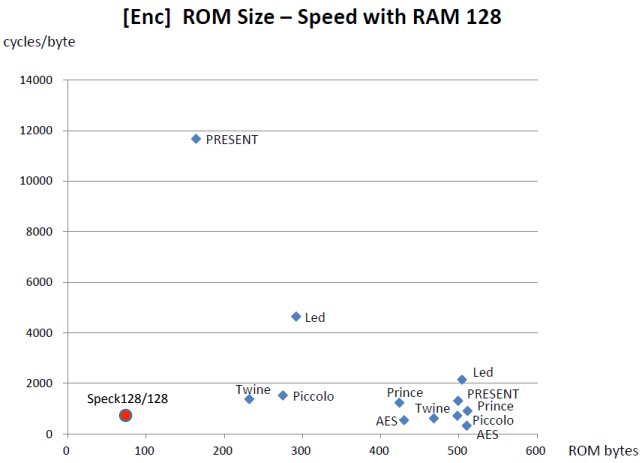


19

評価結果10：(E) Smallest Size



20



21

Lightweight v.s. AES

- アルゴリズム単体で考えるなら、暗号化のみならROM 512B、暗号復号両方こみならROM 1KBあれば、AESで十分
- 実際にはこれに加えモードを含む入出力データ処理が必要、またプロセッサのメモリ全てを暗号が使えるわけではない
- ROM 4KB-8KB, RAM 256B-512Bが、AESをソフトウエアで使えるプロセッサの下限と思われる。
- AESより価値あるソフトウエアLightweightブロック暗号とは…
  - メモリがたくさんあればAESなみの速度がでる
  - 暗号・復号こみでROM 200B以下、RAM 32B以下でそれなりの速度
  - 現時点ではNSAのSimon, Speckが有力候補（安全性は不明）

22

Software Lightweight Design

- 小型化実装は高速化実装と感覚がずいぶん違う
  - 無駄なコードを付け加えることが最終的に小型化に貢献することがある
  - 10バイト減らすと10倍遅くなることがある
- ほんの少しのことがコードサイズに大きく影響する
  - データの単なる移動や定数もオーバーヘッド
  - 数少ない単純な繰り返し構造だけでアルゴリズムを作る必要がある
- 鍵スケジュールがsoftware lightweightでない方式が多い
  - On-the-fly key schedulingを前提に設計すべき
- 回転シフト命令の効率はプロセッサに大きく依存
  - シフト命令もできるだけ避けよ
- Endian Neutralなアルゴリズムが望ましい
  - 今ではほとんどのプロセッサがlittle endianメモリアクセスなのに、多くのアルゴリズムがbig endianを前提に設計されている

23

その他私見

- 今回評価対象としたのはすべてS-box型ブロック暗号
- Lightweight ブロック暗号のトレンドは4ビットS-box
  - Present, LED, Prince, Piccolo, Twine
  - S-box型が安全性の評価がしやすい
- これは Lightweight として正しい方向か？
  - Simon, Speck が問うているもの
  - このタイプのブロック暗号TEAは昔からあった
- 暗号理論的にどこまで完全な安全性をめざすべきか？
  - 現実には side-channel attacks の方が脅威
  - そもそも64ビットブロック暗号がリバイバルしている
  - 安全性の条件を再定義する方向もあるのではないか

24

発行日　2015年 6月30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
国立研究開発法人 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）
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