CRYPTREC Report 2016

平成 29 年 3 月

国立研究開発法人情報通信研究機構
独立行政法人情報処理推進機構

CRYPTREC-RP-0002-2016

「暗号技術評価委員会報告」

目次

はじめに…… 1
本報告書の利用にあたって…… 2
委員会構成…… 3
委員名簿…… 4

第1章　活動の目的 …… 7
1.1　電子政府システムの安全性確保…… 7
1.2　暗号技術評価委員会…… 8
1.3　CRYPTREC 暗号リスト …… 8
1.4　活動の方針…… 9

第2章　委員会の活動 …… 11
2.1　監視活動報告…… 11
2.1.1　共通鍵暗号に関する安全性評価について…… 11
2.1.2　公開鍵暗号に関する安全性評価について…… 11
2.1.3　ハッシュ関数に関する安全性評価について …… 12
2.1.4　KCipher-2 の仕様書の誤記について…… 12
2.1.5　仕様書の参照先の変更について…… 13
2.1.6　共通鍵暗号の安全性調査と MISTY1 について …… 15
2.2　注意喚起レポートの発行…… 20
2.2.1　暗号アルゴリズムの脆弱性に関する情報発信 …… 20
2.2.2　SHA-1 の安全性低下について …… 21
2.3　推奨候補暗号リストへの新規暗号の追加 …… 21
2.3.1　SHAKE128…… 21
2.4　ChaCha20-Poly1305 の CRYPTREC 暗号リストへの追加を視野に
入れた評価について …… 22
2.5　Post Quantum Cryptography に関する動向について…… 24
2.6　文書番号体系について…… 24
2.7　学会等参加状況…… 25
2.7.1　共通鍵暗号の解読技術…… 26
2.7.2　公開鍵暗号の解読技術…… 26
2.7.3　ハッシュ関数の解読技術…… 27
2.8　委員会開催記録…… 29
2.9　暗号技術調査ワーキンググループ開催記録 …… 29

第 3 章　暗号技術調査ワーキンググループの活動 ····· 31
3.1　暗号解析評価ワーキンググループ ····· 31
3.1.1　活動目的 ····· 31
3.1.2　委員構成 ····· 31
3.1.3　活動概要 ····· 31
3.1.4　成果概要 ····· 32
付録 A.1　楕円曲線上の離散対数問題(ECDLP)の困難性
に関する調査····· 39
付録 A.2　多重線形写像(multi-linear map)及び難読化
(Obfuscation)の最新動向に関する調査····· 43
付録 A.3　予測図の更新(素因数分解問題及び楕円曲線上
の離散対数問題の困難性)····· 45

3.2　軽量暗号ワーキンググループ····· 47
3.2.1　活動目的 ····· 47
3.2.2　委員構成 ····· 47
3.2.3　活動概要 ····· 47
3.2.4　成果概要 ····· 48

付録 ····· 51
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) ····· 51
付録 2　CRYPTREC 暗号リスト掲載の暗号技術の問合せ先一覧 ····· 57
付録 3　楕円曲線上の離散対数問題に関する指数計算法 ····· 71
付録 4　多重線形写像に関する最新動向の調査 ····· 101
付録 5　学会等での主要攻撃論文発表等一覧 ····· 155

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運営されている暗号技術評価委員会の 2016 年度活動報告である。

暗号技術評価委員会は、国立研究開発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いる。暗号技術評価委員会の 2016 年度の活動として、

1)暗号技術の安全性及び実装に係る監視及び評価

2)暗号技術に関する注意喚起レポートの公表

3)新しい暗号技術に係る調査および評価

を実施することを暗号技術検討会より承認を得て、活動を実施した。

主な活動として、1)については、ハッシュ関数 SHA-3 ファミリーの 1 つである SHAKE128 について、適切なパラメータを選択すれば、CRYPTREC 暗号リストへの追加に十分な安全性と実装性能を有していることを確認し、推奨候補暗号リストへの追加が適切であると暗号技術検討会に報告した。また、多くのユーザを持ついくつかのブラウザで利用が広まりつつある認証暗号 ChaCha20-Poly1305 について、秘匿を実現する ChaCha20 の安全性評価を行った。次年度さらに認証を実現する Poly1305 の安全性評価および認証暗号としての ChaCha20-Poly1305 の評価を継続する予定である。また、共通鍵暗号の安全性について調査を行い、MISTY1 の今後の利用について提示すべき推奨方針案について検討を行った。2)については、「ハッシュ関数 SHA-1 の衝突困難に初めて成功」との発表を受け、SHA-1 の安全性低下が進んでいることから、SHA-256 等のより安全なハッシュ関数への移行を推奨する注意喚起レポートを発行した。3)については、従来から活動してきた 2 つのワーキンググループ(以下、WG)を継続して設置し、暗号解析評価 WG では、楕円曲線上の離散対数問題、多重線形写像およびその関連技術に関して、安全性調査・評価を継続して行い、技術報告書としてまとめた。併せて、素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量の評価に基づく予測図の更新を行った。軽量暗号 WG では、IoT 等において軽量暗号の活用が期待されることから、方式を選択・利用する際の技術的判断に資すること、今後の利用促進を図ることを目的として軽量暗号技術に関するガイドラインを日本語版・英語版ともに完成させ公開した。

2015 年 9 月に閣議決定されたわが国の「サイバーセキュリティ戦略」においても、暗号技術はサイバーセキュリティのコア技術として国が維持すべき重要な技術と位置づけられ、暗号技術の担う役割の重要性が認識されている。

発足以来 16 年にわたる CRYPTREC の活動は、セキュアな ICT 社会の実現に貢献し、世界的にも通用する CRYPTREC ブランドの信頼の醸成につながっていると認識している。今後も社会の情勢を踏まえ、社会のニーズに対して、暗号技術の安全性という観点から必要とされる活動を展開していきたいと考えている。

暗号技術評価委員会の活動は暗号技術やその実装及び運用に携わる研究者及び技術者の献身的な協力により成り立っている。末筆ではあるが、本活動に様々な形でご協力頂いている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　太田 和夫

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の説明である。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、国立研究開発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。

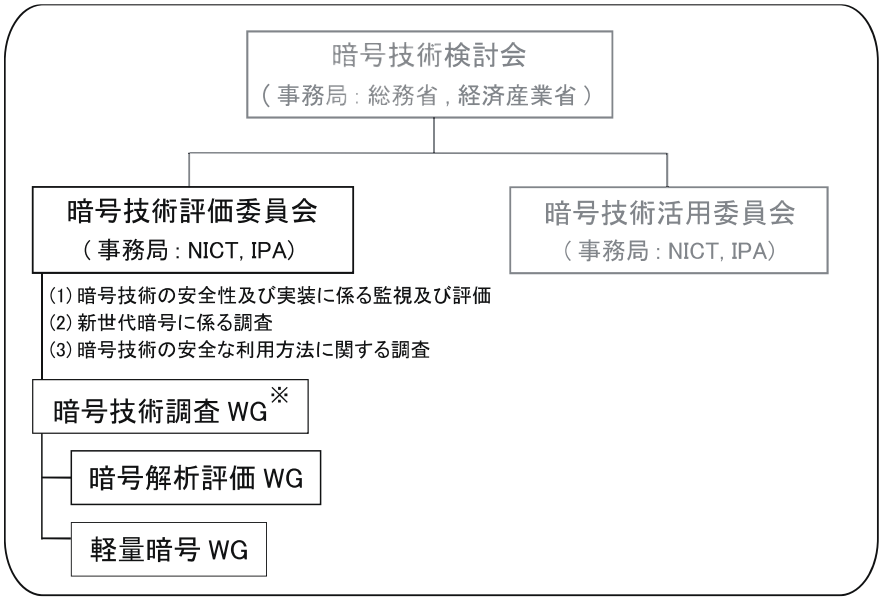
【問合せ先】　info @ cryptrec.go.jp

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、国立研究開発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。2016 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：

- 多重線形写像、難読化及び離散対数問題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	太田 和夫	電気通信大学 教授
委員	岩田 哲	名古屋大学 准教授
委員	上原 哲太郎	立命館大学 教授
委員	金子 敏信	東京理科大学 教授
委員	佐々木 良一	東京電機大学 教授
委員	高木 剛	九州大学 教授
委員	手塚 悟	慶應義塾大学 特任教授
委員	本間 尚文	東北大学 教授
委員	松本 勉	横浜国立大学 教授
委員	松本 泰	セコム株式会社 ディビジョンマネージャー
委員	盛合 志帆	国立研究開発法人情報通信研究機構 研究室長
委員	山村 明弘	秋田大学 教授
委員	渡邊 創	国立研究開発法人産業技術総合研究所 企画主幹

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	九州大学 教授
委員	青木 和麻呂	日本電信電話株式会社 グループリーダ
委員	太田 和夫	電気通信大学 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	東京大学 准教授
委員	下山 武司	株式会社富士通研究所 主管研究員
委員	安田 雅哉	九州大学 准教授

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	東北大学 教授
委員	青木 和麻呂	日本電信電話株式会社 グループリーダ
委員	岩田 哲	名古屋大学 准教授
委員	小川 一人	日本放送協会 上級研究員
委員	小熊 寿	株式会社トヨタ IT 開発センター シニアリサーチャー
委員	崎山 一男	電気通信大学 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

内田 稔	内閣官房内閣サイバーセキュリティセンター[2016 年 10 月から]
久保山 拓	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
眞弓 隆浩	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[2016 年 9 月まで]
中山 慎一	警察庁 情報通信局
赤谷 俊彦	総務省 行政管理局[2016 年 8 月まで]
廣田 亮	総務省 行政管理局
内海 隆明	総務省 自治行政局 住民制度課
筒井 邦弘	総務省 情報流通行政局[2016 年 6 月まで]
上東 孝旭	総務省 情報流通行政局[2016 年 7 月から]
丸橋 弘人	総務省 情報流通行政局
今野 孝紀	総務省 情報流通行政局
佐久間 明彦	外務省 大臣官房
加藤 誠司	経済産業省 産業技術環境局
希代 浩正	経済産業省 商務情報政策局[2016 年 6 月まで]
中野 辰実	経済産業省 商務情報政策局[2016 年 6 月まで]
中村 博美	経済産業省 商務情報政策局[2016 年 6 月まで]
森川 淳	経済産業省 商務情報政策局[2016 年 7 月から]
松本 裕悟	防衛省 整備計画局
多賀 文吾	警察大学校
滝澤 修	国立研究開発法人情報通信研究機構
花岡 悟一郎	国立研究開発法人産業技術総合研究所

事務局

国立研究開発法人情報通信研究機構 （宮崎哲弥、能見正、盛合志帆、大久保美也子、篠原直行、黒川貴司、金森祥子、野島良、吉田真紀、笠井祥、大川晋司）

独立行政法人情報処理推進機構（江口純一、時田俊雄、小暮淳、神田雅透、稲垣詔喬、兼城麻子）

第１章　活動の目的

1.1 電子政府システムの安全性確保

電子政府、電子自治体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 では、「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)」[1] 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。たとえば、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。これらの見解に基づき、情報セキュリティ政策会議において「政府機関の情報システムにおいて使用される暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」[2] が 2008 年度に決定されるに至った。また、CRYPTREC 暗号リスト策定中に実施した安全性評価において、128-bit key RC4 の脆弱性を利用した攻撃が現実的になる場合が指摘されたことから、128-bit key RC4 は SHA-1 とともに CRYPTREC 暗号リストの運用監視暗号リストに記載されることになった。現在、暗号技術評価委員会では、暗号技術に関する安全性について重要な指摘があった場合、CRYPTREC の Web サイト上に注意喚起レポートを掲載する活動を実施している。たとえば、最近では、2017 年 2 月には SHA-1 の衝突が初めて計算されたことから、「SHA-1 の安全性低下について」[3]を Web 掲載した。

暗号技術に対する解析・攻撃技術の高度化が日夜進展している状況にあることから、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 16 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] http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2016.pdf

[2] http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf (2008 年 4 月 22 日決定情報セキュリティ政策会議決定)

[3] http://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html

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[4]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)」[5](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。

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

[4] http://www.cryptrec.go.jp/list_2003.html
[5] http://www.cryptrec.go.jp/list.html

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

2009 年度には、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[6]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。
選定方法及びその結果については、CRYPTREC Report 2012(暗号技術評価委員会報告)に記載されている。

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、ペアリング暗号、耐量子計算機暗号技術等)
(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[7]掲載の暗号技術に対する考え方[8]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 つの段階からなる。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。

[6] http://www.cryptrec.go.jp/topics/cryptrec_201212_listpc.html
[7] 2003 年 2 月 20 日に策定されたものを指す。
[8] 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

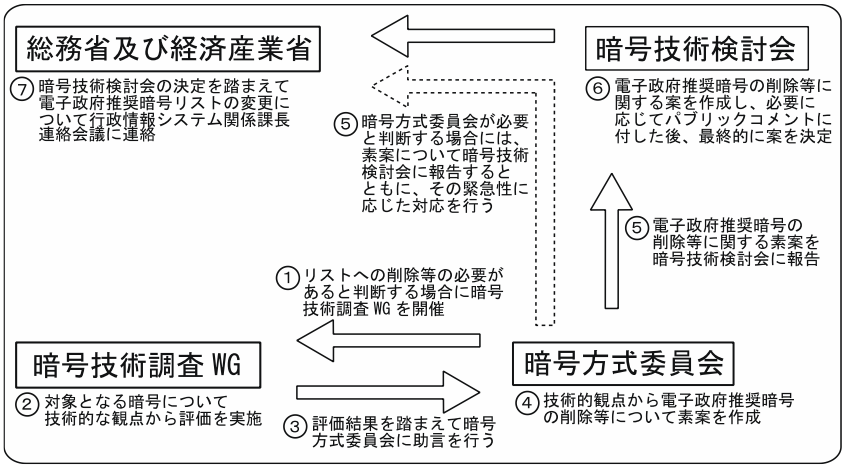


図1.1：電子政府推奨暗号の削除等の手順[9]

(1) 実運用環境において安全性に問題が認められた電子政府推奨暗号は原則としてリストから削除する。

(2) 電子政府推奨暗号の仕様変更は認めない。

(3) 電子政府推奨暗号の仕様変更に到らないパラメータの修正等の簡易な修正を行うことにより当該暗号の安全性が維持される場合には、修正情報を周知して当該暗号をリストに残す。

[9] 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 2016 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

CRYPTREC 暗号リスト掲載のブロック暗号について、Crypto 2016 において 64 ビットブロック暗号 MISTY1 に対する解析結果が発表された。これは藤堂が Crypto 2015 で発表した MISTY1 の Integral Analysis に Division Property を導入する攻撃法を改良したもので解読計算量は約 2^{70} にまで下がっているが、解読に必要なデータ量は 2^{64} であり、まだ現実的な脅威には至っていないと考えられる。本結果は、国際暗号学会 （International Association for Cryptologic Research (IACR)) のアーカイブサイト IACR ePrint Archive にて事前に公開されており、CRYPTREC はホームページにて解読に必要なデータ量・計算量の表および「解読に必要なデータ量が膨大であることから現実的な脅威ではないと考えられる」という見解を公表済である。ただし、Division Property を利用した攻撃研究は進展中であり、MISTY1 以外の他のブロック暗号への適用など、今後の動向が注目される。

CRYPTREC 暗号リスト掲載のストリーム暗号について、安全性については特に大きな変更はなかった。なお、KCipher-2 について CRYPTREC ホームページにて公開している仕様書に軽微な誤記が見つかったが、安全性評価等に影響するものではないことを確認し、仕様書の修正のみ行われた。

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)の解読法に引き続き進展があり、また、楕円曲線 Diffie-Hellman(ECDH: Elliptic Curve Diffie-Hellman)問題に関しては、新たな知見が得られた。

DLP に関しては、Eurocrypt 2016 / Asiacrypt 2016 における Sarkar、Singh の攻撃、Crypto 2016 における Kim、Barbulescu の攻撃、PKC 2017 における Kim、Jeong の攻撃において、計算量削減・高速化の進展が見られたが、電子政府推奨暗号のパラメータは攻撃の適用条件に当てはまらない。

ECDH に関しては、PKC 2017 において Shani が、素体上で定義された楕円曲線の ECDH 鍵交換プロトコルのビットセキュリティに関する結果を初めて示した。それによると、Diffie-Hellman 鍵の x 座標の最上位ビットの約 5/6 を計算することは、鍵全体を計算する

ことと同じくらい困難である。また最下位ビットの約 5/6 についても同様の結果が成り立つ。更に拡大体上の楕円曲線の場合には、Diffie-Hellman 鍵の x 座標または y 座標の 1 成分を計算することは、鍵全体を計算することと同じくらい困難である。

2.1.3. ハッシュ関数に関する安全性評価について

CRYPTREC 暗号リスト掲載のハッシュ関数 SHA-1 に対し攻撃の進展が見られた。Eurocrypt2016 において、Stevens, Karpman, Peyrin らは SHA-1 に対し、Free-Start 衝突攻撃の条件ではあるものの、SHA-1 のフルラウンド(全 80 ステップ中 80 ステップ)に対し、初めて衝突発見に成功したと発表した。本結果は、国際暗号学会 (International Association for Cryptologic Research (IACR)) のアーカイブサイト IACR ePrint Archive にて事前に公開されており、CRYPTREC はホームページにて、従前通り SHA-1 に関する移行対策を実施して頂きたい旨の見解を公表済である。

また、2017 年 2 月 23 日に、CWI Amsterdam と Google Research の共同研究チームが、ハッシュ関数 SHA-1 の衝突発見に初めて成功したと Web ページ(https://shattered.io/)上で発表された。この発表では、全数探索の計算量(2^{80})よりも 10 万倍速い $2^{63.1}$ 回の SHA-1 の計算量で衝突を発見したと報告されている。本発表の内容はまだ著名な国際学会等で発表はされてはいないが、実際にハッシュ関数が同じ異なる PDF ファイルの例も公開された。CRYPTREC では平成 29 年 3 月 1 日付でホームページにて、SHA-1 の安全性低下が進んでいることから、SHA-256 等の「電子政府推奨暗号リスト」または「推奨候補暗号リスト」に掲載されている、安全性が確認されたハッシュ関数への移行を推奨する旨の見解を公開済である。

CRYPTREC 暗号リスト掲載の SHA-1 以外のその他のハッシュ関数の安全性については特に大きな変更はなかった。

2.1.4. KCipher-2 の仕様書の誤記について

2016 月 12 月に IPA の JCMVP から、KCipher-2 の仕様書(以下、旧仕様書という)において、シフトレジスタの定義式と図の間に不整合があるという報告が CRYPTREC 事務局宛てにあった。2017 年 1 月に CRYPTREC 事務局から応募者の KDDI に問い合わせたところ、その指摘通り、シフトレジスタの定義式に誤植があり、定義式を図と整合するものに修正した仕様書(以下、新仕様書という)に差し替えをしたいとの回答があった。

① 暗号技術評価委員会における対応

旧仕様書におけるシフトレジスタの定義式を修正することは、編集上は軽微と判断できるが、誤植を修正したことで、旧仕様書に対して行った安全性評価の結果に影響が及ばないか懸念される。定義式に基づいた評価を行ったか、図に基づいた評価を行ったかの確認が必要であった。

② 審議結果

暗号技術評価委員会では、旧仕様書に基づく安全性評価を依頼した評価者らにどちらに基づいて評価を行ったのかを確認し、回答がともに図に基づいた評価であったので、旧仕様書から新仕様書への差し替えを認める判断を行った。また、2017 年 3 月に開催された第１回暗号技術検討会においても旧仕様書から新仕様書への差し替えが了承された。

なお、新仕様書については、CRYPTREC 暗号の仕様書の Web ページ[1]を参照のこと。

2.1.5. 仕様書の参照先の変更について

表 2.1 の通り、SHA-2、CMAC および DH/ECDH に関する NIST が管理している仕様書に変更があったため、新旧仕様書の差分を調査した。

調査の結果、表 2.2 の通り、変更が軽微であったので、新しい仕様書へ参照先の変更を認めることとなった。

表 2.1：NIST の新旧仕様書

暗号技術名	旧仕様書	新仕様書
SHA-2	FIPS PUB 180-4 March 2012 http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf	FIPS PUB 180-4 August 2015 http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
CMAC	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication (May 2005) http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38b.pdf	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication (Updated Oct. 2016) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf
DH/ECDH	NIST SP 800-56A Revision 1 (March 2007) http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf	NIST SP 800-56A Revision 2 (May 2013) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

[1] http://www.cryptrec.go.jp/method.html

表 2.2：判定結果とその理由

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

＜調査結果の概要＞

ドメインパラメータ及び公開鍵に関する妥当性の確認や秘密鍵が Ephemeral かまたは Static であるという条件に関する仕様を除く、(DH 及び ECDH の)ドメインパラメータの生成に関する仕様及び(DH 及び ECDH の)Diffie-Hellman プリミティブに関する仕様の 2 箇所について、変更が軽微かどうかの確認を行った。

①有限体上の群に関するドメインパラメータ生成

p のサイズが 1024 ビットか 2048 ビットに限定されたこと、及び、p および q の左端のビットが 1 であることの 2 つの条件が追加された。また、q の選択に関する記述が、[1,q-1]の間の整数の範囲からランダムに選択するという記述に修正された。

これら以外は､FIPS 186 に基づいてドメインパラメータが生成されることに変更はない。

③ 有限体上の群に関する Diffie-Hellman プリミティブ

計算途中で生じた値すべてを破壊する(ゼロ化する)ことが明示されたこと以外に変更はない。

③楕円曲線に関するドメインパラメータ生成

d の選択に関する記述が、[1,n-1]の間の整数の範囲からランダムに選択するという記述に修正された。

これ以外は、ANS X9.62 に基づいてドメインパラメータを生成するか、または、FIPS 186 で指定された推奨楕円曲線を選択することに変更はない。

④楕円曲線に関する Diffie-Hellman プリミティブ

計算途中で生じた値すべてを破壊する(ゼロ化する)ことが明示されたこと以外に変更はない。

2.1.6. 共通鍵暗号の安全性調査と MISTY1 について

2015 年度に共通鍵暗号 MISTY1 のフルラウンドへの攻撃が発表されたことを受け、現在、CRYPTREC では共通鍵暗号の将来の安全性の判断基準について指針を有していないこと、また、共通鍵暗号の専門家が学術論文等で記載している解読計算量の表現は非専門家にとっては分かりづらいという指摘があったことなどから、今年度、暗号技術評価委員会にて、外部の共通鍵暗号の専門家グループに下記の調査を依頼した。

＜調査内容＞

① 現在使われている代表的な共通鍵暗号に対する攻撃法の発展（暗号解読に必要な計算量・データ量・メモリ量等の低下）の調査

② 解読手法の進展や計算機能力の向上を勘案した共通鍵暗号の今後の危殆化に関する考察

＜調査結果＞

① AES, Camellia, MISTY1 に対する各攻撃法の発展

図2.1～図2.3 にAES, Camellia, MISTY1のこれまでの安全性評価結果を攻撃技術進化マップとして示す。横軸は攻撃の発表年、縦軸はフルラウンドに対する攻撃成功段数を示し、攻撃成功段数/フル段数の割合で表している。100% はフル段数の攻撃を意味する。また、攻撃進化を鍵長ごとに示しており、赤, 青, 緑がそれぞれ128, 192, 256 ビット鍵を示す。また、攻撃ごとに色分けをしており、ピンク色がIntegral 攻撃、青色が不能差分攻撃、黄色が中間一致攻撃、白色が無相関線形攻撃、灰色が切詰差分攻撃である。

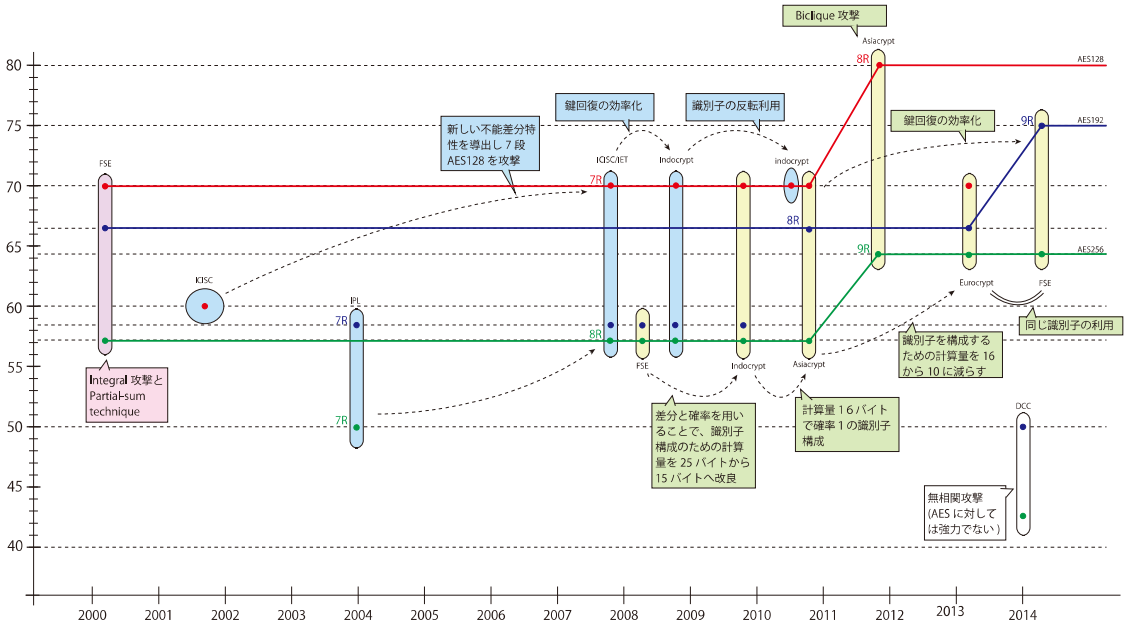


図2.1　AESの攻撃技術進化マップ

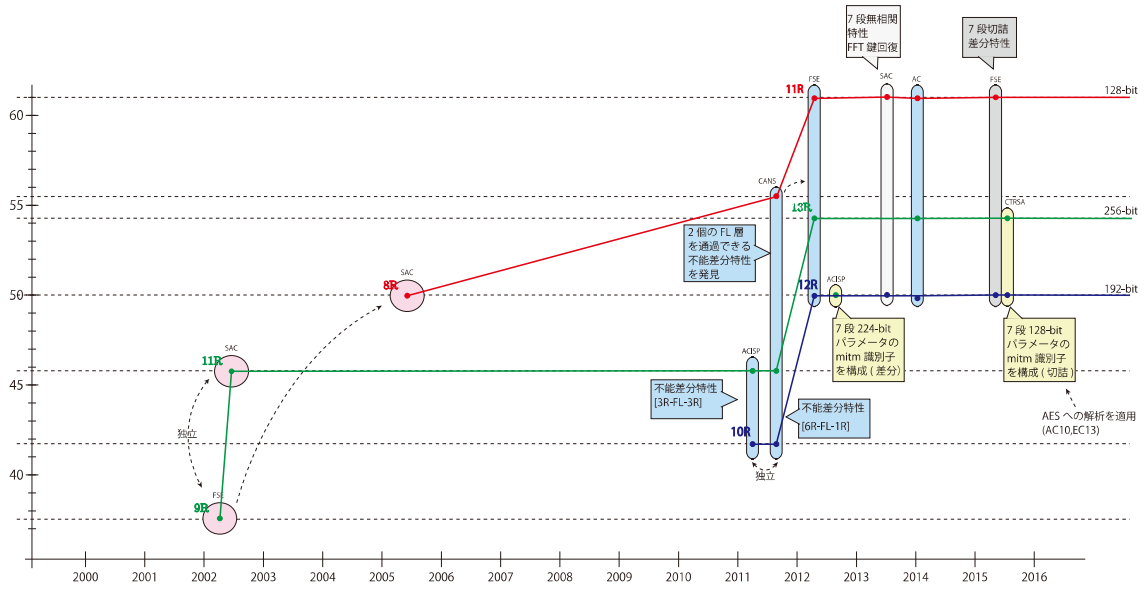


図 2.2　Camellia の攻撃技術進化マップ

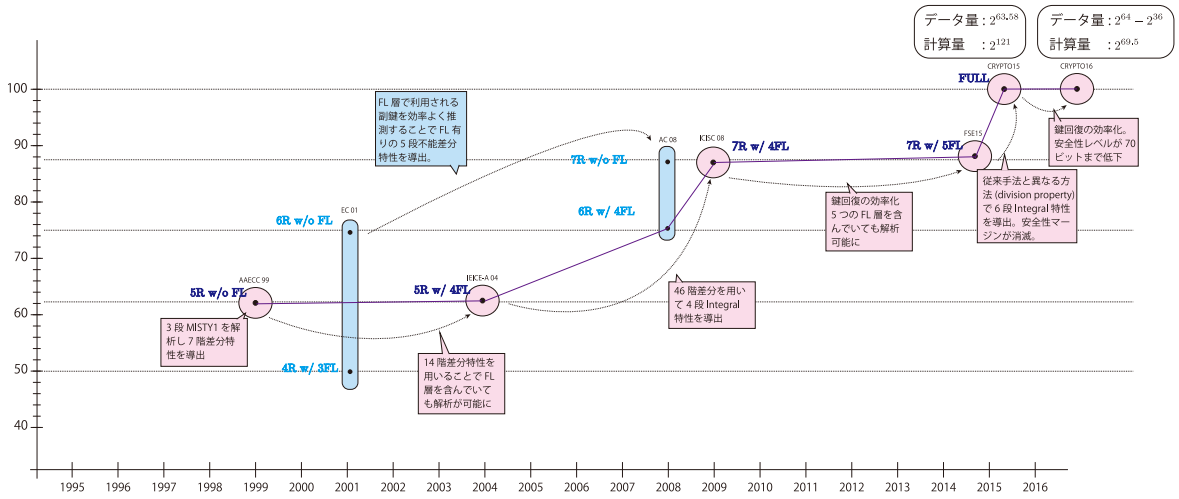


図 2.3　MISTY1 の攻撃技術進化マップ

② 解読手法の進展や計算機能力の向上を勘案した共通鍵暗号の今後の危殆化に関する考察

■公開鍵暗号と共通鍵暗号の安全性評価手法の違いについて（外部の共通鍵暗号の専門家グループによる調査報告書より抜粋）

「公開鍵暗号に対する解析は主に漸近的な解析手法であり、特定パラメータに特化した解析手法は盛んに行われていない。これは (1) 多くの公開鍵暗号はパラメータを大きくすることで安全性を維持できることが多く特定パラメータ特化型な解析手法を研究する動機が削がれること、(2) 攻撃性能が実装依存に依るため計算量の単位が定かではなく、特定パラメータ特化型な解析手法を用いたとしても厳密な計算量見積もりが困難なこと、(3) 漸近的な評価は暗号理論の外側にある計算機科学や数学の分野でも広く議論されるため、学術的確度の高い評価と言えること、などが要因として考えられる。すなわち攻撃が実行可能な小さなパラメータに対して解読可能かを評価し、これを基に大きなパラメータがどの程度の安全性を有するかを予測する。」

「共通鍵暗号に対する解析は主に特定のパラメータに特化した解析手法であり、漸近的な解析手法は行われていない。これは共通鍵暗号の鍵長はそもそも固定のため漸近的な解析手法が議論できないことに起因する。共通鍵暗号は漸近的な評価が出来ない代わりに、実利用のパラメータに対して厳密に安全性を評価する手法が発展している。例えば共通鍵暗号の一回暗号化に要する計算時間を計算量の単位とするという consensus が確立している。」

■共通鍵暗号の危殆化予測に関して（外部の共通鍵暗号の専門家グループによる調査報告書より抜粋）

「学術的な世界においては、設計者が設定した claimed セキュリティが破られた場合に

は、暗号の安全性は破られたとみなされる。例えば、128 ビット鍵の場合、全数探索(2^{128})と比べて鍵の導出に必要な計算量が半分になった場合(2^{127}) でも、理論上は破られたとみなされる。共通鍵暗号における claimed セキュリティは鍵の全数探索を基準としているため、理論上破られたことと、現実的に問題があるレベルにはかい離はあり、理論上の解読が必ずしも現実社会での解読と一致しない。また、鍵の回復に対する計算量を安全性の基準にしているため、全数探索と比較して計算量は少ないが、非常に多くのデータ量が求められる場合も数多く存在する。この場合、実際の攻撃を行うには効率的に攻撃に必要なデータを集める必要があり、ここが実際の攻撃の際にボトルネックとなる場合も考えられる。

しかしながら、理論的な攻撃（claimed セキュリティが破られた場合）と実際的な影響との差を定量的に図ることは不可能である。最悪のケースとしては、理論的に破られたあとにすぐに現実的な攻撃に繋がる可能性もある。例えば、MD5 は2004 年にcollision 攻撃が発表され、そのすぐ2007 年にStevens らによるX.509証明書の偽造攻撃[69] や Sasaki らとLeurent らより電子メールのクライアント認証プロトコルであるAPOP への攻撃[49, 67] が提案されている。 ＜SHA-1、RC4の例中略＞ そのため、共通鍵暗号の世界ではClaimedセキュリティを基準としており、」これが破られた場合、設計者の意図しない脆弱性がはらんでいることから弱い暗号とみなされる。こうなった場合は、学術的な関心は少なくなり、一流の研究者からの解析が行われないため、それ以降の安全性の低下については不明となる。実際,2012 年に中東、イランをターゲットにしたマルウェアFlame には、学術レベルでは未知のMD5 のchosen-prefix collision attack が証明書の偽造に用いられていた[33]。以上の点から、claimed セキュリティが破られた暗号に対しては、新規採用をやめることが望まれる。またアルゴリズム移行には約10 年必要とされていることからも、実際の攻撃に結びつく前にClaimed セキュリティが破られた暗号については移行を検討するべきである。」

■結論（外部の共通鍵暗号の専門家グループによる調査報告書より抜粋）

「上述した通り、暗号学会ではclaimed セキュリティが破られた暗号方式を移行検討の対象とすることで共通鍵暗号の安全性維持に努めている。実際、学術的には攻撃アルゴリズムの進化を予測することは非科学的なため事実上不可能であり、対外的に発表されないアンダーグラウンドな改良の存在も無視できない。仮に継続利用を判断する場合、未発表で改良されている可能性も考慮した上で現在の最良解析手法におけるデータ量・メモリ量・計算量にとらわれることなく慎重な検討が期待される。学術的にはclaimed セキュリティが破られたか否かという厳格な判定基準を設けている以上、継続利用の判断は各利用シーンごとに高度な政治的・経営的判断により行われるべきである。」

＜MISTY1 の攻撃に必要な暗号文データを攻撃者が取得するのに必要な時間（事務局検討）＞

現在知られているMISTY1のフルラウンド攻撃には2^{64}ブロック分の平文・暗号文ペアが必要である。2^{64}ブロックの暗号文データを攻撃者が通信路から入手すると想定した場合に、データ取得に必要な時間をCRYPTREC事務局で調査した（図2.4参照）。IoTデバイス等で暗号化したデータを低速な通信路で伝送する場合から、高速サーバで暗号化したデータを超高速回線で伝送する場合までさまざまなケースがある。 低速回線の例として、交通系等で利用されているICカード規格FeliCa（通信速度： 212kbps）の場合、暗号文データの収集に約3.5億年、超高速回線の例では、メモリ規格HBM(High Bandwidth Memory)2（メモリ帯域：8Tbps）の場合、暗号文データの収集に約9.4年かかる試算になる。

＜暗号技術評価委員会での審議＞

2015年度に出したMISTY1の安全性に関する速報では、「この攻撃は、解読に必要なデータ量が膨大であることから、現実的な脅威ではないと考えられます。CRYPTREC では、MISTY1の安全性に関して引き続き調査を行い、CRYPTREC Webサイトにて報告する予定です。」としている。今年度の調査・検討をふまえて、MISTY1に関して今後どのようなアクションをとるのがよいか、下記の4つの案を例示して審議を行った。

（例）

1. MISTY1の解読に必要なデータ量が膨大であることから、現在の見解を維持する。
2. MISTY1の新規採用は控えるよう、例えばCRYPTREC暗号リストに脚注を加える。（但し現在、64ビットブロック暗号全体に「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。」の脚注あり）
3. 利用形態によりMISTY1からの移行を推奨する。（利用時の注意点を示す）
4. MISTY1からの移行を推奨する。（MISTY1を「推奨候補暗号リスト」から「運用監視暗号リスト」に移す）

審議の結果、1 と 4 はない、2 または 3 を具体的にどうするかについて議論がなされ、

- 今回の外部専門家からの意見等をふまえ、CRYPTRECとして、現在の見解を維持するのではなく、何らかのアクションを検討した方がよいのではないか。例えば、64ビットブロック暗号全体に推奨される安全な利用方法であり、現在報告されているMISTY1に対する攻撃を回避できる方法として、2^{32} ブロックごとに鍵を変更するなどの利用方法を示す。
- MISTY1の利用状況（どこでどう使われているか）の調査を検討してはどうか。すでに利用されている暗号技術に対してCRYPTRECが何かアクションを起こす場合、ユーザにとってどのようなインパクトがあるかを把握しておくことが重要である。

などの意見が出た。

2.2. 注意喚起レポートの発行

2.2.1. 暗号アルゴリズムの脆弱性に関する情報発信

暗号アルゴリズムの脆弱性に関する CRYPTREC からの情報発信について、下記に示すフローチャート(図 2.4)に基づいて取り扱うことが 2015 年度の暗号技術検討会にて承認されている。

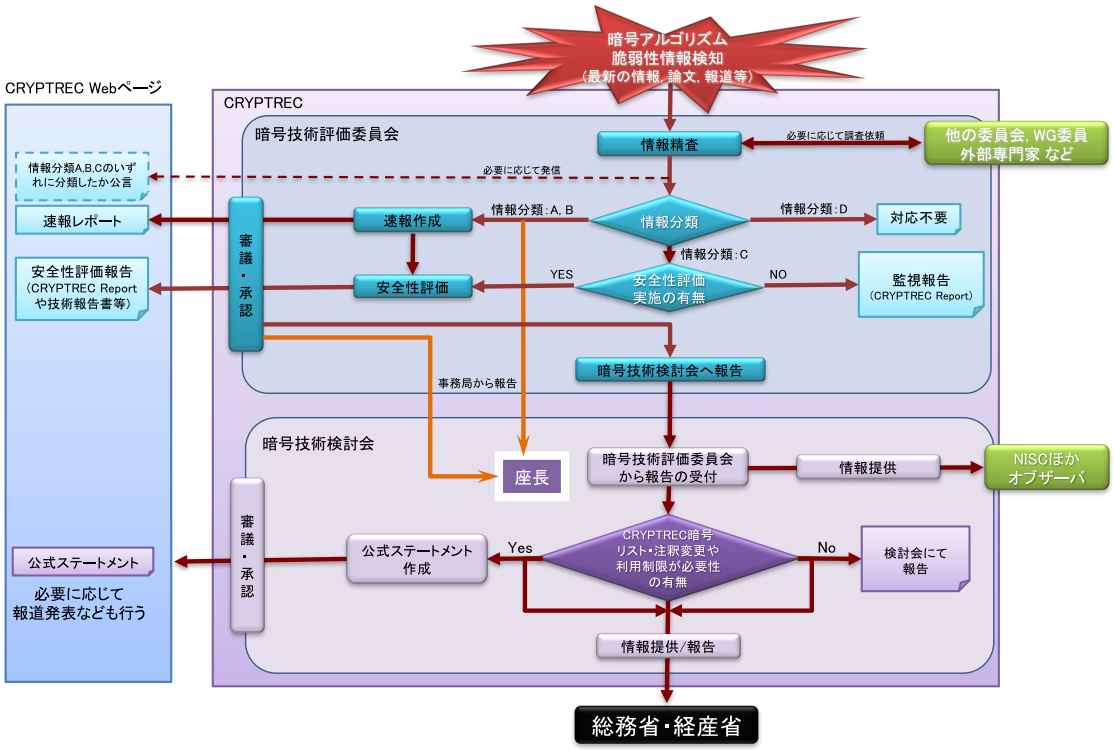


図2.4　暗号アルゴリズムの脆弱性に関する情報発信フロー

[情報発信フローの概要]

(1)　暗号アルゴリズムの脆弱性情報を検知した後、CRYPTREC において参照している仕様に対する攻撃成功に関する情報か、もしくは攻撃成功までは到達していないが攻撃に必要となる計算量の著しい低下につながる結果であるか否かについて判断をし、以下のいずれに属する情報であるかを分類する。

A) 暗号アルゴリズムの完全な危殆化による緊急対応

B) 正確で信頼性の高い情報を発信することによる過剰反応防止

C) 長期的なシステムの安全性維持のための対策喚起

D) 対応不要

(2)　上記の分類のうち、A)もしくは B)に分類される脆弱性情報については、速報を公開し、また、安全性評価を実施し、その評価結果を公開する。C)に分類される脆弱性

情報については、必要に応じて C)に分類された情報であることの公表や安全性評価を実施する。ここで、速報とは、外部で公開されている情報に基づき記載するもので、CRYPTREC では自ら詳細評価は行っていないが、信頼に足る機関・組織等から得た情報に基づくものとする。また、安全性評価報告とは、CRYPTREC として安全性評価を実施しその評価結果をまとめたものとする。

（3） 取り扱う暗号アルゴリズムの範囲は、CRYPTREC 暗号リストに掲載されている暗号技術、および CRYPTREC 暗号リストに掲載されていないが、影響度が高いと暗号技術評価委員会で認められた暗号技術を対象とする。

（4） 速報および安全性評価結果は暗号技術評価委員会の審議に基づき公開される。また、これら脆弱性情報は、暗号技術評価委員会から暗号技術検討会に報告される。

2.2.2. SHA-1 の安全性低下について

2017 年 2 月 23 日に、CWI(オランダ)、Google(USA)の共同研究チームは、Web サイト[2]に論文[3]を公開し、ハッシュ関数 SHA-1 の衝突発見に初めて成功したと発表した。このため、CRYPTREC の Web ページに注意喚起の意味で「SHA-1 の安全性低下について」（平成 29 年 3 月 1 日)[4]を公表した。

2.3. 推奨候補暗号リストへの新規暗号の追加

2.3.1. SHAKE128

2015 年度の審議により、ハッシュ関数 SHA-2、SHA-3 が CRYPTREC 暗号リストへ追加されたが、ハッシュ関数 SHA-3 ファミリーの 1 つである SHAKE128 は現在含まれていない。SHAKE128 について、これまでの安全性評価と実装性能評価の結果の通り、出力長を 256 ビット以上とすれば、CRYPTREC 暗号リストへ追加するのに十分な安全性および実装性能を有していることが暗号技術評価委員会での審議の結果、承認された。また、SHAKE128 の CRYPTREC 暗号リストの推奨候補暗号リストへの追加が 2017 年 3 月に開催された第 1 回暗号技術検討会にて承認された。

なお、SHAKE128 のリスト追加時には、現在の SHAKE256 に対する脚注と同じ「ハッシュ長は 256 ビット以上とすること」という脚注をつける。

① 安全性評価

SHAKE128 を含む SHA-3 について、下記有識者に外部評価を依頼し、安全性に十分なマージンがあり、現実的な脅威の観点から大きな問題点は見つかっていないという評価結果を得ている。

---

[2] https://shattered.io/

[3] https://shattered.io/static/shattered.pdf

[4] http://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html

- Donghoon Chang 氏 (Indraprastha Institute of Information Technology Delhi, India)
  2014 年度 技術報告書 「Security Evaluation Report on SHA-224, SHA-512/224, SHA-512/256, and the six SHA-3 Functions」[5]
- Itai Dinur 氏 (École Normale Supérieure, France)
  2014 年度 技術報告書 「Security Evaluation of SHA-3」[6]

② 実装評価

SHAKE128 を含む SHA-3 について、下記有識者に外部評価を依頼し、ソフトウェア実装、ハードウェア実装ともに十分な実装性能を有するという評価結果を得ている。

- これまでに行われてきた実装性能評価に関する研究結果のサーベイ
  崎山 一男 教授 (電気通信大学)
  2013 年度 技術報告書「ハッシュ関数 SHA-224, SHA-512/224, SHA-512/256 及び SHA-3 (Keccak) に関する実装評価」[7]
- FPGA 上での性能評価
  佐藤 証 教授 (電気通信大学)
  2013 年度 第三回暗号技術評価委員会 資料 2-3 「ハッシュ関数のハードウェア実装およびその性能測定」

2.4. ChaCha20-Poly1305 の CRYPTREC 暗号リストへの追加を視野に入れた評価について

ChaCha20-Poly1305 は、ユーザ数の多いブラウザに採用されるなど、実導入が進んでいるアルゴリズムである。第 1 回暗号技術評価委員会(2016 年 7 月 27 日)および、2015 年度第 3 回重点課題検討タスクフォース(2016 年 2 月 3 日)で、その安全性評価に対する要望が複数あったことから、暗号技術評価委員会にて安全性評価を行った。詳しくは、「Security Analysis of ChaCha2-Poly1305 AEAD」[8]を参照のこと。

① 評価結果 (評価者の見解)

A) 認証暗号 ChaCha20-Poly1305 に対する安全性評価を行った。ChaCha20-Poly1305 は、暗号化のためにストリーム暗号 ChaCha20 が使われ、認証のためにメッセージ認証コード(MAC) Poly1305 が使われている。認証暗号としての安全性に関しては、ChaCha20 が擬似乱数生成器と見なすことができ、かつ、Poly1305 が安全なユニバーサルハッシュ関数であれば、ChaCha20-Poly1305 は、認証暗号としての安全性を満たすことが証明されている[Pro14]。

[5] http://www.cryptrec.go.jp/estimation/techrep_id2403_2.pdf
[6] http://www.cryptrec.go.jp/estimation/techrep_id2402.pdf
[7] http://www.cryptrec.go.jp/estimation/techrep_id2301.pdf
[8] http://www.cryptrec.go.jp/estimation/cryptrec-ex-2601-2016.pdf

B) Poly1305 については、ε-almost-Δ-universal であることが証明でき、安全なユニバーサルハッシュ関数であることが示されている[Ber05b]。

C) 特に ChaCha20 の安全性に注力し、ストリーム暗号に対して提案されている各種攻撃に対する評価を実施した。タイムメモリデータトレードオフ攻撃に対しては、現実的な設定の下では攻撃に要する計算量が膨大になるといえる。サイドチャネル攻撃に対しては、既存の対策手法により防ぐことが可能である。その他の既知の攻撃に対しては、鍵の総当たりよりも効率的なものは見つかっていない。以上から、ChaCha20 については、擬似乱数生成器と見なすことができると考えられる。

D) 以上の結果から、認証暗号 ChaCha20-Poly1305 に対する攻撃は発見されていないと結論付ける。

(参考文献)

[Pro14] Gordon Procter. A Security Analysis of the Composition of ChaCha20 and Poly1305, Cryptology ePrint Archive: Report 2014/613, 2014. (https://eprint.iacr.org/2014/613).

[Ber05b] Daniel Julius Bernstein. The Poly1305-AES Message Authentication Code, FSE 2005, LNCS, volume 3557, pages 32-49, 2005.

② 暗号技術評価委員会での審議結果

評価者からのレポートを踏まえ、現時点では ChaCha20-Poly1305 は、認証暗号として、具体的な脅威は見つかっていないと考えられる。

③ 暗号技術検討会での審議結果

2009 年にリスト改定に伴う公募を行った際は、応募暗号アルゴリズムが評価対象となるための必要条件として、査読付き国際会議に採録されていることを課していた（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)）[9,10]。一方、「国際標準化等の実績がある」ことを理由に事務局選出のアルゴリズムとして評価対象とした例もあった[11]。

「国際標準化等の実績がある」ことを根拠として事務局で選出する暗号アルゴリズムに対して CRYPTREC 暗号リストへの追加を視野に入れた評価を開始する場合には、暗号技術検討会で判断を行い、これを受けて、暗号技術評価委員会で安全性評価・実装性能評価を行う。

[9] http://www.cryptrec.go.jp/topics/cryptrec_20090527_application_guide.html,
[10] http://www.cryptrec.go.jp/topics/cryptrec_20091001_application_guide_2009-2.pdf
[11] CRYPTREC Report 2011 暗号方式委員会報告(2.3.5 事務局選出暗号技術)

2.5. Post Quantum Cryptography に関する動向について

NIST は、Post-Quantum Cryptography に関するアルゴリズムの公募を 2016 年 12 月 20 日から正式に開始した。公募に関する詳細は Web 上[12]で公開されている。公募の〆切は、2017 年 11 月 30 日である。また、下記の通り、PQCrypto 2018 開催後に、応募者のプレゼンテーションがある予定である。

- PQCrypto 2018： Florida, 9--11 April 2018.
- NIST workshop： 12--13 April 2018.

2.6. 文書番号体系について

CRYPTREC では、年度成果物としてガイドライン、報告書を公開しているが、今後は文書の番号から内容(およびその文書の位置づけ)がわかる文書管理をするため、暗号技術検討会が設置した重点課題検討タスクフォースにおいて、CRYPTREC 文書についての番号体系を整理することとした。2017 年 3 月に開催された第 1 回暗号技術検討会にて承認された。詳しくは、暗号技術検討会 2016 年度報告書[13]の 3.1.3 節の(2)を参照のこと。

[12] http://www.nist.gov/pqcrypto
[13] http://www.cryptrec.go.jp/report/c16_kentou_final.pdf

2.7. 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2.3に示す通りである。

表 2.3 国際会議への参加状況

学会名・会議名		開催国・都市	期間
Eurocrypt 2016	International Conference on the Theory and Applications of Cryptographic Techniques	オーストリア・ウィーン	2016年5月9日～2016年5月12日
Crypto 2016	International Cryptology Conference	アメリカ・サンタバーバラ	2016年8月14日～2016年8月18日
FDTC 2016	Fault Diagnosis and Tolerance in Cryptography	アメリカ・サンタバーバラ	2016年8月16日
CHES 2016	Conference on Cryptographic Hardware and Embedded Systems	アメリカ・サンタバーバラ	2016年8月17日～2016年8月19日
PROOFS 2016	Security Proofs for Embedded Systems	アメリカ・サンタバーバラ	2016年8月20日
IWSEC 2016	International Workshop on Security	日本・東京	2016年9月12日～2016年9月14日
ACM CCS 2016	ACM Conference on Computer and Communications Security	オーストリア・ウィーン	2016年10月25日～2016年10月28日
Asiacrypt 2016	International Conference on the Theory and Applications of Cryptology and Information Security	ベトナム・ハノイ	2016年12月4日～2016年12月8日
CT-RSA 2017	RSA Conference Cryptographers' Track	アメリカ・サンフランシスコ	2017年2月13日～2017年2月17日
FSE 2017	International Conference on Fast Software Encryption	日本・東京	2017年3月6日～2017年3月8日
PKC 2017	International Conference on Practice and Theory in Public-Key Cryptography	オランダ・アムステルダム	2017年3月29日～2017年3月31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5 を参照のこと。

2.7.1. 共通鍵暗号の解読技術

・Polytopic Cryptanalysis [Eurocrypt 2016]

Tyge Tiessen

差分暗号解析は、2 つの平文の違いと各々の対応する暗号文の違いとの統計的な依存関係を利用しているが、その拡張としてより多くのテキストの相互依存関係を利用する多面的暗号解析を導入した。不可能差分解析に関しては従来よりも優位性があり、縮退版 DES、および縮退版 AES に関して部分的に既存攻撃を凌ぐ結果を得た。

・A 2^{70} Attack on the Full MISTY1 [Crypto 2016]

Achiya Bar-On and Nathan Keller

64 ビットブロック暗号 MISTY1 に対する鍵回復攻撃が発表された。NTT の藤堂氏の結果を改良したものであり、解読計算量は約 2^{70} にまで下がっているが、解読に必要なデータ量は 2^{64} であり、まだ現実的な脅威とは言えない。本結果は事前にプレプリントで公表されており、CRYPTREC はホームページにて解読に必要なデータ量・計算量の表および「解読に必要なデータ量が膨大であることから現実的な脅威ではないと考えられる」という見解を公表済である。

2.7.2. 公開鍵関数の解読技術

・New Complexity Trade-Offs for the (Multiple) Number Field Sieve Algorithm in Non-Prime Fields [Eurocrypt 2016]

Palash Sarkar and Shashank Singh

位数 $Q=p^n$, $n>1$ の有限体における数体篩法(NFS: Number Field Sieve)の新しい多項式選択アルゴリズムを提案する。$p=L_Q(2/3, c_p)$, $c_p \in [3.39, 20.91]$の場合の NFS は、他の多項式選択アルゴリズムによる NFS/MNFS(Multiple NFS: 複数数体篩)よりも小さい計算量となる。本多項式選択アルゴリズムを使用した MNFS は本多項式選択アルゴリズムを使用した NFS よりも小さい計算量となる。$c_p \in (0, 1.12] \cup [1.45, 3.15]$の場合は、本多項式選択アルゴリズムを使用した MNFS の計算量は、Conjugation を使用した MNFS の計算量と同じであり、それ以外の場合は、本多項式選択アルゴリズムを使用した MNFS の計算量は、あらゆる既存方式よりも小さくなる。

・Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case [Crypto 2016]

Taechan Kim and Razvan Barbulescu

離散対数問題解読における多項式選択ステップの改良により、解読計算量を削減できることを示した。対象とした基礎体は中程度の大きさの素数の拡大体であり、$Q=p^n$ に対して、数体篩法の場合、計算量を $L_Q(1/3, (96/9)^{1/3})$ から $L_Q(1/3, (48/9)^{1/3})$ に下げ、複数数体篩法

の場合、$L_Q(1/3, 2.15)$から $L_Q(1/3, 1.71)$に下げた。CRYPTREC 暗号リストで利用している素体ではないため CRYPTREC に直接的な影響はないが、ペアリング暗号等の条件に当てはまる体を利用している場合には注意が必要である。

・A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm [Asiacrypt 2016]

Palash Sarkar and Shashank Singh

Kim らが扱っていない素数べき $Q=p^n$ の場合の拡張塔数体篩法を扱い、NFS の場合 $L_Q(1/3, (64/9)^{1/3})$、MNFS の場合 $L_Q(1/3, 1.88)$を得た。これまでの最小計算量は、それぞれ $L_Q(1/3, (96/9)^{1/3})$および $L_Q(1/3, 2.12)$であった。

・Extended Tower Number Field Sieve with Application to Finite Fields of Arbitrary Composite Extension Degree [PKC 2017]

Taechan Kim and Jinhyuck Jeong

Crypto2016でKim、Barbulescuによって示されたexTNFS （Extended tower number field sieve）アルゴリズムの一般化を提案している。exTNFSは有限体F（Q） （p ： 素数, $Q=p^n$）に対しての離散対数問題を計算する最先端アルゴリズムであり、$n = \eta\kappa$、gcd（η, κ）＝1の時に適用されるが、一般化により最良の漸近複雑度を維持しつつ任意の合成数nに対して適用可能とした。nが合成数の時、離散対数をL_Q（1/3, 1.71）で計算できることを示した。これはAsiacrypt 2016でSarkar、Singhによって示されたnが2のべき乗の合成数の時の最速値L_Q（1/3, 1.88）より速くなっている。

・On the Bit Security of Elliptic Curve Diffie-Hellman [PKC 2017]

Barak Shani

素体上で定義された楕円曲線の楕円 Diffie-Hellman 鍵交換プロトコルのビットセキュリティを初めて示した。Diffie-Hellman 鍵の x 座標の最上位ビットの約 5/6 を求める計算量と、鍵全体を求める計算量が同等であることを示した。また 5/6 の下位ビットについても同様の結果を示した。これらは楕円曲線 HNP(Elliptic curve Hidden Number Problem)より導かれる。また拡大体上の楕円曲線について既知の手法を改善し、Diffie-Hellman 鍵の x 座標または y 座標の 1 成分を（基礎体において）計算することは、鍵全体を求める計算量と同等であることを示した。

2.7.3. ハッシュ関数の解読技術

・Freestart collision for full SHA-1 [Eurocrypt 2016]

Marc Stevens, Pierre Karpman and Thomas Peyrin

SHA-1 のフリースタート衝突ペアが具体的に示された。64GPU クラスタによる 10 日間の

計算、およそ $2^{57.5}$ 回の圧縮関数呼び出しが攻撃に必要であった。2005 年の理論的衝突攻撃のブレークスルー以来の進歩、特に Crypto 2015 における Karpman らの 76 段 SHA-1 をより高速化するテクニックを使い、また、Eurocrypt 2013 の Stevens の最適な攻撃条件を得る結果を利用した。著者らは、産業界に SHA-1 の利用を止めるよう勧告している。

・The first collision for full SHA-1 [https://shattered.io/]

Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini and Yarik Markov

2017 年 2 月 23 日に、CWI Amsterdam と Google Research の共同研究チームが、ハッシュ関数 SHA-1 の衝突発見に初めて成功したと Web ページ(https://shattered.io/)上で発表した。この発表では、全数探索の計算量(2^{80})よりも 10 万倍速い $2^{63.1}$ 回の SHA-1 の計算量で衝突を発見したと報告されている。本発表の内容はまだ著名な国際学会等で発表はされてはいないが、実際にハッシュ関数が同じ異なる PDF ファイルの例も公開されており、CRYPTREC では 3 月 1 日付でホームページにて本発表に対する見解を速報にて公開した。

2.8. 委員会開催記録

2016 年度、暗号技術評価委員会は、表 2.4 の通り 2 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 2.4　暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2016 年 7 月 27 日	委員会活動計画案の承認、ワーキンググループ活動計画案の承認、外部評価、仕様書の参照先の変更、監視状況報告
第 2 回	2017 年 3 月 21 日	ワーキンググループ活動の年度報告、ChaCha20-Poly 1305 の安全性評価について、仕様書の参照先の変更、KCipher-2 の仕様書の変更について、外部評価結果、共通鍵暗号の安全性調査と MISTY1 について、SHA-1 の安全性低下について、監視状況報告、CRYPTREC Report 2016 目次案

2.9. 暗号技術調査ワーキンググループ開催記録

2016 年度、各暗号技術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 2.5 の通りである。表 2.6 及び表 2.7 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 2.5　2016 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、楕円曲線上の離散対数問題の困難性に関する調査、多重線形写像及び難読化の最新動向に関する調査を行う。また、素因数分解の困難性や楕円曲線上の離散対数問題の困難性に関しては、例年公表している予測図の更新を行う。
軽量暗号ワーキンググループ	本間 尚文	軽量暗号ワーキンググループは、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。軽量暗号を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的とした「暗号技術ガイドライン（軽量暗号）」を発行する。

表 2.6　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	2016 年 7 月 27 日	活動計画案の検討、今年度の調査の進め方の検討
第 2 回	2017 年 2 月 21 日	予測図の更新に関する検討、難読化の調査に関する検討 楕円曲線上の離散対数問題の調査に関する検討、今後の課題に関する検討

表 2.7　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	2016 年 7 月 28 日	暗号技術ガイドライン(軽量暗号)の作成方針に関する検討、軽量暗号に関する実装詳細評価の方針に関する検討、NIST Lightweight Cryptography Workshop 報告、英語版作成方針に関する検討、CAESAR プロジェクト紹介
第 2 回	2016 年 10 月 5 日	暗号技術ガイドライン(軽量暗号)の目次案・掲載するアルゴリズムに関する検討、実装詳細評価に関する検討、英語版作成に関する検討
第 3 回	2017 年 1 月 16 日	暗号技術ガイドライン(軽量暗号)の作成スケジュールに関する検討、軽量暗号のユースケースに関する検討、暗号技術ガイドライン(軽量暗号)の掲載するアルゴリズムに関する検討、軽量暗号に関する実装詳細評価に関する検討、英語版作成に関する検討

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

(1)楕円曲線上の離散対数問題(ECDLP)の困難性に関する調査

2012 年度の暗号技術調査 WG(計算機能力評価)における調査結果において言及があったように、ECDLP に対する指数計算法(Index Calculus)の計算量評価についての研究結果が近年発表されてきている。2015 年～2016 年度は、これらの研究内容を調査し、見解をまとめる。

(2)多重線形写像(Multi linear map)及び難読化(Obfuscation)の最新動向に関する調査

2013 年～2014 年度は、格子問題等の困難性に関する調査を行い、「格子問題等の困難性に関する調査」を作成する。2015 年～2016 年度は、近年研究が進展している多重線形写像及び難読化に関する研究動向を調査する。

(3)予測図の更新

例年公表している予測図の更新に大きく影響を与えるような研究結果等がないかどうかの確認を行う。また、TOP500.ORG[1]が公表する計算機能力に関するデータに基づき、例年公表している予測図の更新を行う。

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	日本電信電話株式会社
委員：	太田　和夫	電気通信大学
委員：	草川　恵太	日本電信電話株式会社
委員：	國廣　昇	東京大学
委員：	下山　武司	株式会社富士通研究所
委員：	安田　雅哉	九州大学

3.1.3. 活動概要

(1)　楕円曲線上の離散対数問題(ECDLP)の困難性に関する調査

- 2015 年度は、ECDLP に対する指数計算法について過去に発表された論文などを精査し、論点や課題を事務局にて整理した。

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

- 2016 年度は、昨年度事務局が整理した論点や課題に基づき、近年発表されている指数計算法を用いた攻撃手法を解説する資料を作成した。

(2) 多重線形写像(Multi linear map)及び難読化(Obfuscation)の最新動向に関する調査

- 2015 年度は、多重線形写像に関する過去の論文を調査し、提案されている代表的な応用例についてまとめた。また、難読化に関して安全性について外部評価を行い、その研究動向についてまとめた。
- 2016 年度は、多重線形写像に関して安全性について外部評価を行い、近年研究が進展している多重線形写像に関する研究動向をまとめた。

(3) 予測図の更新

- 2015 年度は、「素因数分解問題の困難性」及び「楕円曲線上の離散対数問題の困難性」に関するグラフの更新を行った。
- 2016 年度は、予測図の更新に加えて、過去の議論・経緯などを把握できる資料について検討した。

3.1.4. 成果概要

(1) 楕円曲線上の離散対数問題(ECDLP)の困難性に関する調査

楕円曲線上の離散対数問題(ECDLP)に関する指数計算法(Index Calculus)について調査を行い、研究内容をまとめることが第 1 回 WG にて承認され、下記の通り実施した。第 2 回 WG にて承認された当該調査における見解を下記に記す。なお、調査レポートの概要は 3.1 節 付録 A.1 に記す。また、調査レポートは、付録 3(p.71)または、「楕円曲線上の離散対数問題に関する指数計算法」[2]を参照のこと。

[評価レポートにおける見解]

楕円曲線上の離散対数問題(ECDLP)の困難性は楕円曲線暗号やペアリング暗号の安全性の基盤となっている (図 3.1)。今のところ ECDLP を最も効率よく解くアルゴリズムは ρ 法であり、その計算量は群の位数に関して指数時間である。

その一方で、近年、計算量が準指数時間となる、ECDLP に関する指数計算法が提案された[PQ12]。しかし、この計算量評価では検証が不十分な仮定(First Fall Degree Assumption(FFDA)など)が導入されており、その仮定の正当性は理論的にも数値実験的にも十分に立証されていない。さらに ρ 法を利用した場合に解くことが期待できる十分大きな ECDLP が当該指数計算法によって解かれたという成果も報告されていない。

従って、現時点では当該指数計算法より、 ρ 法の方が計算効率が優れていると判断するのが

[2] http://www.cryptrec.go.jp/estimation/cryptrec-ex-2602-2016.pdf

妥当である。

[WG の判断]

当該指数計算法の計算量が準指数時間であることは理論的にも数値実験的にも現時点では十分に立証されていない。従って、ECDLP を安全性の根拠とする暗号の安全性評価について、現時点では、標数に拠らず、今のところ最も効率が良い ρ 法ベースの安全性評価基準を採用していれば十分であると判断する。ただし、引き続き、当該指数計算法の研究動向を把握しておく必要がある。

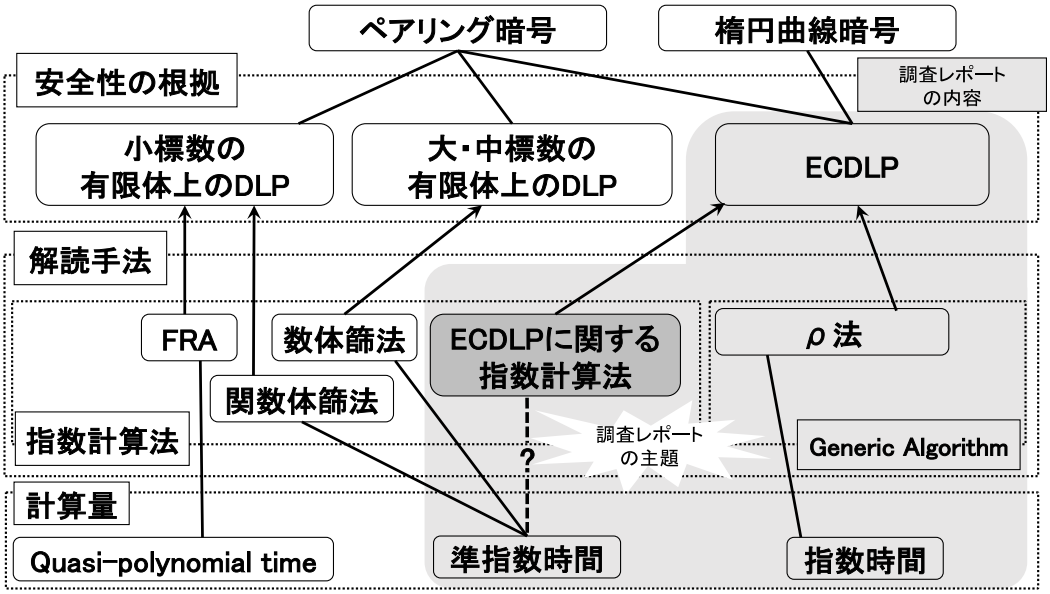


図 3.1:離散対数問題と種々の解読手法との関係

(2) 多重線形写像(Multi linear map)及び難読化(Obfuscation)の最新動向に関する調査

多重線形写像(Multi linear map)の最新動向に関する調査を行い、研究動向をまとめることが第 1 回 WG にて承認され、下記の通り実施した。第 2 回 WG にて承認された多重線形写像の最新動向に関する見解を下記に記す。なお、評価レポートの概要は 3.1 節 付録 A.2 に記す。また、調査レポートは、付録 4(p.101)または、「Cryptographic Multilinear Maps, A Status Report」[3]を参照のこと。

[評価レポートにおける見解]

現在提案されている多重線形写像は、多重線形写像に基づく多重 Diffie-Hellman 鍵交換方式に対して攻撃論文が存在する。知識型暗号方式 (Witness Encryption) や 識別型難読化方式

[3] http://www.cryptrec.go.jp/estimation/cryptrec-ex-2603-2016.pdf

(Indistinguishability Obfuscation) の存在証明に用いられていた多くの安全性仮定が成立しないことも示されている。一方、識別型難読化方式 が存在すれば多重線形写像が構成可能であることも示されている。つまり、識別型難読化方式に対する構成不可能性は示されていないため、その構成可能性は残されている。

[WG の判断]

多重線形写像は、従来技術では実現し難い機能などを提供することができる、有力なプリミティブであり、非常に注目されその進展が目覚ましい技術である。現時点では安全な多重線形写像の構成は実在しないが、その存在の可能性は否定されていないことから、引き続き研究動向は把握しておき、今後具体的な構成方法が提案された折に、改めて評価・検討を行うこととする。

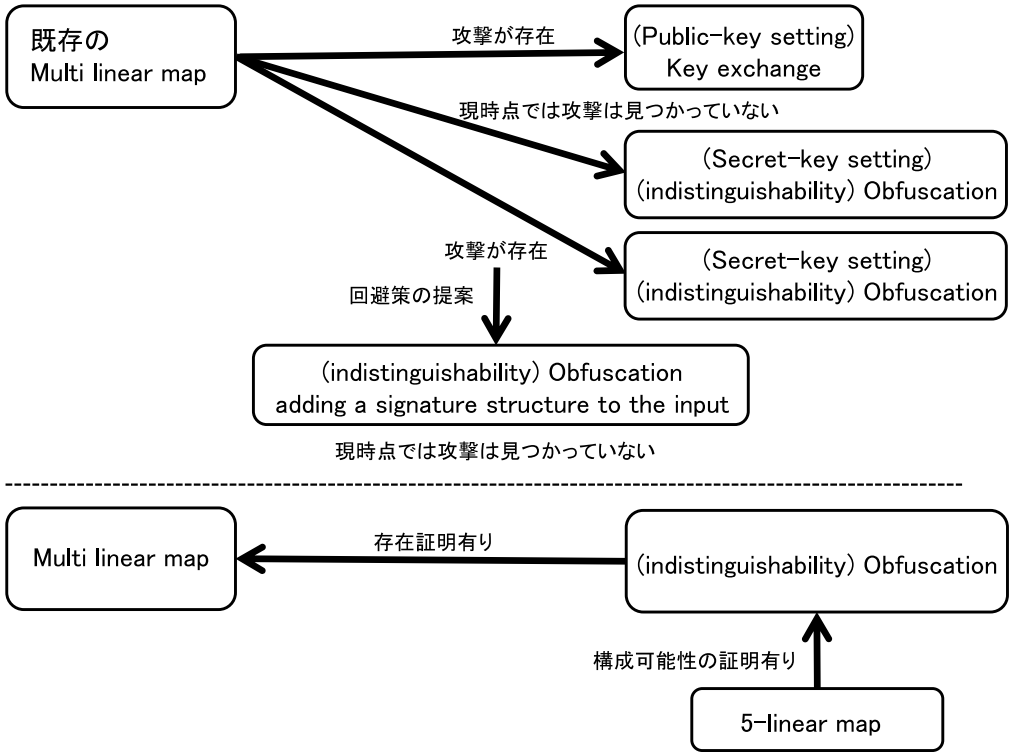


図 3.2：多重線形写像の構成に関する現状

(3) 予測図の更新

「素因数分解問題の困難性」及び「楕円曲線上の離散対数問題の困難性」に関して、2016 年 6 月及び 11 月に TOP500.org のスーパーコンピューターのリストの更新があったため、2015 年度に作成した素因数分解問題及び楕円曲線上の離散対数問題の困難性に関する予測図をそれぞれ更新した（3.1 節 付録 A.3 図 3.3 及び図 3.4)。

図 3 を作成するにあたって使用したふるい処理に関するデータは 2006 年度のものであり、古くなってきたため、更新が必要である。また、過去の議論・経緯などを把握できる資料の作成については、過去の活動内容を Web 上で検索し易いように改善することで今後対応する。

(4) 有限体上の離散対数問題の安全性に関する最新動向について

(a) 768 ビット DLP の求解記録について

2016 年 6 月 16 日に、メーリングリスト NMBRTHRY[4]に 768 ビットのサイズの素体における離散対数の計算に成功したとの報告が掲載された。現在、この結果は Cryptology ePrint Archive 2017/067 に掲載され[5]、EUROCRYPT 2017 に採録される予定となっている。以前の記録は、596 ビット(2014 年 6 月 11 日)であった。篩ステップに 4000 Intel Xeon 2.2GHz・年、線形代数ステップに 900 Intel Xeon 2.2GHz・年を要している(なお、RSA768 については、篩ステップに 1500 Intel Xeon 2.2GHz・年、線形代数ステップに 75 Intel Xeon 2.2GHz・年を要していた。)。

CRYPTREC 暗号リストに掲載されている DSA 及び Diffie-Hellman の安全性については,素体(GF(p),p:素数)から構成されており、p のサイズが 2048 ビット以上であれば直ちに影響はない。

2015 年に Logjam 攻撃を発表した論文[6]では、特定の素数 p に対して事前計算(数体篩法における多項式選択・篩・線形代数の各ステップに相当)を十分に実行しておけば、同じ p に対してターゲットとなる元の離散対数を効率的に計算可能であるリスクがあることを指摘していた。H. Kario 氏のブログ Securitypitfalls の 2016 年 7 月のデータ[7]によれば、約 60 万の主要なサイトのうち、鍵交換において DH が利用できるのは約 54.3%あり、そのうちの約 35.5%は 1024 ビット以下の鍵長である。鍵長を 2048 ビット以上に設定するなどの注意喚起が必要であると考えられる。

(b) Extended Tower Number Field Sieve の影響について

有限体上離散対数問題(DLP)を計算する「数体篩法」の改良 Extended Tower Number Field Sieve(exTNFS)の提案[1]が CRYPTO 2016 に採録された。exTNFS では、有限体の中でも特に合成数次数の拡大体の DLP を考えている。CRYPTREC 暗号リストには合成数次数拡大体の DLP を安全性の根拠とする暗号技術は掲載されていないため影響は無い。しかし、現在、研究・開発が進められているペアリング暗号の中には合成数次数拡大体の DLP が安全性の根拠となるものがある (例: Barreto-Naehrig 曲線上ペアリングでは 12 次拡大体) ため、それらの安全性に影響があると考えられる。

[4] https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1606&L=NMBRTHRY&P=3649
[5] https://eprint.iacr.org/2017/067
[6] https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf
[7] https://securitypitfalls.wordpress.com/2016/09/06/july-2016-scan-results/

拡大体F_Qの DLP に対する数体篩法の漸近的な計算量は

$$L_Q(1/3, c) = \exp((c + o(1))\,(\log Q)^{\frac{1}{3}}\,(\log\log Q)^{\frac{2}{3}}) \qquad (式\ 1)$$

により与えられる。定数cが小さいほど計算量が小さくなる。また、標数の大きさにより漸近的な計算量が異なる (medium prime/boundary/large prime に分けられている)。表 3.1 ([1]から転載)は従来の数体篩法(NFS, TNFS)と exTNFS の計算量の比較である。表中の値は $c = (c'/9)^{1/3}$となるc'である。

表 3.1：式 1 における c' の値([1]から転載)

$p = L_Q(l_p)$	$1/3 < l_p < 2/3$	best $l_p = 2/3$	$2/3 < l_p < 1$
TNFS [5,6]	none	none	64
NFS-JLSV [7]	128	64	64
NFS-(Conj and GJL) [8]	96	48	64
NFS-SS [9]	96	48	64
exTNFS [1]	48	48	64

特に標数が特殊な構造を持っている場合は、その構造を利用してさらに計算量を小さくすることができる。特にこのような場合には特殊数体篩法(SNFS)と呼ばれる。Barreto-Naehrig 曲線のペアリングでは標数が特殊な構造であるため、特殊数体篩法のケースにあたる。SNFS の場合の計算量を表 3.2 ([1]から転載)に示す。

表 3.2：式 1 における c' の値([1]から転載)

$p = L_Q(l_p)$	$1/3 < l_p < 2/3$	$2/3 < l_p < 1$
STNFS-JP [10]	64	32
STNFS [5]	none	32
SexTNFS [1]	32	32

Barreto-Naehrig 曲線のペアリングは、例えば IETF Internet Draft[2]によれば、標数が 254 ビット素数､拡大次数 12 のときおおよそ 128 ビットセキュリティ(より正確には 126 ビット[3])であると考えられていた(これらの安全性解析では, 数体篩法の計算量は$c = (64/9)^{1/3}$で考慮されていたためである。)。SexTNFS により計算量が$c = (32/9)^{1/3}$に削減されたため、128 ビットセキュリティを満たさないと考えるべきだろう。たとえば、論文[4]では、控えめな見積もりとして 108 ビットセキュリティ程度であると推定している(表 3.3)。

表 3.3：拡大次数 12 の時の計算量評価([4]から転載)

n	algorithm	(η, κ, λ)	with constants	without constants
12	exTNFS	(4, 3, -)	2^{138}	2^{116}
	SexTNFS	(6, 2, 4)	2^{155}	2^{108}

ただし、これはあくまで漸近的な計算量に基づいた理論的解析であり、計算実験による計算量

解析はまだ行われていない。実際に安全性にどれだけ影響を与えるか，ビットセキュリティの実際の値はどうなるかを問うためには更なる検証が必要である。

参考文献

[1] T. Kim and R. Barbulescu：Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case, CRYPTO 2016, LNCS 9814, pp.543-571, 2016. (IACR Cryptology ePrint Archive: Report 2015/1027.)

[2] A. Kato, M. Scott, T. Kobayashi and Y. Kawahara：Barreto-Naehrig Curves, https://tools.ietf.org/html/draft-kasamatsu-bncurves-02. (Expires: September 19, 2016)

[3] J. Bos, C. Costello and A. Miele “Elliptic and Hyperelliptic Curves: a Practical Security Analysis”, PKC 2014, LNCS 8383, pp.203-220, 2014. (IACR Cryptology ePrint Archive: Report 2013/644.)

[4] A. Menezes, P. Sarkar and S. Singh：Challenges with Assessing the Impact of NFS Advances on the Security of Pairing-based Cryptography, IACR Cryptology ePrint Archive: Report 2016/1102.

[5]. R. Barbulescu, P. Gaudry and T. Kleinjung：The tower number field sieve, ASIACRYPT 2015. LNCS, vol. 9453, pp. 31-55. Springer, Heidelberg (2015).

[6]. O. Schirokauer：Using number fields to compute logarithms in finite fields. Math. Comput. 69(231), 1267-1283 (2000)

[7]. A. Joux, R. Lercier, N. P. Smart and F. Vercauteren：The number field sieve in the medium prime case, CRYPTO 2006. LNCS, vol. 4117, pp.326-344. Springer, Heidelberg (2006)

[8]. R. Barbulescu, P. Gaudry, A. Guillevic and F. Morain：Improving NFS for the discrete logarithm problem in non-prime finite fields, EUROCRYPT 2015. LNCS, vol. 9056, pp. 129-155. Springer, Heidelberg (2015)

[9]. P. Sarkar and S. Singh：New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields, EUROCRYPT 2016. LNCS, vol. 9665, pp. 429-458. Springer, Heidelberg (2016).

[10]. A. Joux and C. Pierrot：The special number field sieve in Fp^n, Pairing 2013. LNCS, vol. 8365, pp. 45-61. Springer, Heidelberg (2014)

(5) Post-Quantum Cryptography の動向について

NIST は、Post-Quantum Cryptography に関するアルゴリズムの公募を 2016 年 12 月 20 日から正式に開始した。公募に関する詳細は Web 上[8]で公開されている。公募の〆切は、2017 年 11 月 30 日である。また、下記の通り、PQCrypto 開催後に、応募者のプレゼンテーションがある予定である。

- PQCrypto 2018： Florida, 9--11 April 2018.
- NIST workshop： 12--13 April 2018.

(6) 今後の課題について

- Post-Quantum Cryptography に関する技術動向を今後どのように把握していくべきかの検討が必要である。
- 一般数体篩法に関するふるい処理に関するデータは更新が必要である。
- DLP 768 ビットの求解記録に関する注意喚起が必要である。
- SHA-1 の移行問題に観られるように社会基盤に組み込まれた暗号アルゴリズムの移行には、非常に時間がかかる。また、暗号アルゴリズムの評価を行い、暗号アルゴリズムをいつまで利用できるかを検討する際、暗号鍵のライフサイクルを考慮する必要がある。ルート認証局は、すでに RSA2048bit からの移行が始まっているが、これは、20 年以上の有効期限が必要なためである。従来、CRYPTREC では 10 年間は大丈夫としているが、10 年では足りない。社会基盤に組み込まれる暗号技術の観点からは、もっと長期のロードマップに基づいた評価が必要になる。

[8] http://www.nist.gov/pqcrypto

付録 A.1　楕円曲線上の離散対数問題(ECDLP)の困難性に関する調査

［レポートの概要］

楕円曲線上の離散対数問題(ECDLP)の困難性は楕円曲線暗号やペアリング暗号の安全性の基盤となっている（図 3.1)。今のところ ECDLP を最も効率よく解くアルゴリズムは ρ 法であり、その計算量は群の位数に関して指数時間である。そして ρ 法の計算量およびそれを用いた計算機実験の結果から安全な鍵長が見積もられている。なお、計算機実験では現時点では約 110 ビット長以上の ECDLP が解かれている。

近年、ECDLP に関する指数計算法の研究が進められている。当該指数計算法では、多変数連立代数方程式を生成する過程及びその多変数連立代数方程式を解く過程を通じて、ECDLP を線形方程式を解く問題に帰着させる。前者の過程では、Summation polynomial 及び Weil descent 等の手法が、後者の過程では、グレブナー基底等の手法が用いられる。

標数が 2 の場合に、ECDLP に関する指数計算法の計算量が準指数時間であることを主張する論文[PQ12]が発表されているが、計算量評価において、検証が不十分な仮定(First Fall Degree Assumption(FFDA)など)が導入されていることが問題となっており、仮定の妥当性やρ法の計算効率との比較が課題となっている。

現時点では、理論的にも数値実験的にも FFDA 等の仮定の正当性が十分に立証されておらず、ρ 法を利用した場合に解くことが期待できる十分大きな ECDLP が指数計算法によって解かれたという成果も報告されていない。これらは、多変数連立代数方程式を解くのに要求されるリソースが非常に高いことも障害となっている。従って、現時点では、標数に拠らず、今のところ最も効率が良い ρ 法ベースの安全性評価基準を採用していれば十分であると判断する。ただし、引き続き、当該指数計算法の研究動向を把握しておく必要がある。

なお、当該調査では、ECDLP に関する指数計算法の文献に現れる実験データを整理することも目的の一つであった。しかし、整理できるほど十分な量の実験データは存在しなかった。即ち、文献で扱われる実験例は連立代数方程式に関するものが多く、指数計算法によって ECDLP を解いた実験例は少なく、解かれた ECDLP のビット長も十分大きくないものであった。

［レポートの構成］

・1 節：はじめに
・2 節：楕円曲線上の離散対数問題（ECDLP）
  - DLP 及び ECDLP の定義
・3 節：Generic algorithm による DLP の計算

- ρ 法の説明及び ρ 法による ECDLP の世界記録(表 3.4)

表 3.4：ρ 法による ECDLP の世界記録

曲線の種類	サイズ(bit)	年	著者
素体	112	2009	Bos et al.
標数 2 の拡大体	118	2016	Bernstein et al.
Koblitz	113	2014	Wenger and Wolfger

・4 節：ECDLP に関する指数計算法

- 指数計算法の説明（ECDLP を線型方程式に変換）
- ECDLP に関する指数計算法の説明
  - 線型方程式を生成するために、Summation polynomial と Weil descent を利用して連立代数方程式生成する。
  - F_4-style のアルゴリズムと FGLM を利用して連立代数方程式を解き、その解から線型方程式を生成する。
  - 線型方程式を解くことで ECDLP の解がえられる。

$E(F_q^n)$ 上の ECDLP に関する指数計算法の計算量の評価

$$O(2^{m^2} + q^{n'} m!\, C_{dcmp} + q^{n'} \omega)$$

m: Summation polynomial のパラメータ、

n’ m≒n、$2 < \omega \leqq 3$、

C_{dcmp}: 連立代数方程式を解くために必要な計算量（この段階では未知数として扱う）

・5 節：有限体における連立代数方程式の解法

- 多項式集合 F で与えられる連立代数方程式を解く手順：
  - F_4-style のアルゴリズムを用いて、F の全次数逆辞書式順序のグレブナー基底 G_{DRL} を計算する。
  - FGLM を用いて G_{DRL} を辞書式順序のグレブナー基底 G_{LEX} へ変換する。
  - G_{LEX} に含まれる一変数方程式の解を求め、それを G_{LEX} の他の多項式に代入する。この計算を繰り返すことで F の解を得る.
- F_4-style のアルゴリズムの概要
  - d 次のグレブナー基底の計算に必要な S 多項式及び簡約に利用する多項式の係数を行成分とする行列 M(d) を生成する。(M(d) は d 次の Macaulay 行列の部分行列)
  - M(d) に対して行簡約を行い、d 次のグレブナー基底を生成する。
  - 上記の計算をグレブナー基底の計算が終わるまで繰り返す。(最大の d を D_{reg} であらわす。)

- F_4-style のアルゴリズムの計算量とその評価の課題
  - $O((m+D_{reg})^{D_{reg}\omega})$。
    但し、m は変数の個数、$2<\omega \leqq 3$ とする。また、この評価は最悪計算量にあたる。
  - D_{reg} の評価は難しいため、仮定（First Fall Degree Assumption (FFDA) など）を導入する場合がある。
- F_4-style とその使用メモリ量
  - F_4-style では Macaulay 行列の部分行列に対して行簡約を行う。従って、行列が素行列であっても簡約が進むにつれて一般的に非零成分が増加し、最終的に多くのメモリを必要とする傾向がある。特に、変数の個数と D_{reg} の増加に伴い膨大なメモリを必要とする。

・6 節：ECDLP に関する指数計算法及び研究動向

- First fall degree D_{first}：(簡単に言うと）グレブナー基底の計算で生じる多項式簡約で、簡約前の多項式 f より次数の小さい多項式が発生するときの、最小の f の次数。
- FFDA: D_{first} は D_{reg} にほぼ等しい。
- Petit と Quisquater は、$E(F_{2^n})$の場合で Summation polynomial S_m と Weil descent を利用して生成した連立代数方程式に対して $D_{first} \fallingdotseq O(m^2)$と見積もっている[FP12]。この場合、全体の計算量はある定数 C に対して以下で与えられる：

$$O\left(2^{Cn^{\frac{2}{3}}\log n}\right).$$

- FFDA の妥当性
  - 連立代数方程式によっては、FFDA が成り立つ例も成り立たない例も存在する (6.1.2 節)。
  - ECDLP で Summation polynomial と Weil descent を利用した場合、理論的には FFDA が成り立つことも成り立たないことも立証されていない。実験的には $E(F_{2^n})$ で $n \leqq 40$ くらいまでで検証されている。

・7 節：まとめ

- $E(F_{2^n})$上の ECDLP に関する指数計算法で、その計算量が準指数時間になることを主張している文献がいくつか存在する。しかし FFDA など、それらの文献で利用している仮定の正当性は必ずしも保証されていない。
- ECDLP に関する指数計算法とρ法の比較で重要なのは、[GG16] でも述べられているように、現時点で実際にどれくらいの大きさの ECDLP が解かれているかである。
- ρ法で 110 bit 以上の大きさの ECDLP が解かれているのに対して、指数計算法では限られた小さな ECDLP しか解かれていない。

- 以上の理由から、ECDLP に関する指数計算法よりρ法の方が計算効率が優れていると判断する。
- 但し、ECDLP に関する指数計算法に関する研究の動向を今後も見ていく必要がある。

参考文献 ：

[FPPR12] J.-C. Faugère, L. Perret, C. Petit and G. Renault. Improving the complexity of index calculus algorithms in elliptic curves over binary fields. In EUROCRYPT 2012, Proceedings, pp. 27-44, 2012.

[GG16] S. D. Galbraith and P. Gaudry. Recent progress on the elliptic curve discrete logarithm problem. Des. Codes Cryptography, Vol. 78, No. 1, pp. 51-72, 2016.

[PQ12] C. Petit and J.J. Quisquater. On polynomial systems arising from a Weil descent. In ASIACRYPT 2012, Proceedings, pp. 451-466, 2012.

付録 A.2　多重線形写像(multi-linear map)及び難読化(Obfuscation)の最新動向に関する調査

［レポートの概要］

・構成

本レポートは、エクゼクティブサマリ、 1 章 序章、2 章 定義及び構成、3 章 既知の攻撃の紹介、4 章まとめ及び今後の展望となっている。本レポートは、現時点での主要結果を俯瞰したものであり、新しい定義・構成方法・主たるアプリケーション・提案方式に対する攻撃方法・安全性に対する議論等について言及している。なお、このレポートは、2017 年 1 月時点の情報に基づいている。

・要旨

- 多重線形写像には、主たる提案が 3 つある。最初の提案は、Garg, Gentry, Halevi らによるもので、次数付き擬暗号化方式 (Graded Encoding Scheme) を用いた構成(GGH13) [GGH13a] である。これに続いて、 Coron, Lepoint, Tibouchi らにより、整数上で動作する構成 (CLT13) [CLT13a] が提案された。さらに、Gentry, Gorbunov, Halevi らにより、グラフ誘導擬暗号化方式 (Graph-induced Encoding Scheme) を用いた構成 (GGH15) [GGH15] が提案された。 (Section 2.4.1, Section 2.4.2, Section 2.4.3, Section 2.5)
- 多重線形写像の構成については、解法困難と仮定される問題への帰着などの安全性証明は示されていない。(Section 1.3)
- 多重線形写像の重要なアプリケーションである Diffie-Hellman 多重鍵交換プロトコルについては、それぞれの多重線形写像に基づく方式について、多項式時間で実行可能な攻撃方法が存在する。さらに、知識型暗号方式 (Witness Encryption)や識別型難読化方式 (Indistinguishability Obfuscation) 等の存在証明に用いられている安全性仮定の多くが成立しないことが明らかとなっている。(Section 3)
- これらの状況は、必ずしも具体的な構成に対する攻撃につながるものばかりではない。実際、GGH13・CLT13・GGH15 のそれぞれの多重線形写像に基づいた、具体的攻撃は知られていない識別型難読化方式の構成は存在する。(Section 4.1)
- 理論的に、PRF などが存在する仮定の下では、識別型難読化方式 と関数型暗号 (Functional Encryption) とが、本質的に等価であることが知られている。このことは、十分大きな n に対する n 重線形写像の存在可能性を意味する。このことから、識別型難読化方式 や関数型暗号を構成する手法を応用した安全な多重線形写像の構成可能性が期待できる。しかし、現時点では具体的な構成は見つかってはいない。(Section 1.4)
- 5 重線形写像 が存在すれば、それを基に識別型難読化方式 が構成可能であることも近年示

されている。しかし、双線形写像から 5 重線形写像への拡張方法は現在知られていない。(Section 2.3.2, Section 4.2)

- 効率性については、今後の課題の一つとなっている。(Section 4.1)

参考文献 :

[GGH13a] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, EUROCRYPT 2013, volume 7881 of LNCS, pages 1-17, Athens, Greece, May 26-30, 2013. Springer, Heidelberg, Germany.

[CLT13a] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In Ran Canetti and Juan A. Garay, editors, CRYPTO 2013, Part I, volume 8042 of LNCS, pages 476-493, Santa Barbara, CA, USA, August 18-22, 2013. Springer, Heidelberg, Germany.

[GGH15] Craig Gentry, Sergey Gorbunov, and Shai Halevi. Graph-induced multilinear maps from lattices. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, TCC 2015, Part II, volume 9015 of LNCS, pages 498-527, Warsaw, Poland, March 23-25, 2015. Springer, Heidelberg, Germany.

付録 A.3　予測図の更新(素因数分解問題及び楕円曲線上の離散対数問題の困難性)

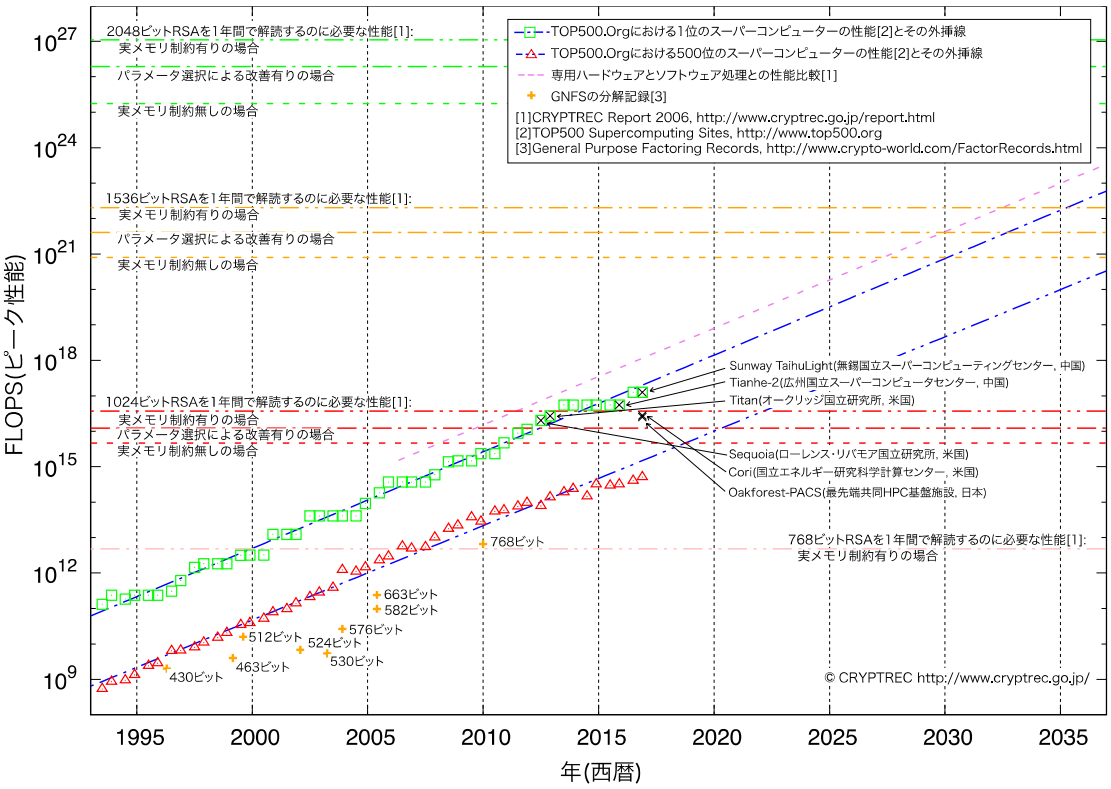


図 3.3：1 年間でふるい処理を完了するのに要求される処理能力の予測
(2017 年 2 月更新)[9]

[9] スーパーコンピューターの性能の伸びに関する外挿線は僅かではあるが鈍化してきている。

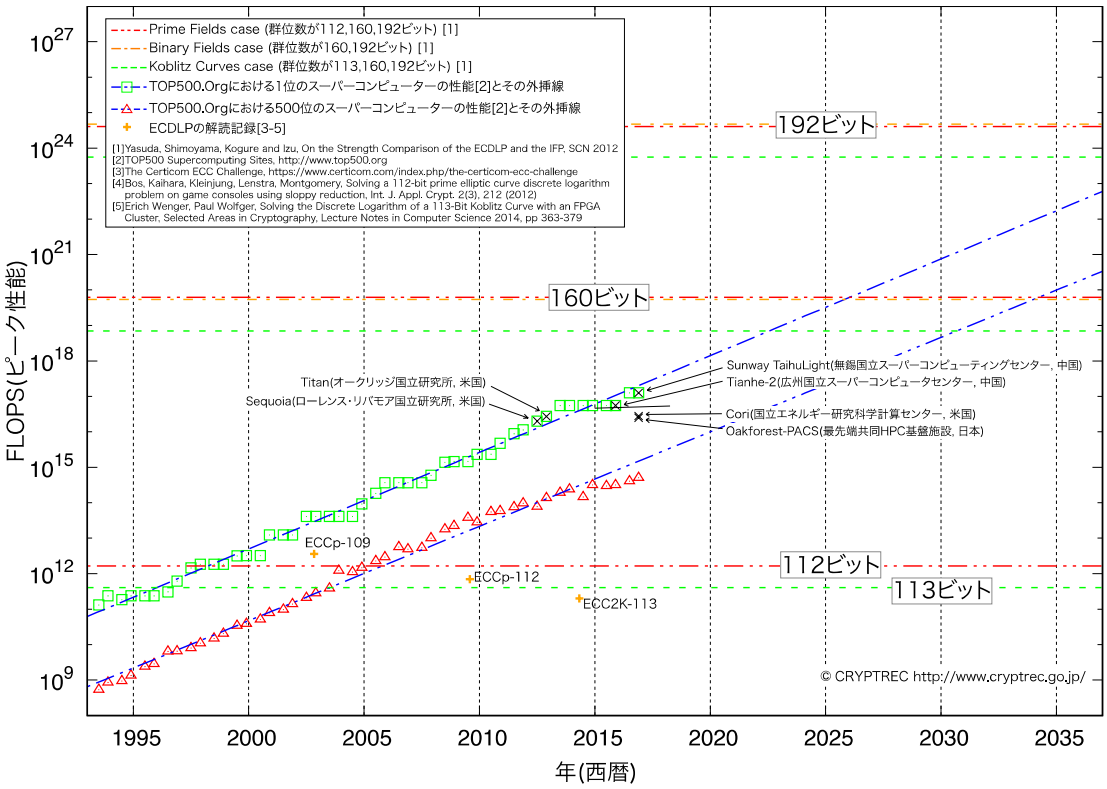


図 3.4： ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測
(2017 年 2 月更新)[10]

[10] スーパーコンピューターの性能の伸びに関する外挿線は僅かではあるが鈍化してきている。

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一般のシステムにおいて、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活動を行う。

2015 年度から、軽量暗号を選択・利用する際の技術的判断に資する、今後の利用促進をはかることを目的とした「暗号技術ガイドライン（軽量暗号)」を発行するために、2 年かけて詳細評価を行う。

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	日本電信電話株式会社
委員：	岩田　哲	名古屋大学
委員：	小川　一人	日本放送協会
委員：	小熊　寿	株式会社トヨタIT開発センター
委員：	﨑山　一男	電気通信大学
委員：	渋谷　香士	ソニーグローバルマニュファクチャリング＆オペレーションズ株式会社
委員：	鈴木　大輔	三菱電機株式会社
委員：	成吉　雄一郎	ルネサスエレクトロニクス株式会社
委員：	峯松　一彦	日本電気株式会社
委員：	三宅　秀享	株式会社東芝
委員：	渡辺　大	株式会社日立製作所

3.2.3. 活動概要

2015 年度に、ガイドラインの作成方針を決定し、ガイドラインに記載する軽量暗号アルゴリズムを選択し、実装詳細評価方針を決定し、軽量暗号 WG 活動の対外的アピールのあり方に関する検討をした。

2016 年度は、2015 年度の検討結果に基づき、実際に「暗号技術ガイドライン（軽量暗号)」の日本語版・英語版の執筆を行った。ガイドライン執筆に併せて、実装詳細評価を行った。スケジュールは図 3.5 のとおり。

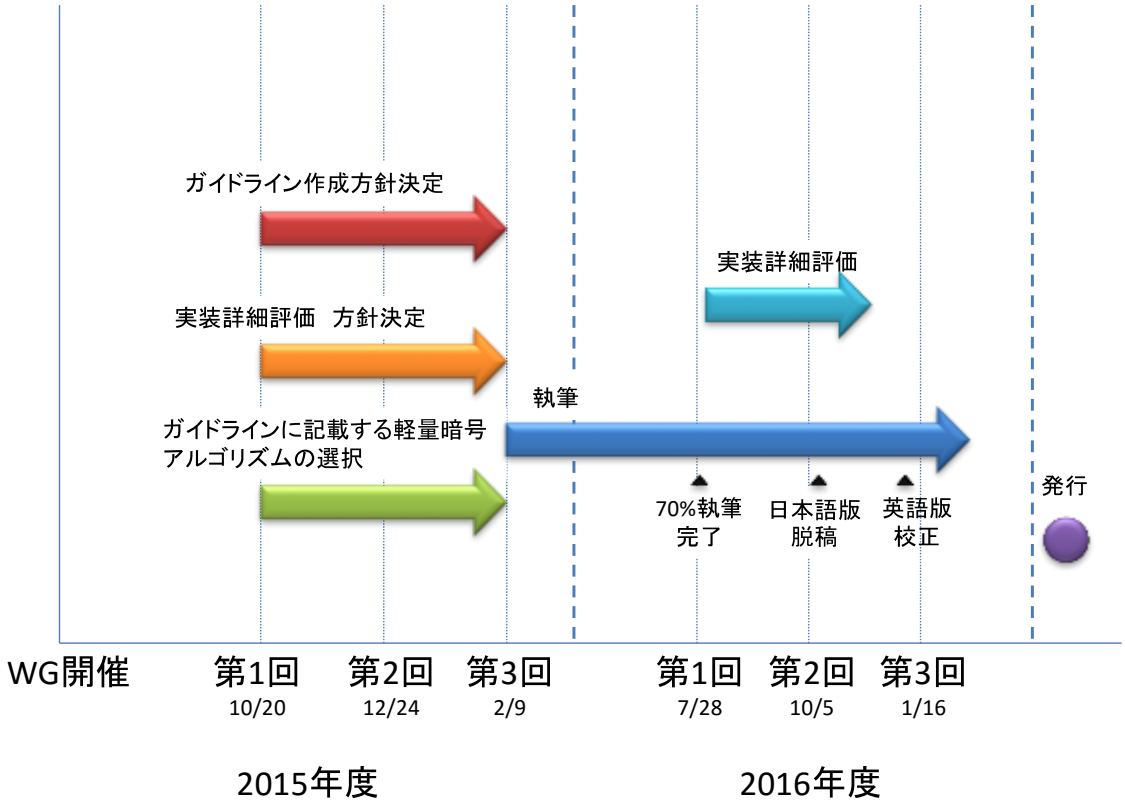


図 3.5：暗号技術ガイドライン（軽量暗号）作成スケジュール

3.2.4. 成果概要

「暗号技術ガイドライン（軽量暗号)」の目次を参考ため掲げておく(表 3.5)。詳しくは、「暗号技術ガイドライン（軽量暗号)」の日本語版[11]・英語版[12]を参照のこと。

表 3.5：「暗号技術ガイドライン（軽量暗号)」　目次

第 1 章　はじめに

第 2 章　軽量暗号とその活用法

2.1　軽量暗号とは

回路規模

消費電力量

レイテンシ

メモリサイズ

2.2　軽量暗号はどこに使えるのか

2.2.1　家電・スマートテレビ

2.2.2　RFID タグ利用のアプリケーション（物流管理等）

[11] http://www.cryptrec.go.jp/report/cryptrec-gl-0001-2016-j.pdf
[12] http://www.cryptrec.go.jp/report/cryptrec-gl-0001-2016-e.pdf

2.2.3　センサーを利用したスマート農業
2.2.4　医療
2.2.5　産業用システム
2.2.6　自動車
2.3　どんな軽量暗号、パラメータを選べばいいか
2.3.1　一般的方針
2.3.2　鍵長の選択
2.3.3　ブロック長の選択
2.3.4　処理データ量と鍵更新、その他の対策
2.3.5　利用シナリオ
2.3.6　その他の留意点
2.3.7　CRYPTREC 暗号リストの暗号との違い
2.4　軽量暗号活用例と効果
2.4.1　家電・スマートテレビ
2.4.2　RFID タグ利用のアプリケーション（物流管理等）
2.4.3　センサーを利用したスマート農業
2.4.4　医療
2.4.5　産業用システム
2.4.6　自動車
第 3 章　軽量暗号の性能比較
3.1 ブロック暗号
3.1.1　ハードウェア実装評価
3.1.1.1　性能比較
3.1.1.2　評価方法の概要
3.1.2　ソフトウェア実装評価
3.1.2.1　性能評価
AES、Camellia、CLEFIA、TDES、LED、PRINCE、
PRESENT、Piccolo、TWINE、SIMON、SPECK、Midori
3.1.2.2　性能比較
メモリサイズを限定した実装（暗号化のみ）
メモリサイズを限定した実装（暗号化・復号）
メモリサイズを限定した実装（まとめ）
高速実装
最小実装
その他の考察
3.1.2.3　評価方法の概要

組み込みマイコン RL78 と評価環境
実装条件
3.2 認証暗号
3.2.1 ソフトウェア実装評価
3.2.1.1 性能比較
認証暗号の実装評価結果
3.2.1.2 評価方法の概要
コーディングの方針とインターフェース仕様
AES-GCM、CLOC、SILC、Minalpher、AES-OTR、Ketje、
ACORN、AES-OCB、JAMBU、Ascon
第 4 章 代表的な軽量暗号
4.1 ブロック暗号
4.2 ストリーム暗号
4.3 ハッシュ関数
4.4 メッセージ認証コード
4.5 認証暗号

付録１

CRYPTREC-LS-0001-2016

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		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
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。

（注12） ハッシュ長は 256 ビット以上とすること。

[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） 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。

[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。

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 3月27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。
平成28年 3月29日	推奨候補暗号リスト（技術分類：ハッシュ関数）	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)
	(注12)	[新規追加]	ハッシュ長は256ビット以上とすること。
平成29年 3月30日	推奨候補暗号リスト（技術分類：ハッシュ関数）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128(注12) SHAKE256(注12)

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://www.fujitsu.com/jp/group/labs/resources/tech/external-activities/crypto/ 英文：http://www.fujitsu.com/jp/group/labs/en/resources/tech/external-activities/crypto/ ・参照 URL ・SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) <http://www.secg.org/SEC1-Ver-1.0.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：fj-soft-crypto-ml@dl.jp.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 パートナー営業部 インサイド セールス チーム　左、高石 TEL：03-6830-3341, FAX：03-5308-8979 E-MAIL：Hanae.Hidari@rsa.com, Hiromi.Takaishi@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 パートナー営業部 インサイド セールス チーム　左、高石 TEL：03-6830-3341, FAX：03-5308-8979 E-MAIL：Hanae.Hidari@rsa.com, Hiromi.Takaishi@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 インサイド　セールスチーム　左、高石 TEL：03-6830-3341, FAX：03-5308-8979 E-MAIL：Hanae.Hidari@rsa.com, Hiromi.Takaishi@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 2 (May 2013), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography 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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.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://www.fujitsu.com/jp/group/labs/resources/tech/external-activities/crypto/ 英文：http://www.fujitsu.com/jp/group/labs/en/resources/tech/external-activities/crypto/ ・参照 URL ・SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) 〈http://www.secg.org/SEC1-Ver-1.0.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：fj-soft-crypto-ml@dl.jp.fujitsu.com
関連情報 2	仕様 ・NIST Special Publication SP 800-56A Revision 2(May 2013), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography において、C(2e,0s,ECC CDH)として規定されたもの。 ・参照 URL <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.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://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.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://nvlpubs.nist.gov/nistpubs/FIPS/NIST.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.kddi-research.jp/products/kcipher2.html 英文：http://www.kddi-research.jp/english/products/kcipher2.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 総合研究所　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@kddi-research.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://nvlpubs.nist.gov/nistpubs/FIPS/NIST.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	仕様 ・NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation Methods and Techniques ・ 参照 URL <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.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	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://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.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://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf>

6. メッセージ認証コード

暗号名	CMAC
関連情報	仕様 ・NIST FIPS SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005.(Updated Oct. 2016) ・ 参照 URL <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf>

暗号名	HMAC
関連情報	仕様 ・NIST FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008. ・ 参照 URL <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.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 signature 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/sdk/cipherunicorn-e.html 英文：http://www.nec.co.jp/cced/SecureWare/sdk/cipherunicorn-e-en.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　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 電子政府推奨暗号 問い合わせ窓口 E-MAIL: rdc-crypt-info@ml.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	〒247-8520 神奈川県鎌倉市上町屋 325 番地 三菱電機株式会社 インフォメーションシステム統括事業部 トータルソリューションシステム第一部 システム第三課　坂上 勉 TEL：0467-41-3560 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/sdk/cipherunicorn-a.html 英文： http://www.nec.co.jp/cced/SecureWare/sdk/cipherunicorn-a-en.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　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：https://www.sony.co.jp/Products/cryptography/clefia/ 英文：https://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 電子政府推奨暗号 問い合わせ窓口 E-MAIL: rdc-crypt-info@ml.toshiba.co.jp

暗号名	SC2000
関連情報	公開ホームページ 和文：http://www.fujitsu.com/jp/group/labs/resources/tech/external-activities/crypto/ 英文：http://www.fujitsu.com/jp/group/labs/en/resources/tech/external-activities/crypto/
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： fj-soft-crypto-ml@dl.jp.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	〒140-8572 東京都品川区南大井 6-27-18 株式会社日立製作所 セキュリティ事業統括本部 セキュリティ先端技術本部 HIRT センタ 主任技師 栗田 博司 TEL：044-555-0894(ダイヤルイン), FAX ： 03-5471-4677 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：050-3135-2017, FAX：050-3135-3392 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	〒140-8572 東京都品川区南大井 6-27-18 株式会社日立製作所 セキュリティ事業統括本部 セキュリティ先端技術本部 HIRT センタ 主任技師 栗田 博司 TEL：044-555-0894(ダイヤルイン), FAX ： 03-5471-4677 E-MAIL：hiroshi.kurita.wp@hitachi.com

3. ハッシュ関数

暗号名	**SHA-512/256**
関連情報	仕様 ・FIPS PUB 180-4, Secure Hash Standard (SHS) ・参照 URL 〈http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf〉

暗号名	**SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256**
関連情報	仕様 ・FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions ・参照 URL <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>

4. 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　セキュリティ研究所　主任研究員 峯松 一彦 TEL：044-431-7686, FAX：044-431-7680 E-MAIL: k-minematsu@ah.jp.nec.com

5. 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 パートナー営業部 インサイド セールス チーム 左、高石 TEL：03-6830-3341, FAX：03-5308-8979 E-MAIL：Hanae.Hidari@rsa.com, Hiromi.Takaishi@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 180-4, Secure Hash Standard (SHS) ・参照 URL〈http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.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。

楕円曲線上の離散対数問題に関する指数計算法

篠原 直行[†] 野呂 正行[‡] 横山 和弘[‡]

[†]NICT [‡]立教大学

概 要

楕円曲線暗号は現在, 実際に使用されている代表的な公開鍵暗号方式である. また, 実用化が進められている公開鍵暗号方式としてペアリング暗号が挙げられ, ペアリング暗号を基盤技術として様々な高度な暗号技術を利用できることが知られている. これらの公開鍵暗号方式は有限体上の楕円曲線を利用しており, その楕円曲線において与えられる離散対数問題 (ECDLP) が解かれると解読されてしまう.

ECDLP だけではなく一般的に, 有限巡回群上の離散対数問題 (DLP) を解くアルゴリズムとして指数計算法がある. 例えば, 有限体上の DLP を効率良く解く指数計算法として数体篩法や関数体篩法などが挙げられる. 近年, summation polynomial やグレブナー基底などを利用して, ECDLP に対して有効な指数計算法を構築する研究が進められている.

本稿では, 楕円曲線暗号やペアリング暗号に対するこれらの新たな攻撃方法を紹介し, それらの影響について述べる. また, 現時点ではこれらの新たな攻撃方法より, Pollard の ρ 法等の既存の攻撃方法の方が計算効率が良いと結論づける. しかし, ECDLP に関する指数計算法の研究の動向は注視する必要がある.

1 はじめに

楕円曲線暗号は現時点で広く使用されている代表的な公開鍵暗号方式の一つであり, 楕円曲線暗号で利用する楕円曲線において与えられる離散対数問題 (ECDLP) が解かれると解読されてしまう. また, 高度な暗号技術を実現するための基盤技術として, ペアリング暗号とよばれる公開鍵暗号方式があり, その実用化に向けて研究が進められている. ペアリング暗号は, 有限体上の離散対数問題 (DLP) と ECDLP の双方を解く計算の困難性をその安全性の基盤としている. 従ってこれらの暗号の安全性を維持する上で, ECDLP は重要な研究課題である.

DLP を解くアルゴリズムは群の固有の性質を利用するか否かで大きく二つの方法に分類される. 群の固有の性質に依存しないものは generic algorithm とよばれ, DLP を定義できる任意の有限群に対して適用できる. 代表的な generic algorithm として Shanks の Baby-step-giant-step や, Pollard の ρ

法, λ 法 (kangaroo-algorithm) が挙げられる. DLP が定義されている有限群 G の位数を $\#G$ としたときに, これらのアルゴリズムの計算量は $O(\sqrt{\#G})$ である. 群の固有の性質を利用することで, DLP を解くために必要な計算量を $O(\sqrt{\#G})$ より小さくすることに成功しているアルゴリズムが存在する. 例えば, 標数の大きい有限体上の DLP に対しては数体篩法, 標数の小さい有限体上の DLP に対しては関数体篩法や Frobenius representation discrete logarithm algorithm 等が挙げられる. これらのアルゴリズムは指数計算法とよばれる枠組みに属している.

上記のように指数計算法は有限体上の DLP を解く場合において, それを解く計算コストの削減に成功しているが, ECDLP に対する効率の良い指数計算法の研究はまだ模索の段階にある. これまでは, ECDLP を最も効率よく解く方法は generic algorithm であったことから, 楕円曲線暗号やペアリング暗号で利用する楕円曲線等の暗号パラメータの設定には, generic algorithm の計算量とそれを使用した数値実験の結果が利用されてきた.

近年, ECDLP に対する指数計算法の研究において, Semaev の summation polynomial やグレブナー基底等を利用した新たな指数計算法が多数提案されている. その中には generic algorithm よりも計算効率が良いことを主張する文献が存在し, また一方で逆の主張をする文献も存在している. そのため, generic algorithm との比較を考慮して, これらの新たな指数計算法の効率性を議論する必要が生じている.

この比較について本稿は, generic algorithm よりも効率よく ECDLP を解くアルゴリズムが現時点では提案されていないと結論づける. その理由として以下の二つの事実を挙げる: 一つは, 新たな指数計算法の計算量評価において導入されている仮定 (frist fall degree assumption など) について, それらの仮定の正当性が理論的にも数値実験的にも十分に示されているとは言えないことである [15]. もう一つは適切な暗号パラメータ (十分大きな有限巡回群等) において, 新たな指数計算法の有効性を示す数値実験的な結果が現時点では報告されていないことである.

本稿の構成は以下のとおりである: 第 2 節では楕円曲線や ECDLP の定義など, 基本的な内容を説明する. 第 3 節では generic algorithm 及び ECDLP を解く計算の世界記録を紹介する. 第 4 節では ECDLP に対する基本的な指数計算法について述べ, 第 5 節では, それらのアルゴリズムの計算量を理解する上で必要となる, 連立代数方程式を解くアルゴリズムとその計算量について説明する. 第 6 節で近年の成果について紹介し, 第 7 節で ECDLP に対する新たな指数計算法の影響についてまとめる.

2　楕円曲線上の離散対数問題 (ECDLP)

この節ではまず楕円曲線に関するいくつかの定義及びその性質について紹介する. さらに一般の群上の離散対数問題 (DLP) 及び楕円曲線の有理点のなす群上で与えられる離散対数問題 (ECDLP) について説明する. (参考文献として [5] を挙げる.)

体 K の代数閉包を $\overline{K}$ で表す. 本稿では楕円曲線の以下の定義を採用する:

定義 2.1. K を体として $a_1, a_2, a_3, a_4, a_6 \in K$ とする. このとき等式 E を以下のように定義する:

$$E: \ f(x,y) := y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0.$$

E を満たす任意の $(x_1, y_1) \in \overline{K}^2$ において, $(\partial f/\partial x, \partial f/\partial y) \neq (0,0)$ が成り立つとき, E を K 上の楕円曲線とよぶ[1].

集合 $E(K)$ を次のように定める:

$$E(K) := \{(x,y) \in K^2 : \ f(x,y) = 0\} \cup \{\mathcal{O}\}.$$

(但し, $\mathcal{O}$ は無限遠点とする.) 本稿では特に断りのない限り, $\mathcal{P} \in E(K)$ と書いた場合は $\mathcal{P} \neq \mathcal{O}$ とする. 下記のように演算等を定義することで $E(K)$ は加法群を成す (但し $\mathcal{P}_i := (x_i, y_i) \in E(K)$ とする):

- $\mathcal{O}$ を単位元とする.
- $\mathcal{P}_1$ の逆元を $-\mathcal{P}_1 := (x_1, -y_1 - a_1x_1 - a_3)$ とする.
- $\mathcal{P}_1 \neq -\mathcal{P}_2$ のとき $\mathcal{P}_3 := \mathcal{P}_1 + \mathcal{P}_2$ を以下のように定める:

$$\begin{aligned} \lambda &= \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } x_1 \neq x_2, \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } x_1 = x_2, \end{cases} \\ x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3. \end{aligned}$$

正整数 m に対して m 個の $\mathcal{P} \in E(K)$ の和を $[m]\mathcal{P}$ で表す. さらに $[0]\mathcal{P} := \mathcal{O}$ とし, $[-m]\mathcal{P} := -[m]\mathcal{P}$ とする. 体 K が有限体であるとき, 即ちある素数べき q に対して $K = \mathbb{F}_{q^n}$ であるとき, $E(\mathbb{F}_{q^n})$ は有限群である. 従って $\mathcal{P} \in E(\mathbb{F}_{q^n})$ を生成元として有限巡回群 $\langle \mathcal{P} \rangle$ を構成できる.

次に離散対数問題 (DLP) について説明する. 群 G の位数を $\#G$ で表す. 有限群 G 上の DLP とは, 与えられた $g, T \in G$ に対して以下の条件を満たす $X \in \mathbb{Z}/\#G\mathbb{Z}$ が存在するならばそれを求める問題である:

$$T = g^X. \tag{1}$$

[1] 特にこの定義の曲線を Weierstrass model とよぶ.

((1) が解 X を持つならば, X を $\log_g T$ とかく.) 有限群 G が $E(\mathbb{F}_{q^n})$ であるとき, その離散対数問題は “楕円曲線上の離散対数問題 (ECDLP) ” とよばれる. この場合, 楕円曲線から与えられる加法群の表記方法に合わせて, 一般的に以下のように ECDLP を表す. 即ち, ECDLP とは $\mathcal{T}, \mathcal{P} \in G$ に対して以下の条件を満たす $X \in \mathbb{Z}/\#G\mathbb{Z}$ が存在するならばそれを計算する問題である:

$$\mathcal{T} = [X]\mathcal{P}. \tag{2}$$

本稿では, “有限体上の離散対数問題[2]” 等の一般的によく使用される呼び方に適した, 上述の DLP の定義を採用した. しかし, 特に暗号の分野では解が存在する DLP について考える理由等から, 一般的には有限群 G は有限巡回群で定義され, 議論される. 例えば (2) で与えられる ECDLP の場合, G は $E(\mathbb{F}_{q^n})$ ではなく巡回群 $\langle \mathcal{P} \rangle$ で考える.

楕円曲線暗号やペアリング暗号は ECDLP が解かれると解読されてしまう. 従ってこれらの暗号を安全に運用するには, ECDLP を解く計算に十分な計算時間が必要となるように適切な有限体 $\mathbb{F}_{q^n}$, 曲線 E, 及び巡回群 $\langle \mathcal{P} \rangle$ 等を選択する必要がある. その選択の例として, DLP を与える巡回群 G の位数 $\#G$ を十分大きな素数にすることや, $E(\mathbb{F}_{2^n})$ 上での ECDLP を利用する場合は n は素数となるように選ぶことなどが挙げられる. (参考文献として [15] を挙げる.) 以降の節で ECDLP を解くアルゴリズムについて説明していく.

3 Generic algorithm による DLP の計算

この節では任意の有限群上で定義されている DLP を解くことに適用可能なアルゴリズムである generic algorithm について説明する. また, その代表的なアルゴリズムである Shanks の baby-step-giant-step [28], Pollard の ρ 法及び λ 法 [25] について簡単に述べる. これらのアルゴリズムの計算量は, 与えらた有限群を G としたときに, 大まかには $O(\sqrt{\#G})$ であることが知られている[3].

3.1 Generic algorithm

本稿では [5] の定義 19.1 に基づいた以下の generic algorithm アルゴリズムの定義を採用する:

定義 3.1. 有限群 G が与えられているとして, G における以下の演算のみを行うアルゴリズムを generic algorithm とよぶ:

- 二項演算,

[2]有限体 $\mathbb{F}_{q^n}$ 上の DLP とは, 乗法群 $G = \mathbb{F}_{q^n}^*$ 上の DLP のことである.
[3]Shanks の baby-step-giant-step の計算量は正確には $O(\sqrt{\#G}\log \#G)$ である.

- 逆元の演算,
- 二つの元が等しいか否かの確認.

Generic algorithm では, 与えらえた有限群が固有の性質[4]を持っていたとしても, それを利用した計算が行われない.

3.2 Shanks の baby-step-giant-step

Shanks の baby-step-giant-step [28] について簡単に説明する. 式 (1) で表される, 巡回群 $G = \langle g \rangle$ 上の DLP を解くことを考える. まず $M := \lceil \#G \rceil$ として $h = (g^{-1})^M$ を計算し, 以下のリスト BL, GL を計算する:

$$\begin{aligned} BL &= \{g^i : \ i = 0, \cdots M-1\}, \\ GL &= \{Th^j : \ j = 0, \cdots M-1\}. \end{aligned}$$

(BL の計算は baby-step, GL の計算は giant-step とよばれる.) リスト BL, GL を並べ替え, 重複箇所 $g^i = Th^j$ を探し, $X = i + jM \pmod{\#G}$ を返す. このアルゴリズムは, リストの生成で $O(\sqrt{\#G})$ 回の群演算及び $O(\sqrt{\#G})$ のデータ保存空間を必要とし, さらにリストの並び替えと重複箇所の探索で $O(\sqrt{\#G}\log \#G)$ 回の比較を実行する. このアルゴリズムの様々な改良が提案されているがオーダーとしての計算量は変わらない. (参考文献として [15] を挙げる.)

3.3 Pollard の ρ 法と λ 法

第 3.2 節で紹介した Shanks の baby-step-giant-step は確定的なアルゴリズムであるが多くのデータ保存空間を必要とする. 一方で Pollard の ρ 法や λ 法は birthday paradox を利用する確率的なアルゴリズムである. しかし, データ保存空間は baby-step-giant-step に比べてずっと小さく, 巡回群 G 上の DLP を解くために必要な群演算の回数は $O(\sqrt{\#G})$ である. この節では基本的な ρ 法を説明する [7]. (詳しくは [5], [15] を参照されたい.)

ここでも第 3.2 節と同じ DLP (1) を解くとする. 基本的な ρ 法では, まず巡回群 G を三つのほぼ同じ位数を持つ互いに交わりのない集合 G_1, G_2, G_3 に分割する:

$$G = G_1 \cup G_2 \cup G_3.$$

[4]例えば群の位数が小さな素数の積で表される場合等が挙げられる.

表 1: ECDLP に関する計算の記録

曲線の種類	サイズ (bit)	年	著者
素体	112	2009	Bos et al. [2]
標数 2 の拡大体	118	2016	Bernstein et al. [1]
Koblitz	113	2014	Wenger and Wolfger[29]

次に $(a_i, b_i) \in (\mathbb{Z}/\#G\mathbb{Z})^2$ に対して, $h_i := T^{a_i} g^{b_i} \in G$ なる数列 $\{h_i\}$ を考える. 但し, $a_0 = b_0 = 0, h_0 = e$ (e は G の単位元) とし,

$$(a_{i+1}, b_{i+1}) = \begin{cases} (a_i + 1, b_i) & (h_i \in G_1), \\ (2a_i, 2b_i) & (h_i \in G_2), \\ (a_i, b_i + 1) & (h_i \in G_3) \end{cases}$$

とする. このとき次が成り立つ:

$$h_{i+1} = \begin{cases} Th_i & (h_i \in G_1), \\ h_i^2 & (h_i \in G_2), \\ gh_i & (h_i \in G_3). \end{cases}$$

実際の計算では $(h_i, a_i, b_i, h_{2i}, a_{2i}, b_{2i})$ のみを保持し, $h_i = h_{2i}$ なる i を計算する. このとき $T^{a_i} g^{b_i} = T^{a_{2i}} g^{b_{2i}}$ であることから次が成り立つ:

$$T^{a_i - a_{2i}} = g^{b_{2i} - b_i}.$$

暗号では $\#G$ は十分大きな素数となるように設定されるため, 高い確率で $\gcd(a_i - a_{2i}, \#G) = 1$ が期待できることから,

$$X = (b_{2i} - b_i)(a_i - a_{2i})^{-1} \pmod{\#G}$$

を計算することで解 X が得られる.

ρ 法の計算量について説明する. $\{h_i\}$ がランダムな数列であれば birthday paradox により, $i = O(\sqrt{\#G})$ で $h_i = h_{2i}$ となる確率が 1/2 以上になると期待できる. また, $(h_i, a_i, b_i, h_{2i}, a_{2i}, b_{2i})$ から $(h_{i+1}, a_{i+1}, b_{i+1}, h_{2(i+1)}, a_{2(i+1)}, b_{2(i+1)})$ を計算するには 3 回の群演算を必要とするだけであることから, 合計で $O(\sqrt{\#G})$ 回の群演算を必要とする.

ここで ECDLP に関する近年の代表的な計算の記録を紹介する. 表 1 の結果は ρ 法を改良した generic algorithm によるものである [18]. このことは, 楕円曲線の有理点のなす群が持つ固有の性質を利用して, ECDLP を効率良く解くアルゴリズムがまだ発見されていないことを意味する.

4 ECDLP に関する指数計算法

第 3 節で述べたように, generic algorithm を用いることで, 任意に与えられた有限群 G 上の DLP は $O(\sqrt{\#G})$ 回の群演算, 即ち指数時間で解くことがで

きる. 一方で有限体上の DLP は, 数体篩法や関数体篩法など, 指数計算法とよばれる枠組みに属する方法を使用することで指数時間より小さい計算量, 即ち準指数時間や quasi-polynomial time で解かれることが知られている. (詳しくは [5] [8] を参照.) 近年, 指数計算法を ECDLP に導入した研究が進められている. この節では, 指数計算法について簡単に説明し, それを ECDLP に導入する際に道具として使われる Semaev の summation polynomial と Weil descent について述べる. (参考文献として [15] を挙げる.)

4.1 指数計算法

指数計算法は大きく二つの種類に分けられるため, これら二つの違いについて説明する. 第 4.1.1 節で述べる指数計算法は ECDLP を解く場合によく議論されており, 第 4.1.2 節で紹介する指数計算法は有限体上の DLP を解く場合によく利用されている. 本稿では前者を指数計算法 1, 後者を指数計算法 2 とよぶことにする. また本稿では指数計算法 1 を中心に議論をする.

以下二つの注意を紹介する. 指数計算法は任意の有限群に適用することができるが, 計算効率を上げるために与えられた群が持つ固有の性質を利用するため, 一般的には generic algorithm に分類されない. 第 4.1 節では (1) で表される, 有限巡回群 $G = \langle g \rangle$ 上の DLP が与えられているとする.

4.1.1 指数計算法 1

ECDLP を考える場合によく扱われる指数計算法 1 の概要を以下に与える;

初期設定段階: 因子基底とよばれる G の部分集合 $FB := \{\pi_1, \cdots \pi_s\}$ を設定する.

関係 (relation) 探索段階:

(i) $a, b \in \mathbb{N}$ を選び $R = g^a T^b \in G$ を計算する.

(ii) 下記の等式を満たす非負整数 e_ℓ の組 $(e_1, \cdots, e_s)$ が存在するかを判定し[5], 存在するならばそれを計算する:

$$R = \prod_{\ell=1}^{s} \pi_\ell^{e_\ell}. \tag{3}$$

等式 (3) は relation とよばる. この relation から, 因子基底の元および T の 離散対数を解とする線形方程式

$$a + bX \equiv \sum_{\ell=1}^{s} e_\ell \log_g \pi_\ell \pmod{\#G}$$

[5]一般的に e_ℓ には上界が与えらているため, 常に (3) を満たす $(e_1, \cdots, e_s)$ が存在する保証はない.

が生成される. 実際の計算では (a, b) と $(e_1, \cdots, e_s)$ を結合したベクトルを行列の行 (または列) として保存する.

(iii) (i), (ii) の計算を十分な個数の relation が得られるまで繰り返す.

線形代数段階: 関係探索段階で得られた行列に対して, $\#G$ を法とする行列操作を行うことで以下を満たす X_1, X_2 を計算する:

$$e = g^{X_1} T^{X_2}.$$

(但し e は G の単位元とする.)

離散対数計算段階: $X_2^{-1} \pmod{\#G}$ が存在するならば以下を返す:

$$X = -X_1 X_2^{-1} \pmod{\#G}.$$

上記のように, 指数計算法は四つの計算段階から構成される. 初期設定段階では因子基底を設定するとしているが, 他にも G の表現に使用する数値等 (例えば有限次拡大体を表す多項式など) を設定することもある. この段階に必要な計算コストは一般的に無視できるほど小さい. 従って, 文献によっては初期設定段階を一つの計算段階として数えず, 指数計算法は他の三つの計算段階から構成されていると定義する場合もある.

因子基底の設定は指数計算法の効率を決定する重要な要素である. 以下に因子基底に求められる性質について紹介する:

- 因子基底の個数 s に対して, 線形代数段階で扱われる行列の大きさは $O(s)$ である. よって, この段階での行列操作の計算量は, ある定数 $2 < \omega \leq 3$ に対して $O(s^\omega)$ であるため, 因子基底の個数 s は可能な限り小さいことが望ましい.

- Relation が得られる確率が可能な限り高くなるように因子基底を設定する必要がある. その理由は, この確率が低いと関係探索段階での計算を繰り返す回数が大きくなってしまうことである. 因子基底の個数 s が小さいほどその確率は小さくなる. 従って関係探索段階と線形代数段階の計算コストはトレードオフの関係にある.

- Relation を計算するコストが小さくなるように因子基底を設定する必要がある.

第 4.4 節で説明するように, 指数計算法 1 で ECDLP を解く場合, relation (3) を生成するために有理点 R を因子基底の元である有理点の和で表す計算を効率良く実行する必要がある. この計算を point decomposition とよぶ. 近年では Semaev の summation polynomial (第 4.2 節) に Weil descent (第 4.3) を適用することで連立代数方程式を生成し, それをグレブナー基底を計算するアルゴリズムなどを利用して解くこと (第 5 節) で point decomposition を実行する研究が進められている.

4.1.2 指数計算法 2

有限体上の DLP を解く場合に数体篩法や関数体篩法などおいて, 上述の指数計算法 1 を少し変更した指数計算法 2 の枠組みがよく利用される. 本稿を理解する上でこの節を読み飛ばしても問題ないが, 指数計算法 2 を ECDLP に適用する議論もあるため, この節で簡単に紹介する. その主な変更内容は関係探索段階において, 与えられた DLP を定義する T を含まない relation を生成することと, T を因子基底の元で表す計算を離散対数計算段階に追加することである. 以下に指数計算法 2 の概要を与える;

初期設定段階: 因子基底 $FB := \{\pi_1, \cdots \pi_s\}$ を設定する.

関係探索段階:

(i) 下記の等式を満たす非負整数 e_ℓ の組 $(e_1, \cdots, e_L, e_{L+1}, \cdots e_s)$ が存在するかを判定し, 存在するならばそれを計算する:

$$\prod_{\ell=1}^{L} \pi_\ell^{e_\ell} = \prod_{\ell=L+1}^{s} \pi_\ell^{e_\ell}. \tag{4}$$

この relation は以下の線形方程式に対応する:

$$\sum_{\ell=1}^{L} e_\ell \log_g \pi_\ell \equiv \sum_{\ell=L+1}^{s} e_\ell \log_g \pi_\ell \pmod{\#G}.$$

ベクトル $(e_1, \cdots, e_s)$ を行列の行 (または列) として保存する.

(ii) (i) の計算を十分な個数の relation が得られるまで繰り返す.

線形代数段階: 関係探索段階で得られた線形方程式の解 $\log_g \pi_1, \cdots, \log_g \pi_s$ を求める.

離散対数計算段階: $a, b \in \mathbb{N}$ を選び $R = g^a T^b$ を因子基底の元で表す:

$$R = \prod_{\ell=1}^{s} \pi_\ell^{t_\ell}.$$

このとき $b^{-1} \pmod{\#G}$ が存在するならば

$$X = (\sum_{\ell=1}^{s} t_\ell \log_g \pi_\ell - a) b^{-1} \pmod{\#G}$$

が成り立つことから, 線形代数段階で計算した解を上記の等式に代入することで X を得る.

4.2 Semaev の Summation polynomial

第 4.2 節以降では ECDLP について議論するため, 式 (2) で表される等式について考える. 指数計算法 1 で ECDLP を解く場合, 関係探索段階において選んだ $a, b \in \mathbb{N}$ に対して

$$\mathcal{R} = [a]\mathcal{P} + [b]\mathcal{T} \tag{5}$$

を計算する. 次に $\mathcal{R}$ を因子基底 $FB = \{\pi_1, \cdots, \pi_s\}$ の和

$$\mathcal{R} = \sum_{\ell=1}^{s} [e_\ell]\pi_\ell$$

として表現する計算, 即ち point decomposition を試み, それが可能であれば

$$\log_{\mathcal{P}} \mathcal{R} \equiv \sum_{\ell=1}^{s} [e_\ell] \log_{\mathcal{P}} \pi_\ell \pmod{\#\langle \mathcal{P} \rangle}$$

を得る.

Semaev は, 標数が 2 でも 3 でもない有限体 $\mathbb{F}_{q^n}$ 上の楕円曲線 E が与えられた場合に, point decomposition の計算に使用する道具として summation polynomial を提案した [26]. この場合, E は以下の式で表すことができる:

$$y^2 = x^3 + Ax + B. \tag{6}$$

(但し A, B は $\mathbb{F}_{q^n}$ の元で $\Delta := 4A^3 + 27B^2 \neq 0$ を満たすものとする.)

定理 4.1. q は 5 以上の奇数素数のべきとし, $E: y^2 = x^3 + Ax + B$ は $\mathbb{F}_{q^n}$ 上の 楕円曲線とする. このとき $2 \leq m \in \mathbb{N}$ に対して第 m-summation polynomial S_m を以下のように定義する:

$$\begin{aligned}
S_2(x_1, x_2) &= x_1 - x_2, \\
S_3(x_1, x_2, x_3) &= (x_1 - x_2)^2 x_3^2 - 2((x_1 + x_2)(x_1 x_2 + A) + 2B)x_3 \\
&\quad + (x_1 x_2 - A)^2 - 4B(x_1 + x_2), \\
S_m(x_1, \cdots, x_m) &= \mathrm{Res}_x(S_{m-M}(x_1, \cdots, x_{m-M-1}, x), S_{M+2}(x_{m-M}, \cdots, x_m, x)) \\
&\quad (\text{if } m \geq 4, 1 \leq M \leq m-3).
\end{aligned}$$

ただし, Res は終結式とする [4]. $m \geq 3$ のとき, S_m は絶対既約で対称な多項式であり, さらに各変数 x_i に対して $\deg_{x_i}(S_m) = 2^{m-2}$ である.

Summation polynomial S_m は標数が 2 または 3 の場合にも自然に拡張できる [14] [15] [26].

ここで point decomposition に利用する S_m の性質を紹介する: 即ち $\overline{x_1}, \cdots, \overline{x_m} \in \overline{\mathbb{F}_{q^n}}$ が

$$S_m(\overline{x_1}, \cdots, \overline{x_m}) = 0 \tag{7}$$

を満たすことと,

$$\mathcal{P}_1 + \cdots + \mathcal{P}_m = \mathcal{O}$$

なる $\mathcal{P}_i = (\overline{x_i}, \overline{y_i}) \in E(\overline{\mathbb{F}_{q^n}})$ が存在することは同値である. この S_m の性質を利用して, 関係探索段階で与えられた (5) の $\mathcal{R}$ を因子基底 $FB = \{\pi_1, \cdots, \pi_s\}$ の元の和で

$$\mathcal{R} = \pi_{\ell_1} + \cdots + \pi_{\ell_m} \tag{8}$$

のように表すことを考える. まず $\mathcal{Q} := (x, y) \in E(\overline{\mathbb{F}_{q^n}})$ の x 座標を以下のように表記する:

$$x(\mathcal{Q}) := x.$$

S_{m+1} の x_{m+1} に $x(\mathcal{R})$ を代入した等式

$$S_{m+1}(x_1, \cdots, x_m, x(\mathcal{R})) = 0 \tag{9}$$

を解くことを試みたとして, その解 $(\overline{x_1}, \cdots, \overline{x_m}) \in (\mathbb{F}_{q^n})^m$ が存在したとする[6]. このとき, 各 $\overline{x_i}$ に対して $\overline{x_i} = x(\pi_{\ell_i})$ なる $\pi_{\ell_i} \in FB$ が存在するならば relation が得られる[7].

代数方程式 (9) を効率良く解くために, Frobenius 写像を利用した等式と (9) から構成される下記の連立代数方程式を解く方法が考えられる:

$$\begin{cases} 0 = S_{m+1}(x_1, \cdots, x_m, x(\mathcal{R})), \\ 0 = x_1^{q^n} - x_1, \\ \vdots \\ 0 = x_m^{q^n} - x_m. \end{cases} \tag{10}$$

次の第 4.3 節では連立代数方程式 (10) を解くために Weil descent を導入した方法について説明する. またグレブナー基底を利用した連立代数方程式の解法については第 5 節で説明する.

4.3 Weil descent

Semaev によって導入された summation polynomial を利用して ECDLP を解く指数計算法は, Weil descent を導入することによって, Diem や Gaudry らによって改良されていった [9] [16]. この節では Weil descent を紹介し, それを連立代数方程式 (10) を解くためにどのように利用するかを説明する.

まず Weil descent に関する以下の補題を紹介する [15]:

[6]存在しない場合は relation が得られないため, $\mathcal{R}$ をとりなおして同様の計算を行うことになる.

[7]この場合も relation が得られないため, $\mathcal{R}$ をとりなおして同様の計算を行うことになる.

補題 4.2. 素数べき q と自然数 n に対して, $\mathbb{F}_{q^n}$ を n 次元の $\mathbb{F}_q$ ベクトル空間としてみたときの基底を $\{\theta_1, ..., \theta_n\}$ とする. さらに $f(x_1, ..., x_m) \in \mathbb{F}_{q^n}[x_1, ..., x_m]$ とする. このとき $Z := \{z_{i,j} : 1 \leq i \leq m,\ 1 \leq j \leq n\}$ に対して, 以下の等式を満たす $f_k(Z) \in \mathbb{F}_q[Z]$ がただ一つ存在する:

$$f(z_{1,1}\theta_1 + \cdots + z_{1,n}\theta_n, \cdots, z_{m,1}\theta_1 + \cdots + z_{m,n}\theta_n) = \sum_{k=1}^{n} \theta_k f_k(Z).$$

さらに, ある $(\overline{x_1}, \cdots, \overline{x_m}) \in (\mathbb{F}_{q^n})^m$ に対して $f(\overline{x_1}, \cdots, \overline{x_m}) = 0$ であるならば, ある $\overline{z_{i,j}} \in \mathbb{F}_q$ が存在して以下の条件を満たす:

$$\begin{aligned} \overline{x_i} &= \sum_{j=1}^{n} \overline{z_{i,j}}\theta_j, \\ f_k(\overline{Z}) &= 0\ (1 \leq k \leq n). \end{aligned}$$

補題 4.2 により, $\mathbb{F}_{q^n}$ 係数の m 変数代数方程式は $\mathbb{F}_q$ 係数の mn 変数の n 個の代数方程式に変換される. さらに補題 4.2 における $f(x_1, \cdots, x_m)$ を (9) の左辺の多項式としたときに, Weil descent によって連立代数方程式 (10) は $\mathbb{F}_q$ 係数の mn 変数の $n + mn$ 個の等式で構成される以下の形の連立代数方程式に変換される:

$$\begin{cases} 0 = f_1(Z), \\ \vdots \\ 0 = f_n(Z), \\ 0 = z_{1,1}^q - z_1, \\ \vdots \\ 0 = z_{m,n}^q - z_{m,n}. \end{cases} \tag{11}$$

Weil descent を行う前に比べて, 変数と等式の個数はともに増加するが, 連立代数方程式を解く際に扱う多項式の各変数の次数を q より小さくできることが利点である.

因子基底の設定を工夫することで, Weil descent によって生成される連立代数方程式の変数の個数を削減することができる. まず $\mathbb{F}_{q^n}$ のある $\mathbb{F}_q$ ベクトル部分空間を V とし, その次元を $1 \leq n' < n$ とする. このとき因子基底 FB を次のように定める:

$$FB = \{\pi_\ell \in E(\mathbb{F}_{q^n}) \mid x(\pi_\ell) \in V\}. \tag{12}$$

この因子基底の設定により x_i は Weil descent によって n' 個の変数 $z_{i,j}$ $(1 \leq j \leq n')$ で表されるため, 方程式 (9) は $\mathbb{F}_q$ 係数の $mn'(< mn)$ 変数の n 個の代数方程式に変換される. 最終的にはそれらの代数方程式に Frobenius map に対応する等式 $z_{i,j}^q - z_{i,j} = 0$ を加えた以下の形の連立代数方程式を解

く (但し $Z' := \{z_{i,j} : 1 \leq i \leq m,\ 1 \leq j \leq n'\} \subsetneq Z$ で $z_{i,j} \in Z'$ とする.):

$$\begin{cases} 0 = f_1(Z'), \\ \vdots \\ 0 = f_n(Z'), \\ 0 = z_{1,1}^q - z_1, \\ \vdots \\ 0 = z_{m,n'}^q - z_{m,n'}. \end{cases} \tag{13}$$

n' を小さくすると (13) の変数が少なくなることによりそれを解くために必要な計算コストは削減されるが, (13) が解をもつ確率も下がってしまう.

4.4 ECDLP に関する指数計算法の概要

ECDLP に指数計算法を適用する様々な方法が提案されている [15]. その中で近年, 議論が進められている代表的な方法として, 指数計算法 1 に Semaev の summation polynomial と Weil descent を導入する方法が挙げられる. この節ではその方法について簡単に紹介し, その計算量評価について説明する. またその説明のため, 式 (2) で表される $E(\mathbb{F}_{q^n})$ 上の ECDLP が与えられているとする:

$$\mathcal{T} = [X]\mathcal{P} \in G = \langle \mathcal{P} \rangle \subset E(\mathbb{F}_{q^n}).$$

ECDLP に関する指数計算法;

初期設定段階: 因子基底 FB を (12) のように設定する:

$$FB = \{\pi_\ell \in E(\mathbb{F}_{q^n}) \mid x(\pi_\ell) \in V\}$$

関係探索段階:

(i) $a, b \in \mathbb{N}$ を選び $\mathcal{R} = [a]\mathcal{P} + [b]\mathcal{T}$ を計算する.

(ii) Semaev の summation polynomial S_{m+1} の x_{m+1} に $x(\mathcal{R})$ を代入し[8], それに対して Weil descent を実行することで連立代数方程式 (13) を計算する:

$$\begin{cases} 0 = f_1(Z'), \\ \vdots \\ 0 = f_n(Z'), \\ 0 = z_{1,1}^q - z_1, \\ \vdots \\ 0 = z_{m,n'}^q - z_{m,n'}. \end{cases}$$

[8] m は固定された自然数である.

この連立代数方程式を解き, その解

$$(\overline{z_{1,1}}, \cdots, \overline{z_{m,n'}}) \in (\mathbb{F}_q)^{mn'}$$

が存在するならば[9], その解に対応する $(\overline{x_1}, \cdots, \overline{x_m}) \in (\mathbb{F}_{q^n})^m$ を求める. 即ち V の基底 $\theta_1, \cdots, \theta_{n'} \in \mathbb{F}_{q^n}$ に対して

$$\overline{x_i} = \sum_{j=1}^{n'} \overline{z_{i,j}}\theta_j \in V$$

を計算する. そのような一つの組 $(\overline{x_1}, \cdots, \overline{x_m})$ に対して

$$(\overline{x_1}, \cdots, \overline{x_m}) = (x(\pi_{\ell_1}), \cdots, x(\pi_{\ell_m})) \tag{14}$$

を満たす因子基底の元の組 $(\pi_{\ell_1}, \cdots, \pi_{\ell_m})$ は高々 2^m 個存在する. その中から

$$\mathcal{R} = \sum_{i=1}^{m} \pi_{\ell_i} \tag{15}$$

を満たすものを求め, 下記の等式を満たす非負整数 e_ℓ の組み $(e_1, \cdots, e_s)$ を決定する:

$$\mathcal{R} = \sum_{\ell=1}^{s} [e_\ell]\pi_\ell. \tag{16}$$

この relation (16) は下記の線形方程式に対応する:

$$a + bX \equiv \sum_{\ell=1}^{s} e_\ell \log_{\mathcal{P}} \pi_\ell \pmod{\#G}.$$

実際の計算では (a, b) と $(e_1, \cdots, e_s)$ を結合したベクトルを行列の行 (または列) として保存する.

(iii) (i), (ii) の計算を十分な個数の relation が得られるまで繰り返す.

線形代数段階: 関係探索段階で得られた行列に対して, $\#G$ を法とする行列操作を行うことで以下を満たす X_1, X_2 を計算する:

$$\mathcal{O} = [X_1]\mathcal{P} + [X_2]\mathcal{T}.$$

離散対数計算段階: $X_2^{-1} \pmod{\#G}$ が存在するならば[10] 以下を返す:

$$X = -X_1 X_2^{-1} \pmod{\#G}.$$

[9]存在しないならば, 新しく a, b を選び直して $\mathcal{R}$ を生成して, 同様の計算を続ける.

[10]暗号で利用する ECDLP を考えた場合, $\#G$ は十分大きな素数となるように選ばれるため, $X_2^{-1} \pmod{\#G}$ が存在しない確率は無視できる.

ここから上記のアルゴリズムの計算量について議論する．この計算量の基本的な評価方法の概要は [15] でまとめられている．さらに [15] では，$E(\mathbb{F}_{q^n})$ 上の ECDLP が与えらえているとして，q が n に比べて十分小さい場合及びその逆の場合について分類して説明している．これは暗号で利用される楕円曲線が，$\mathbb{F}_{2^n}$ (n は素数) または $\mathbb{F}_{q^n}$ (q は素数で n は十分小さい) 上で定義されたものが多いためである．

有限体に関する上記の分類によらず，S_{m+1} の m と $n'(=\dim V)$ は一般的に

$$mn' \approx n \tag{17}$$

となるように設定される [14]．(このように設定しない方法もある [15].) また，S_{m+1} の生成に必要な体演算は

$$O(2^{m^2}) \tag{18}$$

であることが知られている [14].

関係探索段階で生成した $\mathcal{R}$ が (15) のように表される確率 $\mathrm{Prob}_{\mathrm{sum}}$ について考える．ここからの議論の準備として，因子基底の個数 s は

$$s \approx \#V \tag{19}$$

を満たすとして良い．その理由は，ランダムに選んだ $\overline{x_i} \in \mathbb{F}_{q^n}$ を与えられた楕円曲線の x 座標として持つ有理点が存在する確率が約 1/2 であることと，同じ x 座標を持つ有理点の個数の期待値が約 2 であることである．

さらに，この節の目的は上述の指数計算法とその計算量の評価方法を大まかに理解することであるため，$q << n$ の場合について議論する．(その逆の場合，即ち $q >> n$ の場合も計算量の評価方法はほぼ同様である．参考文献として [15] を挙げる.) この場合，(19) より

$$s \approx q^{n'} \tag{20}$$

が成り立つ．

確率 $\mathrm{Prob}_{\mathrm{sum}}$ は，因子基底 FB に属する m 個の元の和でかける有理点 $\mathcal{R} \in E(\mathbb{F}_{q^n})$ の割合で見積もる．そのため，そのような m 個の元の和において生じる重複を無視できると仮定している．和の対称性を考慮して，因子基底 FB から m 個の元を選ぶ組み合わせの数は大まかに $s^m/m!$ である．また，$E(\mathbb{F}_{q^n})$ の位数は約 q^n であることと，(20) より

$$\mathrm{Prob}_{\mathrm{sum}} \approx \frac{s^m}{m! \cdot q^n} \approx \frac{1}{m!} \tag{21}$$

が成り立つ．

線形代数段階で扱う行列のランクが $O(\#V) = O(s)$ であることと (21) より，関係探索段階で実行される point decomposition の回数は

$$O(m!s) = O(m!q^{n'})$$

と評価される. 従って, point decomposition の計算コストを $\mathrm{C}_{\mathrm{dcmp}}$ とすると, 関係探索段階の計算量は

$$O(q^{n'} m! \mathrm{C}_{\mathrm{dcmp}}) \tag{22}$$

となる. 線形代数段階の計算量は, 実行可能行列乗算指数 $2 < \omega \leq 3$ に対して

$$O(s^{\omega}) = O(q^{n'\omega}) \tag{23}$$

である. よって, (18), (22), (23) より, 全体の計算量は

$$O(2^{m^2} + q^{n'} m! \mathrm{C}_{\mathrm{dcmp}} + q^{n'\omega}) \tag{24}$$

である.

ここで問題となるのが point decomposition の計算量 $\mathrm{C}_{\mathrm{dcmp}}$ の評価である. この計算量は連立代数方程式 (13) を解くために必要な計算量である. 連立代数方程式を効率よく解く方法については第 5 節で説明する.

5 有限体における連立代数方程式の解法

連立代数方程式 (13) を更生する多項式集合で生成されるイデアルは 0 次元であるため, この節で扱う多項式集合 F も同様の性質を持つとする. そのような F で表現される連立代数方程式を効率よく解く方法として以下の計算を組み合わせる方法が知られている:

- F_4-style のアルゴリズム (第 5.2 節) によって多項式集合 F の全次数逆辞書式順序のグレブナー基底 GB_{DRL} を計算する.
- FGLM (第 5.3 節) を利用して GB_{DRL} を辞書式順序のグレブナー基底 GB_{LEX} に変換する.

GB_{LEX} は, F で与えられる連立代数方程式と同じ解の集合を持つ連立代数方程式を構成する多項式集合である. また, F で生成されるイデアルが 0 次元であるとき, GB_{LEX} はある変数に関する一変数多項式を含む. さらに, その一変数多項式の解を GB_{LEX} の他の多項式に代入することで新たな一変数多項式を得る. この計算を繰り返すことで連立代数方程式の全ての解を解の個数の多項式時間で計算することができる. しかし, GB_{LEX} の計算コストは GB_{DRL} のそれより大きいことが経験的に知られている. そこでまずは GB_{DRL} を計算し, FGLM を利用して GB_{DRL} を GB_{LEX} に変換する.

この節では F_4-style のアルゴリズムと FGLM の計算量について簡単に説明する. また K を体, X を $\{x_1, \cdots, x_m\}$ なる変数の集合とし, $F := \{f_1, \cdots, f_k\} \subset K[X]$ とする. さらに X で生成される項全体の集合を $\mathrm{T}(X)$ で表す.

5.1 連立代数方程式とグレブナー基底の計算

第 5 節で述べたように, 多項式集合 F で与えられる連立代数方程式を解くために, まず F_4-style のアルゴリズムで F の GB_{DRL} 計算する必要がある. この節では F_4-style のアルゴリズムを理解する準備として, グレブナー基底の基本的な計算方法である Buchberger アルゴリズムのキーポイントを説明する.

定義 5.1. 多項式 $f \in K[X]$ と $K[X]$ における項順序 $\prec$ が与えられているとする. この項順序に関して f で最も大きい項 $HT_{\prec}(f)$ を頭項とよび, その係数 $HC_{\prec}(f)$ を頭係数とよぶ. さらに $HC_{\prec}(f)HT_{\prec}(f)$ を頭単項式とよび $HM_{\prec}(f)$ で表す.

Buchberger アルゴリズムでは, S 多項式の計算と多項式集合による多項式の簡約の計算を繰り返すことでグレブナー基底を計算する. 多項式 $f_1, f_2 \in K[X]$ の S 多項式 $\mathrm{Spoly}(f_1, f_2)$ は次のように定義される:

$$\mathrm{Spoly}(f_1, f_2) := \frac{\mathrm{lcm}(\mathrm{HT}_{\prec}(f_1), \mathrm{HT}_{\prec}(f_2))}{\mathrm{HM}_{\prec}(f_1)} f_1 - \frac{\mathrm{lcm}(\mathrm{HT}_{\prec}(f_1), \mathrm{HT}_{\prec}(f_2))}{\mathrm{HM}_{\prec}(f_2)} f_2. \tag{25}$$

ただし, 単項式 m_1, m_2 に対して $\mathrm{lcm}(m_1, m_2)$ はそれらの最小公倍単項式とし, その係数は 1 とする. F_4-style のアルゴリズムにおいて, (25) に現れる f_1 の倍多項式は left-side とよばれ, 同様に f_2 の倍多項式は right-side とよばれる. $\mathrm{Spoly}(f_1, f_2)$ の計算では, f_1, f_2 をそれぞれ単項式倍したものの集合 $\{m_i f_i : m_i \in \mathrm{T}(X)\}$ の中から頭項が一致する項順序が最小の組 $(m_1 f_1, m_2 f_2)$ を選び, その差を計算することでその頭項を消去している. これは互除法において最大の項を削除する計算の一般化である.

次に多項式集合による多項式の簡約について説明する.

定義 5.2. $f_1, f_2 \in K[X]$ としたときに, $\mathrm{HT}_{\prec}(f_2)$ で割り切れる f_1 の項 M が存在し, その係数を C_M とする. このとき

$$f_3 := f_1 - \frac{C_M M}{\mathrm{HM}(f_2)} f_2$$

とする. この操作を f_1 の f_2 による単項簡約とよび,

$$f_1 \underset{f_2}{\longrightarrow} f_3 \tag{26}$$

と書く.

多項式による単項簡約 (26) は多項式集合 F の元による 0 回以上の単項簡約に拡張することができ,

$$f_1 \xrightarrow[F]{*} f_3 \tag{27}$$

のように表す. この操作は単に F による f_1 の簡約とよぶ. また, (27) の f_3 に対して F による単項簡約を 1 回以上実行できないとき, f_3 は f_1 の F による剰余とよぶ.

Buchberger アルゴリズムで実行される多項式の簡約操作の計算効率を上げるアルゴリズムとして F_4-style のアルゴリズムが挙げられる. 第 5.2 節で F_4-style のアルゴリズムについて述べる. Buchberger アルゴリズムの詳細については [6] を参照されたい.

5.2 F_4-style のアルゴリズムとその計算量

グレブナー基底を効率よく解くアルゴリズムとして, J.-C. Faugére によって提案された F_4 アルゴリズム [10] 及び F_5 アルゴリズム [11] が存在する. (以後, それぞれを単純に F_4, F_5 とよぶ.) これら二つのアルゴリズムはグレブナー基底の計算の高速化を図ったものである. F_4 は Macaulay 行列 (定義 5.3) の性質を利用することで多項式の簡約操作の効率化を行う. このようなアルゴリズムは F_4-style のアルゴリズムとよばれる. F_5 では F_4-style のアルゴリズムに signature という概念を導入して不要な S 多項式の生成を排除している.

F_4-style のアルゴリズムの計算量は, 基本的に入力とする多項式集合 F が生成するイデアルが斉次の場合で評価されている. 非斉次の場合には, 新たに変数を一つ追加して F の各多項式を斉次化した上で計算量を評価する. そのため F の生成するイデアルが 0 次元のとき, 斉次化した多項式が生成するイデアルは一般に 1 次元となる.

以下でも特に断らない限り, 入力とする多項式集合 F が生成するイデアルは 0 次元, 即ち零点が有限個の場合に限定して説明する. イデアルのグレブナー基底計算は Macaulay 行列の行簡約化が基本となる.

5.2.1 F_4-style のアルゴリズム

F_4-style のアルゴリズムでは Macaulay 行列の部分行列を利用する:

定義 5.3. $F = \{f_1, \cdots, f_k\} \subset K[X]$ はある $d \in \mathbb{N}$ に対して $\deg(f_1), \cdots, \deg(f_k) \leq d$ [11] を満たすとする. $m_1, m_2, \cdots \in \mathrm{T}(X)$ に対しては $m_1 \succ m_2 \succ \cdots$ が成り立つとする. さらに $t_{i,j}$ は $\deg(t_{i,j} f_i) \leq d$ を満たす全ての $t_{i,j} \in \mathrm{T}(X)$ とし, $t_{i,j} f_i = \sum_\ell c_{i,j,\ell} m_\ell$ $(c_{i,j,\ell} \in K)$ のように表現するとする. このとき F の

[11] $\deg(f_i)$ は f_i の全次数である.

d 次の Macaulay 行列 $M_d(F)$ を以下のように定義する:

$$M_d(F) := \begin{array}{c} \\ t_{i,j}f_i \end{array} \begin{array}{c} \begin{array}{ccc} m_1 & m_2 & \cdots \end{array} \\ \begin{pmatrix} \vdots & \vdots & \\ c_{i,j,1} & c_{i,j,2} & \cdots \\ \vdots & \vdots & \end{pmatrix} \end{array}.$$

F_4-style のアルゴリズムでは各次数 d ごとに, S 多項式の left-side, right-side, 及び多項式集合の簡約で利用される多項式から構成される Macaulay 行列の部分行列を生成してグレブナー基底を計算する. 即ち, その部分行列に対して行簡約操作 (ガウス消去, 掃き出し法など) を行うことで階段形を計算し, この形からグレブナー基底の元を抽出する [21].

F_4-style のアルゴリズムによる計算の特徴として, その計算は一般に大量のメモリを必要とすることが挙げられる. F_4-style のアルゴリズムでは, そのアルゴリズムの性質上, スパース（疎）な行列を扱うことになる[12]. （これは, Macaulay 行列の部分行列である. ）巨大なスパース行列の処理を必要とする別の代表的なアルゴリズムとして数体篩法がある. 数体篩法ではスパース行列で表される線形方程式の解を求めることが目的であるため, 行列のスパース性を保持したまま効率良く計算するアルゴリズム（Lanczos 法など）を効果的に利用できる. しかし, グレブナー基底を計算する F_4-style のアルゴリズムでは簡約した結果の行列が必要であるため, スパース性を保持したまま効率良く計算することは一般的に難しい. F_4-style のアルゴリズムでは前処理として, 行列のスパース性を利用して行列のサイズを小さくするアルゴリズム（structured Gaussian elimination）を利用することが推奨されている [10]. Magma などでの F_4 の実装はブラックボックスであるため, その詳細は不明であるが, 簡約した行列を高速に計算するために, 最終的にはスパース性を犠牲にして実メモリ上で掃き出し法を実行すると考えられる. そのため, Magma で実装されている F_4 のような効率的な実装でさえ使用するメモリ量は結果として膨大になると考えられる.

5.2.2 F_4-style のアルゴリズムの計算量

F_4-style のアルゴリズムで実際に使用する部分行列の大きさは, 入力される多項式集合の多項式の個数や次数のみからでは精密には評価できない. 従って, F_4-style のアルゴリズムの計算量は, Macaulay 行列の簡約操作の計算量と同じオーダーで上から評価される[13]. (これは最悪計算量を見積もっている

[12] スパースな行列を扱う理由として, 例えば, d を初期値からいくつか大きくしたときに, 簡約で利用される多項式に対応する行が一般に疎になる傾向があることが挙げられる.

[13] F_5 の計算量評価では, F_5 による不要な計算の効果を考慮しない Macaulay 行列の行簡約操作の計算量を見積もることになる. 一方, F_4-style のアルゴリズムの場合でも, ECDLP の特殊性を考慮して部分行列のサイズをより詳細に評価する研究もある [14].

ことを意味する.) よって, グレブナー基底の計算量はグレブナー基底の元の最大次数を D とすると, D 次までの Macaulay 行列の簡約操作の計算量となる.

D 次の Macaulay 行列 $M_D(F)$ のサイズは斉次イデアルの場合には D 次の単項式の個数以下になり, それは, m 個の変数から重複を許して D 個を選ぶ組み合わせの個数である. 行列のサイズを N とするとき, 掃き出しの計算量は N^ω であることから, F_4-style の計算量は以下のように見積もられる:

$$O\left(\binom{m+D}{m}^\omega\right).$$

一方, 既約なグレブナー基底の元の最大次数 D は生成元の次数を用いて評価されている. 現在の方針ではイデアルによって定まる Hilbert 多項式の degree of regularity D_{reg} が D の上からの評価を与えるため, D_{reg} の大きさを評価することになる.

多項式集合 F が regular sequence とよばれる形になっていれば, D_{reg} は F に属する多項式の次数の和で抑えられるが, そうでない場合にはそれらの次数の積等で抑えることになる. F が regular sequence でないときは, そのイデアルの元で regular sequence になるものを抽出し, その差分を考えることで次数 D_{reg} を評価する.

実際に変数を $x_1, \cdots, x_m$ とし, 1 次元斉次イデアル I が $f_1, \cdots, f_k (k \geq m-1)$ で生成されているとする. ここで, d_i は f_i の次数で $d_1 \geq d_2 \geq \cdots \geq d_k$ とする. $k = m-1$ で $f_1, \cdots, f_k$ が regular sequence であれば,

$$D_{\mathrm{reg}} \leq d_1 + \cdots + d_{m-1} - m$$

である [20], [21]. しかし, regular sequence でない場合でも, 射影次元が 0 以下であれば同様のことが成り立つ [21]. また, 非斉次の場合には斉次化を行うことで, グレブナー基底の元の最大次数が評価される.

一方で, イデアルの生成系を斉次化したものがイデアル自体の斉次化を生成する場合には, 斉次での評価がそのまま使える. また, F の多項式をランダムにとった場合には, ほとんどの場合に最初の $m-1$ 個が regular sequence になる. そこで, 実際的な計算量として斉次化との計算量のギャップがないものと仮定し, かつ regular sequence の場合を想定して計算量の評価をする方向性もある. 詳細は異なるが本質的には [12], [14], などがこれに対応するものと考える.

以上より, 任意に与えられた F に対して, そのグレブナー基底を計算することなく, その D_{reg} を厳密に評価する方法は現時点では知られていない. そこで, F 自身の持つ代数的な性質を利用して D_{reg} を可能な限り厳密に評価する研究が進められている. このような背景から, 第 6.1 節で説明する first fall degree assumption (FFDA) の導入が議論されている.

5.3 FGLM とその計算量

5.3.1 グレブナー基底の項順序変換

体 K 上の多項式環 $R = K[X]$ のイデアル I の零点をグレブナー基底を用いて求める方法として, I の辞書式順序に関するグレブナー基底を求めて, 変数の少ない多項式から順に零点を求めて代入していくという方法がある. この場合, 一般に辞書式順序グレブナー基底を I の生成系から直接 Buchberger アルゴリズムや F_4 などで求めるのは効率がよくない. よって, 全次数逆辞書式順序など, グレブナー基底が比較的求めやすい項順序に関するグレブナー基底を求めておき, 辞書式順序など, 他の項順序に関するグレブナー基底を求める, 項順序変換 (Change of Ordering) と呼ばれる方法がいくつか提案されている. FGLM [13] は 0 次元イデアルに対して線形代数を応用して項順序変換を行うアルゴリズムである.

5.3.2 FGLM アルゴリズム

イデアル I が 0 次元イデアルのときは, 剰余環 R/I が K 上の線形空間として有限次元であり, I の $\overline{K}$ における零点の個数が有限個である. 以下で, $\prec$ に関するグレブナー基底 G による f の剰余を $\mathrm{NF}_{\prec}(f, G)$ と書くことにする. FGLM アルゴリズムは Algorithm 1 で与えられる.

FGLM アルゴリズムの原理は単項式 h を $\prec_1$ に関する頭項とする多項式がイデアル I の中に含まれるかを, 未定係数法により, h を $\prec_1$ に関する昇順で取り替えながら調べていくというものである. 調べる多項式は $f_h = h + \sum_{t \in B} \lambda_t t$ である. ここで B は, それまでに得られた G_1 の元の頭項 (これは H に格納されている) のどれでも割り切れない単項式が格納されている. $f_h|_{\lambda_t = a_t} \in I$ となるような $a_t \in K (t \in B)$ が存在するとき, $f_h|_{\lambda_t = a_t}$ が G_1 に追加され, 存在しないとき h が B に追加される. $\prec_1$ に関する簡約グレブナー基底を求めるには, h としてそれまでに得られた H のどの元でも割り切れないもののみを考えればよい. これが Algorithm 1 の 11 行目の意味である.

G が $\prec$ に関する I のグレブナー基底であることから

$$f_h|_{\lambda_t = a_t} \in I \Leftrightarrow \mathrm{NF}_{\prec}(f_h|_{\lambda_t = a_t}, G) = 0$$

である. NF の線形性により $\mathrm{NF}_{\prec}(f_h|_{\lambda_t = a_t}, G) = E|_{\lambda_t = a_t}$ を得る. E を R の単項式について整理すると

$$E = \sum_{s \in S} c_s(\lambda_t; t \in B) s$$

と書ける. ここで S は G に関する標準単項式集合 (G のどの先頭単項式でも割れないような単項式の集合) である. よって $E = 0$ は

$$c_s(\lambda_t) = 0 \quad (\forall s \in S)$$

Algorithm 1 FGLM アルゴリズム

Input : 0 次元イデアル I の $\prec$ に関するグレブナー基底 G
Output : I の $\prec_1$ に関する簡約グレブナー基底

$G_1 \leftarrow \emptyset$; $B \leftarrow \emptyset$; $N \leftarrow \emptyset$; $H \leftarrow \emptyset$; $h \leftarrow 1$
loop
  $E \leftarrow \mathrm{NF}_{\prec}(h, G) + \sum_{t \in B} \lambda_t \mathrm{NF}_{\prec}(t, G)$
  if $E = 0$ を満たす $\lambda_t = a_t \in K$ $(t \in B)$ が存在する **then**
    $G_1 \leftarrow G_1 \cup \{h + \sum_{t \in B} a_t t\}$
    $H \leftarrow H \cup \{h\}$
  else
    $B \leftarrow B \cup \{h\}$
    $N \leftarrow N \cup \{x_1 h, \ldots, x_m h\}$
  end if
  $N \leftarrow N \cap \{t \mid t$ は単項式で, すべての $s \in H$ に対し $s \not| t\}$
  if $N = \emptyset$ **then**
    return G_1
  else
    $h \leftarrow N$ 中で $\prec_1$ に関して最小の単項式
    $N \leftarrow N \setminus \{h\}$
  end if
end loop

となる. $c_s(\lambda_t)$ は λ_t の一次式なので, $E=0$ をみたす $\lambda_t = a_t$ を探すことは線形方程式系の求解に帰着される.

5.3.3 FGLM アルゴリズムの計算量

FGLM における主な計算は, $\mathrm{NF}_\prec(t, G)$ の計算と, $f_h|_{\lambda_t=a_t} \in I$ をみたす $\lambda_t = a_t$ が存在するかどうか線形方程式系を解いて調べる計算である. これ以外の手間は, 単項式のリスト操作などであり無視できる. 以下で $\dim_K R/I$ を γ とおく. γ は I の零点の個数と等しい.

- $\mathrm{NF}_\prec(h, G)$ の計算

  $h \neq 1$ のとき $h = x_i h'$ と書けるので, $\mathrm{NF}_\prec(h, G) = \mathrm{NF}_\prec(x_i \mathrm{NF}(h', G), G)$ により, x_i 倍写像 $f \mapsto \mathrm{NF}_\prec(x_i f, G)$ の, R/I の線形空間としての基底 S に関する表現行列を求めておけば, 一つの $\mathrm{NF}_\prec(h, G)$ は, 既に求めてあるはずの $\mathrm{NF}_\prec(h', G)$ から手間 γ^2 で計算できる. この表現行列の計算は, γ 個の単項式 $s \in S$ に関する $\mathrm{NF}_\prec(x_i s, G)$ の計算であるが, これを既に計算してある値を再利用しながら行うことで, x_i 倍写像 $(i = 1, \ldots, m)$ の表現行列を $O(m\gamma^3)$ で行うことができる.

- 線形方程式の求解

  各ステップにおける λ_t の線形方程式系は高々 $O(\gamma^3)$ で解けるが, それを単純にループの回数 ($O(m\gamma)$ であることが示される) だけ繰り返すと $O(m\gamma^4)$ となってしまう. しかし, 各 $\mathrm{NF}_\prec(t, G)$ たちを $s \in S$ の一次式として三角化したものに置き換えて保持しておけば, 新たな $\mathrm{NF}_\prec(h, G)$ に対し $E = 0$ となる $\lambda_t = a_t$ が存在するかどうかは, この三角基底による剰余計算により判定でき, 1 ステップ $O(\gamma^2)$ となる. さらに, この剰余が 0 でないとき, この剰余を付け加えても三角基底という性質は保たれる. よって, ループの回数と合わせて, 線形方程式求解で必要となる手間は $O(m\gamma^3)$ である.

以上により, FGLM アルゴリズムの計算量は $O(m\gamma^3)$ となる.

Summation polynomial から構成される代数方程式系の場合, 変数は $z_{i,j}$ $(i = 1, \ldots, m,\ j = 1, \ldots, n')$ の mn' 個であり, 各 $z_{i,j}$ に対し $z_{i,j}^q - z_{i,j} = 0$ がイデアルの生成系に入っているので, 解の個数は高々 $q^{mn'}$ 個である. よって γ は高々 $q^{mn'}$ となり, FGLM による辞書式順序グレブナー基底への項順序変換の最悪計算量は $O(mn'q^{3mn'})$ となる. しかし, ECDLP の場合は一般的に γ は計算量的に無視できるほどに小さいことが知られている[14]. 従って,

[14] この γ は連立代数方程式の解の個数と等しいことから, ECDLP を指数計算法で解く場合は, γ が大きいほど得られる relation の個数が増加する. これは指数計算法で連立代数方程式を解く回数が減ることにつながる. しかし, 現時点では γ を増加させて計算効率を上げるアルゴリズムは発表されていない.

ECDLP を指数計算法で解く場合, F_4-style のアルゴリズムで必要とされる計算コストに比べて, FGLM のそれは無視できるほどに小さい.

6 ECDLP に関する指数計算法の研究動向

ECDLP に関する指数計算法の研究動向については [15] にまとめられており, 特にその 10.2 節では $E(\mathbb{F}_{2^n})$ 上の ECDLP を準指数時間で解く指数計算法の実現可能性について述べられている. その議論のキーワードとなっているのが first fall degree assumption である. この節では first fall degree assumption について説明する. また, 素体 $\mathbb{F}_p$ における ECDLP への指数計算法の適用 [23] についても述べる.

6.1 First fall degree assumption (FFDA)

2012 年, Petit と Quisquater は first fall degree assumption (FFDA) とよばれる仮定を導入することで, $E(\mathbb{F}_{2^n})$ 上の ECDLP を指数計算法で解くために必要な計算量が準指数時間 $O(2^{C'n^{2/3}\log n})$ であることを示した [24]. 但し C' は 2 未満の定数とする. さらに, 拡大次数 n がおよそ 2000 より大きい場合は, 指数計算法の計算コストは generic algorithm のそれより小さくなることを示した. しかし ECDLP における first fall degree assumption の妥当性については議論が分かれている [15]. この節では first fall degree assumption に関する近年の研究動向について述べる.

6.1.1 First fall degree assumption (FFDA) を仮定した計算量評価

ECDLP に対する指数計算法では一般的に FGLM の計算量は F_4-style の計算量 C_{F_4} より小さいため, point decomposition の計算量 C_{dcmp} は C_{F_4} で評価される. さらに C_{F_4} は degree of regularity D_{reg} で決定される.

この D_{reg} を近似する値として, Petit と Quisquater は first fall degree D_{first} を導入した (この節でも $X = \{x_1, \cdots, x_m\}$ であることに注意.):

定義 6.1. 多項式環 $R := \mathbb{F}_{q^n}[X]$ に対して $F := \{f_1, \cdots, f_k\} \subset R$ とする. ある $h_1, \cdots, h_k \in R$ に対して, D_{first} が以下の条件を満たす最小の次数であるとき, D_{first} を F の first fall degree とよぶ:

- $\sum_{i=1}^{k} h_i f_i \neq 0$,
- $\deg(\sum_{i=1}^{k} h_i f_i) < D_{\mathrm{first}}$,
- $D_{\mathrm{first}} = \max_i(\deg(f_i) + \deg(h_i))$.

(この節でも $Z' = \{z_{1,1}, \cdots, z_{m,n'}\}$ であることに注意.) さらに, first fall degree に対して以下の仮定を導入した:

仮定 6.2. $f \in \mathbb{F}_{2^n}[X]$ は各変数 x_i に対して $\deg_{x_i} f \leq 2^t - 1$ を満たすとする. $\mathbb{F}_{2^n}$ を $\mathbb{F}_2$-ベクトル空間としてみたときの部分ベクトル空間 V の次元を n' とする. V を利用した f への Weil descent で生成される連立代数方程式を構成する多項式集合を $F_f \subset \mathbb{F}_2[Z']$ とし, さらに F_f に全ての $z_{i,j}^2 - z_{i,j}$ を加えた集合を $F_{f,\mathrm{Frob}}$ とする. このとき $F_{f,\mathrm{Frob}}$ の D_{reg} ついて以下が成り立つ:

$$D_{\mathrm{reg}} \approx D_{\mathrm{first}}.$$

Summation polynomial S_{m+1} の x_m に $r \in \mathbb{F}_{2^n}$ を代入した多項式 $S_{m+1}|_{x_{m+1}=r}$ は仮定 6.2 の f の条件を満たす. そのためさらに以下の仮定を導入している:

仮定 6.3. f が summation polynomial から生成された多項式であっても仮定 6.2 は成り立つ.

仮定 6.2 の f を $S_{m+1}|_{x_{m+1}=r}$ に対応させたときの $F_{f,\mathrm{Frob}}$ を $F_{S_{m+1},\mathrm{Frob}}$ とする. このとき, Petit と Quisquater は $F_{S_{m+1},\mathrm{Frob}}$ で与えらえる連立代数方程式を解くことに適した方法として, ブロックグレブナー基底アルゴリズムを主張しており, 仮定 6.3 のもとでそれを解くために必要な計算量 C_{dcmp} は $O((n')^{\omega D_{\mathrm{first}}})$ で, $D_{\mathrm{first}} \approx m^2$ と見積もっている:

$$C_{\mathrm{dcmp}} = O((n')^{\omega m^2}). \tag{28}$$

ただし, $2 < \omega \leq 3$ は実行可能行列乗算指数とする.

(24) に (28) を代入して $E(\mathbb{F}_{2^n})$ 上の ECDLP を解くために必要な計算量 $C_{\mathrm{total}}(\mathbb{F}_{2^n})$ を評価する:

$$O(2^{m^2} + 2^{n'} m!(n')^{\omega m^2} + 2^{n'\omega}). \tag{29}$$

ここで $1/2 < \alpha < 1$ に対して $n' = n^\alpha$, $m = n^{1-\alpha}$ とする. このとき

$$m! \approx n^{1-\alpha} \log n^{1-\alpha} \tag{30}$$

が成り立つ [14]. 従って, (29), (30) より

$$\begin{aligned} C_{\mathrm{total}}(\mathbb{F}_{2^n}) &= O(2^{t_1} + 2^{t_3} + 2^{t_2}), \\ t_1 &:= n^{2(1-\alpha)}, \\ t_2 &:= n^\alpha + n^{1-\alpha}(1-\alpha)\log n + \omega n^{2(1-\alpha)}\alpha \log n, \\ t_3 &:= \omega n^\alpha. \end{aligned} \tag{31}$$

よって最適化することで, (31) で $\alpha = 2/3$ を代入することにより以下を得る:

$$C_{\mathrm{total}}(\mathbb{F}_{2^n}) = O(2^{Cn^{2/3}\log n})$$

ただし定数 C は $C < 2$ を満たす.

6.1.2 First fall degree assumption (FFDA) の妥当性

仮定 6.2, 6.3 は first fall degree assumption (FFDA) とよばれ, いくつかの文献では FFDA を支持する結果や, それを利用して $\mathbb{F}_{2^n}$ 上の ECDLP を解くために必要な計算量を見積もっている [19], [24], [27]. しかしそれらの文献において FFDA は証明されていない. さらにこれらの文献の数値実験で扱われた有限体 $\mathbb{F}_{2^n}$ の拡大次数 n の大きさは, [19] では $n = 26$, [24] では $n = 20$, [27] では $n = 40$ までとなっており, generic algorithm による ECDLP に関する計算の記録 (表 1) に比べてずっと小さい.

FFDA が成り立たない場合は存在する. 例えば多項式集合 $F_1 \subset \mathbb{F}[x_1, x_2]$ と $F_2 \subset \mathbb{F}[x_3, x_4]$ が与えられたとして, F_1, F_2 の degree of regularity をそれぞれ $D_{\mathrm{reg},1}$, $D_{\mathrm{reg},2}$ とし, 同様にそれぞれの first fall degree を $D_{\mathrm{first},1}$, $D_{\mathrm{first},2}$ とする. さらに以下が成り立つとする:

$$D_{\mathrm{first},1} \approx D_{\mathrm{reg},1} << D_{\mathrm{reg},2} \approx D_{\mathrm{first},2}.$$

これは F_1, F_2 において FFDA が成り立っていることを意味する. しかし $F = F_1 \cup F_2 \subset \mathbb{F}[x_1, \cdots, x_4]$ について考えたとき, F の degree of regularity は $D_{\mathrm{reg},2}$ であり, また first fall degree は $D_{\mathrm{first},1}$ であるため FFDA は成り立たない.

FFDA の正当性に疑問を示す結果が存在する. 例えば [17] では, いくつかの $n \leq 40$ に対して $E(\mathbb{F}_{2^n})$ 上の ECDLP を S_3 を利用して解く実験を行っており, D_{first} と D_{reg} の差は n に依存する実験結果を与えた. 即ち, これは FFDA が成り立たないことを主張している.

上述のように FFDA は成り立つことも成り立たないことも厳密にはまだ証明されておらず, また十分大きな拡大体での数値実験の検証も実行されていない. しかし, summation polynomial と Weil descent を利用した ECDLP に関する指数計算法によって, 十分大きな拡大体での数値実験が現時点で成功していないことを考慮すると, FFDA は有効でないと推測される [15].

6.2 素体 $\mathbb{F}_p$ に関する ECDLP と指数計算法

ECDLP だけではなく, (1) のような一般の DLP を解く場合において, 巡回群 G の位数が小さな素数の積で表される場合, 即ち相異なる素数 p_i によって

$$\#G = \prod_{i=1}^{k} p_i^{e_i}$$

のように表されるとき, この G 上の DLP は Pohlig-Hellman のアルゴリズムで

$$O\left(\sum_{i=1}^{k}(e_i(\log \#G + \sqrt{p_i}))\right)$$

回の群演算で解かれることが知られている. 従って, 暗号で利用する巡回群の位数は素数となるように設定している.

2016 年, Petit らは素体上の楕円曲線 $E(\mathbb{F}_p)$ における ECDLP を解く場合に, 巡回群の位数ではなく, 標数 p について以下の条件が成り立つときに有効と思われる指数計算法の因子基底の設定を提案した [23]:

$$p-1=:ST,\ T:=\prod_{j=1}^{k}p_j\approx p^{1/m}.$$

ただし, p_i は与えられた定数 B 以下の素数とし[15], m は利用する summation polynomal S_{m+1} で与えられるとする. $\mathbb{F}_p^*$ の乗法部分群で位数が T であるものを V として因子基底 F を次のように設定する:

$$F=\{\pi_\ell\in E(\mathbb{F}_p)\mid x(\pi_\ell)\in V\}.$$

このとき, $x(\pi_\ell)$ は $\mathbb{F}_p$ における

$$L(x)=1-x^T \tag{32}$$

の根である. この L は以下の関数の合成関数として表すことができる,

$$\begin{aligned}L_j(x) &= x^{p_j}\ (j=1,\cdots,k-1),\\ L_k(x) &= 1-x^{p_k},\\ L(x) &= (L_k\circ\cdots\circ L_1)(x).\end{aligned}$$

このとき以下の多項式で与えられる連立代数方程式を解くことで relation を得ることができる:

$$\begin{aligned}0 &= S_{m+1}(x_{1,1},\cdots,x_{m,1},x(\mathcal{R})),\ (\mathcal{R}=[a]\mathcal{P}+[b]\mathcal{T}\in E(\mathbb{F}_p)),\\ x_{i,j+1} &= L_j(x_{i,j})\ (i=1,\cdots,m;j=1,\cdots,k-1),\\ 0 &= L_k(x_{i,k})\ (i=1,\cdots,m).\end{aligned}$$

この提案方法の計算量の評価は与えられていない. また [23] ではこの提案方法を基にしたいくつかの工夫について述べられているが, 20-bit 程度の大きさの p に対する実験結果が報告されているだけで, 現時点では楕円曲線暗号の脅威とはなっていない.

7 まとめ

本稿では研究が近年盛んに行なわれている, summation polynomial と Weil descent を利用した, ECDLP に関する指数計算法について議論した. その内

[15] $i\neq i'$ に対して $p_i\neq p_{i'}$ である必要はない.

容は, サーベイ論文 [15] を基に, この種の計算方法の概要を整理したものである. [15] では連立代数方程式を解く方法に関する記述が少ないが, この部分は first fall degree assumption などの理解に必要な部分であるため, その主な計算方法として F_4-style のアルゴリズムと FGLM を組み合わせた方法に関する節を設けた. また [15] が公開された後に発表された, 素体上の楕円曲線 $E(\mathbb{F}_p)$ 上の ECDLP を考慮した指数計算法 [23] についても説明した.

第 6 節で述べたように $E(\mathbb{F}_{2^n})$ 上の ECDLP を解く指数計算法で, その計算量が準指数時間になると主張している文献がいくつか存在する. しかし first fall degree assumption など, 利用している仮定の正当性は必ずしも保証されているとは限らない. Generic algorithm と ECDLP を解く指数計算法の比較で重要なのは, [15] でも述べられているように, 現時点で実際にどれくらいの大きさの有限体における ECDLP が解けているかである. 指数計算法の場合は, 限られた小さな有限体上の楕円曲線における実験しか報告例がないことから, 現時点では ECDLP を利用した暗号の安全性は generic algorithm の計算量によって評価されるべきである. また, 十分大きな有限体上における ECDLP を指数計算法で解く場合に, 第 5.2.1 節で述べたように, F_4-style のアルゴリズムが膨大な量のメモリを必要とすることが障害となっている. このことを, ECDLP に関する指数計算法が現時点で有効でない一因として挙げる. しかしながら, ECDLP に関する指数計算法の研究動向は今後も注視する必要がある.

参考文献

[1] D. J. Bernstein, S. Engels, T. Lange, R. Niederhagen, C. Paar, P. Schwabe, and R. Zimmermann. Faster discrete logarithms on fpgas. *IACR Cryptology ePrint Archive*, Vol. 2016, p. 382, 2016.

[2] J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra, and P. L. Montgomery. Solving a 112-bit prime elliptic curve discrete logarithm problem on game consoles using sloppy reduction. *IJACT*, Vol. 2, No. 3, pp. 212–228, 2012.

[3] Certicom Research. Certicom ECC challenge (latest update: November 10, 2009). https://www.certicom.com/images/pdfs/challenge-2009.pdf, 2009.

[4] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer, 1993.

[5] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall/CRC, 2005.

[6] D. A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer, 1998.

[7] R. Crandall and C. Pomerance. *Prime Numbers: A Computational Perspective (2nd Edition)*. Springer, 2005.

[8] CRYPTREC. CRYPTREC Report 2014, 2014. `http://www.cryptrec.go.jp/report/c14\_eval\_web.pdf`.

[9] C. Diem. On the discrete logarithm problem in elliptic curves. *Compositio Mathematica*, Vol. 147, pp. 75–104, 2011.

[10] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure and Applied Algebra*, Vol. 139, No. 1–3, pp. 61–88, 1999.

[11] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *ISSAC 2002, Proceedings*, pp. 75–83, 2002.

[12] J.-C. Faugère, P. Gaudry, L. Huot, and G. Renault. Using symmetries in the index calculus for elliptic curves discrete logarithm. *J. Cryptology*, Vol. 27, No. 4, pp. 595–635, 2014.

[13] J.-C. Faugère, P. M. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional gröbner bases by change of ordering. *J. Symb. Comput.*, Vol. 16, No. 4, pp. 329–344, 1993.

[14] J.-C. Faugère, L. Perret, C. Petit, and G. Renault. Improving the complexity of index calculus algorithms in elliptic curves over binary fields. In *EUROCRYPT 2012, Proceedings*, pp. 27–44, 2012.

[15] S. D. Galbraith and P. Gaudry. Recent progress on the elliptic curve discrete logarithm problem. *Des. Codes Cryptography*, Vol. 78, No. 1, pp. 51–72, 2016.

[16] P. Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *J. Symb. Comput.*, Vol. 44, No. 12, pp. 1690–1702, 2009.

[17] M.-D. A. Huang, M. Kosters, and S. L. Yeo. Last fall degree, hfe, and weil descent attacks on ECDLP. In *CRYPTO 2015, Proceedings, Part I*, pp. 581–600, 2015.

[18] T. Izu. Current status on solving ECDLP. In *SCIS 2017, Proceedings*, 2017.

[19] K. Karabina. Point decomposition problem in binary elliptic curves. *IACR Cryptology ePrint Archive*, 2015. `http://eprint.iacr.org/2015/319`.

[20] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 2*. Spromger, 2005.

[21] D. Lazard. Gröbner-bases, gaussian elimination and resolution of systems of algebraic equations. In *EUROCAL '83, Proceedings*, pp. 146–156, 1983.

[22] E. W. Mayr and S. Ritscher. Dimension-dependent bounds for gröbner bases of polynomial ideals. *J. Symb. Comput.*, Vol. 49, pp. 78–94, 2013.

[23] C. Petit, M. Kosters, and A. Messeng. Algebraic approaches for the elliptic curve discrete logarithm problem over prime fields. In *PKC 2016, Proceedings, Part II*, pp. 3–18, 2016.

[24] C. Petit and J.J. Quisquater. On polynomial systems arising from a Weil descent. In *ASIACRYPT 2012, Proceedings*, pp. 451–466, 2012.

[25] J. M. Pollard. Monte carlo methods for index computation (mod p). *Math. Comp.*, Vol. 32, pp. 918–924, 1978.

[26] I. A. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. *IACR Cryptology ePrint Archive*, 2004. `http://eprint.iacr.org/2004/031`.

[27] I. A. Semaev. New algorithm for the discrete logarithm problem on elliptic curves. *IACR Cryptology ePrint Archive*, 2015. `http://eprint.iacr.org/2015/310`.

[28] D. Shanks. Class number, a theory of factorization and genera. In *Proc. Symp. Pure Math. 20*, pp. 415–440, 1971.

[29] E. Wenger and P. Wolfger. Solving the discrete logarithm of a 113-bit koblitz curve with an fpga cluster. In *SAC 2014, Proceedings*, pp. 363–379, 2014.

[30] E. Wenger and P. Wolfger. Harder, better, faster, stronger: elliptic curve discrete logarithm computations on fpgas. *J. Cryptographic Engineering*, Vol. 6, No. 4, pp. 287–297, 2016.

Cryptographic Multilinear Maps

A Status Report

Mehdi Tibouchi
NTT Secure Platform Laboratories

January 2017

Executive Summary

A few years ago, Garg, Gentry and Halevi (EUROCRYPT 2013) proposed the first candidate construction of *cryptographic multilinear maps*, a primitive first envisioned a decade earlier by Boneh and Silverberg (Contemp. Math. 2003) as a higher-dimensional generalization of bilinear pairings on elliptic curves.

Boneh and Silverberg themselves had pointed out several interesting applications of multilinear maps, such as one-round multiparty key agreement, verifiable pseudorandom functions and efficient broadcast encryption. Furthermore, following the construction of Garg et al., a flurry of new research uncovered even more far-reaching applications, including long-awaited primitives like attribute-based encryption for all circuits and general functional encryption, fruitful new ideas like witness encryption, and the startlingly powerful notion of *indistinguishability obfuscation*.

However, the candidate construction of Garg et al. was not provably secure. As a result, part of the new research focused on clarifying its security, and on exploring alternate techniques to achieve multilinear maps.

This document aims at giving a bird's eye view of the main results so far, in terms of new definitions, candidate constructions and major applications, and to summarize known attacks against existing schemes, discussing their current status as far as security is concerned.

This is a very active and rapidly evolving area of research, so we cannot even come close to an exhaustive survey of existing literature, and although we have strived to take into account some of the most recent published results as of late 2016, significant shifts in our understanding of multilinear maps in the near future are not only impossible to rule out but even likely to occur. Indeed, it has happened on several occasions already that a newly proposed scheme has been broken, fixed and broken again within the span of a few weeks.

With those caveats, here are some notable takeaways from the state of the art at this point in time:

- There are three main constructions proposed for multilinear maps: the original one from Garg, Gentry and Halevi (GGH13), a variant "over the integers" due to

Coron, Lepoint and Tibouchi (CLT13), and a "graph-induced" construction by Gentry, Gorbunov and Halevi (GGH15).

- Although these constructions are conceptually inspired by fully homomorphic encryption schemes that can be proved secure under well-understood hardness assumptions, the multilinear map schemes themselves have no proof of security. (Note that the same is true for bilinear pairings as well).

- Over each of the three constructions, *there exists a polynomial time attack against the basic Diffie–Hellman key multiparty exchange protocol.* In fact, the conceptual counterpart of the CDH assumption fails to hold. As a result, most of the (stronger) assumptions used to prove the existence of more interesting cryptographic notions like witness encryption and indistinguishability obfuscation also fail to hold.

- However, this does not necessarily translate to a direct attack against the actual instantiations of the primitives themselves. For indistinguishability obfuscation, in particular, attacks are known against some instantiations, but countermeasures have been proposed to circumvent them. Thus, *there are constructions of indistinguishability obfuscation* over GGH13, CLT13 and GGH15 *against which no attack is known* at the present time. Whether this will continue to hold is difficult to predict.

- Theoretically speaking, and assuming standard cryptographic hardness assumptions, it is known that indistinguishability obfuscation and secure functional encryption are essentially equivalent, and imply the existence of secure n-linear maps for polynomially large n (both in the original sense of Boneh and Silverberg and in the sense of graded encodings, as introduced by Garg et al.). This means that any alternate method to construct indistinguishability obfuscation or functional encryption would indirectly yield secure multilinear maps. Unfortunately, no such method is known at present.

- Conversely, it has also been shown that 5-linear maps for which the (subexponential) DDH assumption holds are sufficient to obtain indistinguishability obfuscation. This means that one can bootstrap constant-degree multilinear maps to arbitrary polynomial degree, and also that we seem to be tantalizingly close to achieving indistinguishability obfuscation (and hence everything else) from bilinear pairings, a primitive that we are much more confident does exist. Closing the gap from degree 5 to degree 2, however, appears to be an elusive problem.

- There is no prospect of achieving practical levels of efficiency for any of the primitives considered in this document in the foreseeable future.

Contents

Executive Summary **3**

1 Introduction **7**
1.1 From Diffie–Hellman to multilinear maps 7
1.2 Multilinear maps from geometry? 8
1.3 Fully homomorphic encryption and graded encoding schemes 10
1.4 Some applications of multilinear maps 12
1.5 Attacks against multilinear map constructions 15

2 Definitions and Constructions **17**
2.1 Multilinear maps 17
2.2 Graded encoding schemes 18
2.3 Security definitions: the example of Diffie–Hellman key exchange 20
2.4 A concrete instantiation: the CLT13 graded encoding scheme 22
2.5 GGH15 and the graph-induced approach 26

3 Overview of Known Attacks **31**
3.1 Zeroizing attacks: breaking Diffie–Hellman key exchange over GGH13 and CLT13 31
3.2 Graph-induced cryptanalysis: breaking GGH15 key exchange 34
3.3 Attacks on obfuscation 39

4 Conclusions and Perspectives **43**
4.1 Status of multilinear map-based primitives 43
4.2 Future prospects 44

Bibliography **45**

Chapter 1

Introduction

1.1 From Diffie–Hellman to multilinear maps

"We stand today on the brink of a revolution in cryptography," wrote Diffie and Hellman in their seminal *New Directions* paper from 1976 [DH76], which introduced the main ideas of public-key cryptography. In particular, they described the well-known key exchange protocol which bears their name: Alice and Bob can derive a common secret by exchanging messages publicly on an insecure channel. To do so, they agree on a group $\mathbb{G}$ (say a cyclic subgroup of large prime order q in the multiplicative group $\mathbb{F}_p^*$ of a finite field $\mathbb{F}_p$) and a generator g of $\mathbb{G}$. Then Alice and Bob choose random exponents $a, b \in \{0, \ldots, q-1\}$, and compute the group elements

$$A = g^a \quad \text{and} \quad B = g^b$$

respectively. Alice sends A to Bob and Bob B to Alice, and they can then both compute the common group element $g^{ab} = A^b = B^a$. However, the problem of distinguishing g^{ab} from a random element of $\mathbb{G}$ given g, g^a and g^b is believed to be hard (for the group $\mathbb{G}$ mentioned above, and many other groups like suitably chosen elliptic curves). As a result, an eavesdropper learns no information about the common secret by intercepting the communication between the two parties.

As we well know, that idea, and the corresponding Decisional Diffie–Hellman (DDH) hardness assumption, proved extremely fruitful. It can be used to construct semantically secure homomorphic encryption [ElG85], digital signatures [Sch91], efficient pseudorandom functions [NR04], CCA-secure encryption [CS03] and more. And it is cited as one of the main reason for Diffie and Hellman's Turing award.

Nevertheless, some cryptographic primitives cannot be constructed from DDH. For example, Papakonstantinou et al. were able to obtain a black-box separation result [PRV12] between DDH and identity-based encryption (IBE). To construct IBE, a more powerful setting is necessary, and that setting emerged in the early 2000s, bringing about what would be fair to call a second "revolution in cryptography": the era of bilinear pairings.

The existence of efficiently computable bilinear pairings between certain families of elliptic curve groups was first understood as a cryptanalytic liability [MVO93], but Joux

noticed that it could be used constructively to generalize Diffie–Hellman key exchange to three parties in one round [Jou04]. Indeed, if $\mathbb{G}$ is a cyclic group of prime order q endowed with a symmetric non degenerate bilinear pairing $e\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, Alice, Bob and Charlie can use it to derive a common secret as follows. They choose $a, b, c \in \{0, \ldots, q-1\}$ at random and compute

$$A = g^a, \quad B = g^b \quad \text{and} \quad C = g^c$$

respectively, for some agreed upon generator g. They can then all compute the common value

$$e(g,g)^{abc} = e(A,B)^c = e(B,C)^a = e(C,A)^b$$

but an eavesdropper seeing A, B and C cannot distinguish that value from a random element of $\mathbb{G}_T$, assuming the hardness of the *decisional bilinear Diffie–Hellman* (DBDH) problem, which is believed to be hard over well-constructed pairing-friendly elliptic curves.

Using this new bilinear structure, Boneh and Franklin were then able to construct the first IBE scheme [BF03], opening up the path to numerous new cryptographic notions, including public-key encryption with keyword search [BDOP04], attribute-based encryption (for boolean formulas) [GPSW06a] and homomorphic encryption for quadratic polynomials [BGN05]. It also led to more efficient constructions of previous primitives such as signatures [BLS04], group signatures [BBS04], non-interactive zero-knowledge proofs [GS08] and more. In short, the possibility offered by bilinear pairings to carry out not only linear operations in the exponent of group elements but also *one* level of multiplication proved to be particularly fecund. It also earned Joux, Boneh and Franklin the 2013 Gödel prize.

Soon after the cryptographic community realized the power of bilinear maps, Boneh and Silverberg [BS03] asked the natural question of whether this development could be pursued further, in such a way that *several* levels of multiplications could be carried out in the exponent of group elements. This would be possible using what they called *cryptographic multilinear maps*.

1.2 Multilinear maps from geometry?

For cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ of prime order q, a map $e\colon \mathbb{G}^n \to \mathbb{G}_T$ is said to be a (symmetric) *n-linear map* (or just a *multilinear map* when n is omitted) if for any $a_1, \ldots, a_n \in \mathbb{Z}$ and $g_1, \ldots, g_n \in \mathbb{G}$, we have

$$e(g_1^{a_1}, \ldots, g_n^{a_n}) = e(g_1, \ldots, g_n)^{a_1 \cdots a_n},$$

and furthermore e is non-degenerate in the sense that $e(g, \ldots, g)$ is a generator of $\mathbb{G}_T$ for any generator g of $\mathbb{G}$. For such a structure to be of cryptographic interest, one needs to be able to compute efficiently with it (in the sense that e itself and the group operations on $\mathbb{G}$ and $\mathbb{G}_T$ are efficiently computable), and it needs to satisfy some notion of security—the most basic of which would be to ask that the discrete logarithm problem in $\mathbb{G}$ be hard (which implies that it is hard in $\mathbb{G}_T$ as well). This is in essence how Boneh and Silverberg define cryptographic multilinear maps [BS03].

They observed that if one can construct such cryptographic multilinear maps (satisfying slightly stronger security notions that the basic discrete log one), a number of interesting cryptographic consequences follow, beyond what can be done with bilinear pairings. In particular, using an n-linear maps, one can obtain a one-round Diffie–Hellman-like key exchange protocol between $n+1$ parties, as a direct generalization of Joux's protocol. Indeed, if users $U_0, \ldots, U_n$ want to derive a common secret, they can simply pick random exponents $a_0, \ldots, a_n$, compute the group elements $A_i = g^{a_i} \in \mathbb{G}$ and broadcast them. They are then able to compute the common value $e(g, \ldots, g)^{a_0 \cdots a_n}$: user U_j can obtain it as $e(A_{j+1}, \ldots, A_n, A_0, \ldots, A_{j-1})^{a_j}$. However, under the obvious generalization of the decisional Diffie–Hellman assumption, that value is indistinguishable from a random element of $\mathbb{G}_T$ given only the A_i's, making the protocol secure against eavesdroppers.

Other applications mentioned by Boneh and Silverberg include efficient unique signatures and broadcast encryption with short keys and optimal communication complexity. It turns out that multilinear maps also imply much stronger cryptographic notions, including indistinguishability obfuscation (see §1.4 below).

So do these multilinear maps exist? The question is especially natural in view of the fact that bilinear pairings on elliptic curves are a special case of a type of multilinear structure that exists on very large classes of algebraic geometric objects. Roughly speaking, a geometric object (say a project algebraic variety) gives rises to certain groups called "cohomology groups," together with multilinear maps between them known as cup-products. An object of dimension d has cohomology groups of degrees 0 to $2d$ and degrees add up in cup-products, so one could in principle construct a $2d$-linear map from degree 1 to degree $2d$ from any d-dimensional object; in fact, elliptic curve pairings are essentially of that form. However, it is unclear in general how to compute on those groups efficiently (or what the suitable analogue of pairing-friendly elliptic curves would be).

Boneh and Silverberg carried out a detailed analysis of the most direct generalization of elliptic curves to higher dimensions, namely abelian varieties. As for elliptic curves, their set of points is endowed with an efficiently computable group law, and that group is isomorphic to degree 1 cohomology, so that one can actually compute inside that cohomology. This makes it possible to define multilinear maps in various ways. Unfortunately, Boneh and Silverberg found that, unlike what happens with elliptic curves, the *target group* of those multilinear maps does not appear to lend itself to efficient arithmetic operations: what one gets is essentially a higher tensor power of the multiplicative group. For example, over the finite field $\mathbb{F}_p$, the target group is essentially $\mathbb{F}_p^*$, except that g^a is represented as the tuple $(g^{a_1}, \ldots, g^{a_d}) \in (\mathbb{F}_p^*)^d$ for any $(a_1, \ldots, a_d)$ such that $a = a_1 \cdots a_d$. Clearly, one cannot even efficiently decide equality in that group without breaking the computational Diffie–Hellman problem.

More generally, their paper shows that, under widely believed assumptions, it is impossible to construct n-linear maps from geometry whose target group is $\mathbb{F}_p^*$ itself (as opposed to a higher tensor power, say) for any $n > 2$. This does not entirely rule out multilinear maps from geometry (e.g. one could still conceivably have multilinear maps whose target group would lie in an elliptic curve or some other group with efficient arithmetic), but makes it implausible enough that the problem has only been revisited on a handful of occasions

since then [RH09]. In any case, after Boneh and Silverberg's paper, constructing multilinear maps was considered intractable for at least a decade.

1.3 Fully homomorphic encryption and graded encoding schemes

New ideas to tackle the problem of obtaining multilinear maps only came about after a third "revolution" swept the world of cryptography, mainly from the mid-2000s onwards: lattice-based cryptography, ultimately leading to the construction by Gentry of a *fully-homomorphic encryption scheme* [Gen09], which solved a major, 30-year old open problem [RAD78].

Before Gentry, some encryption schemes like those of ElGamal and Paillier [ElG85, Pai99] had made it possible to carry out *either* additions *or* multiplications on ciphertexts. The pairing-based scheme of Boneh, Goh and Nissim [BGN05] supported arbitrarily many additions and *one* level of multiplications. In contrast, fully-homomorphic encryption (FHE) makes it possible to carry out *both* additions and multiplications on ciphertexts, arbitrarily many times (and as a result, any efficient function can be evaluated homomorphically on ciphertexts).

A few years later, this led to the intuition that FHE ciphertexts behave a bit like the exponents of group elements in a multilinear map. More precisely, they behave similarly to the exponents of group elements in what Garg, Gentry and Halevi call a *graded encoding scheme* [GGH13a]. Roughly speaking, such a scheme is a family of efficient cyclic groups $\mathbb{G}_0, \ldots, \mathbb{G}_n$ of the same prime order q together with efficient non-degenerate bilinear pairings $e\colon \mathbb{G}_i \times \mathbb{G}_j \to \mathbb{G}_{i+j}$ whenever $i + j \leq n$. In other words, if we fix a family of generators g_i of the $\mathbb{G}_i$'s in such a way that $g_{i+j} = e(g_i, g_j)$, we can *add* exponents within a given group $\mathbb{G}_i$:

$$g_i^a \cdot g_i^b = g_i^{a+b}$$

and *multiply* exponents from two groups $\mathbb{G}_i, \mathbb{G}_j$ as long as $i + j \leq n$:

$$e(g_i^a, g_j^b) = g_{i+j}^{a \cdot b}.$$

This makes g_1^a somewhat similar to an "FHE encryption" of a.

Of course, there are a number of differences. First, FHE ciphertexts should be randomized. This is not a serious difficulty: one can allow for randomized representations of group elements as well, and such representations are in fact permitted in Garg et al.'s definition of a graded encoding scheme. However, one should still make it possible to test the equality of two (randomized representations of) group elements in $\mathbb{G}_n$, say; this cannot be done publicly in an FHE scheme, as it would break semantic security. Nevertheless, this may be doable once some limited information about the FHE secret key is made public. Finally, a third difference is that one should not be able to invert the bilinear pairings, so the representations of g_i^a and g_j^a cannot be of the same form when $i \neq j$. This can be dealt with by introducing some secret multiplicative factor in ciphertexts that will appear at the power i in the ciphertext corresponding to an element of $\mathbb{G}_i$.

These intuitive ideas essentially describe how Garg, Gentry and Halevi's GGH13 multilinear maps [GGH13a] are obtained based on (the large message space, somewhat homomorphic variant of) Gentry's FHE scheme [Gen09].

More precisely, Gentry's scheme is defined over the cyclotomic ring $R = \mathbb{Z}[\mathbf{x}]/(\mathbf{x}^m + 1)$ for some m, with respect to a certain principal ideal $I = \langle \mathbf{g} \rangle$ with small generator $\mathbf{g}$. The plaintext space consists of small elements in R/I (say polynomials with $0/1$ coefficients) and a message $\mathbf{m}$ is encrypted as $\mathbf{c} = \mathbf{m} + \mathbf{r} \cdot \mathbf{g} \bmod q \in R_q = R/qR$ for some small noise $\mathbf{r}$. In contrast, a GGH13 encoding of $\mathbf{m}$ at level i is of the form:

$$\mathbf{c}_i = \frac{\mathbf{m} + \mathbf{r} \cdot \mathbf{g}}{\mathbf{z}^i} \bmod q,$$

where $\mathbf{z}$ is a secret masking element, and one can see that linear operations at a given level as well as multiplications between levels work as expected (as long as the noise values $\mathbf{r}$ remain appropriately small). Equality tests at level n are carried out using a *zero-testing parameter* $\mathbf{p}_{\text{zt}}$ of the form:

$$\mathbf{p}_{\text{zt}} = \mathbf{h} \cdot \mathbf{z}^n \cdot \mathbf{g}^{-1} \bmod q$$

where $\mathbf{h}$ is small: the idea is that $\mathbf{p}_{\text{zt}} \cdot \mathbf{c}_n \equiv \mathbf{h} \cdot (\mathbf{m}\mathbf{g}^{-1} + \mathbf{r}) \bmod q$ will be small if and only if $\mathbf{m} = 0$, allowing to test for equality to zero, and then usual equality by linearity.

For Gentry's scheme to be secure, the generator $\mathbf{g}$ of I has to be kept secret, although a "bad" basis of I consisting of large vectors can be published. Since $\mathbf{p}_{\text{zt}}$ depends on $\mathbf{g}$, we can see that the zero-testing parameters reveals some information about the FHE secret key as expected. This partial key leakage, which is inherent to the conceptual construction of multilinear maps from FHE, is the reason why we are not able to prove the scheme secure even though the FHE scheme itself has a proof of security.

Soon after Garg et al. published their candidate construction, another FHE-inspired construction was described by Coron, Lepoint and Tibouchi [CLT13a], related this time to the FHE scheme "over the integers" of van Dijk et al. [vDGHV10] (or more precisely, on the batch variant due to Cheon et al. [CCK+13]). The main ingredients of the construction are essentially the same as those of [GGH13a], although a number of technical details are different.

Later on, variants of those two constructions were proposed to address certain technical issues, although with limited success [LSS14, CLT15]. In addition, a substantially different construction (GGH15) was introduced by Gentry, Gorbunov and Halevi [GGH15], inspired by the LWE-based FHE scheme of Gentry, Sahai and Waters [GSW13]. The functionality achieved in GGH15 differs syntactically from that of GGH13 and CLT13: instead of being arranged in a graded structure, the "groups" containing the encodings correspond to edges on a directed acyclic graph, and two encodings can be multiplied together if and only if their associated edges are adjacent. It is not immediately obvious how to use that primitive to construct the same cryptographic objects as with standard multilinear maps, but Gentry et al. showed how it can be done in a number of specific instances, including multiparty key exchange and obfuscation.

1.4 Some applications of multilinear maps

Multiparty Diffie–Hellman key exchange. As we have mentioned, the most direct application of n-linear maps is a one-round protocol for $(n+1)$-way Diffie–Hellman key exchange. This protocol can also be instantiated in the *graded encoding scheme* setting of Garg et al. [GGH13a]. Note however that since encodings are randomized, to derive a common shared key, the parties need to be able to extract some deterministic value depending only on the underlying "group element" that randomized encoding represent. This procedure is an extension of the zero-testing algorithm alluded to above, and is part of the formal definition of a graded encoding scheme. See §2.2 for details, and §2.3 for a formal description of the multiparty Diffie–Hellman key exchange protocol over graded encoding schemes.

Attribute-based encryption for circuits. One of the great successes of pairing-based cryptography is the realization of the notion of *attribute-based encryption* (ABE) [SW05, GPSW06a]. In a (ciphertext-policy) ABE scheme, users have secret keys associated with certain sets of attributes, and messages are encrypted with respect to policies which are Boolean functions of the attributes. Thus, a user with attributes x and y can decrypt ciphertexts associated with the policy $x \wedge y$, or the policy $x \vee z$, but not the policy $x \wedge z$. A major challenge in constructing ABE is the requirement that the scheme should achieve *collusion-resistance*: if Alice has the attributes x, y and Bob has the attributes y, z, they should not be able to decrypt a ciphertext with policy $x \wedge z$ even when colluding together.

There are constructions of ABE based on bilinear pairings that support policies represented by arbitrary Boolean *formulas* of the attributes, or more generally by span programs [GPSW06b], but techniques based on pairings have so far failed to achieve ABE for arbitrary polynomial-size Boolean *circuits*. One seems to encounter a fundamental limitation of bilinearity when trying to obtain collusion-resistance for arbitrary circuits, due to a class of attack known as backtracking [GGH+13c, §1].

On the other hand, over *multilinear maps*, relatively direct generalizations of the classical pairing-based constructions of ABE yield ABE for all circuits right away, as shown by Garg et al. [GGH+13c, GGHZ14]. Later on, Gorbunov, Vaikuntanathan and Wee were able to construct attribute-based encryption for circuits from standard lattice assumptions as well [GVW13], but the problem of a pairing-based realization remains open.

Witness encryption. Shortly after the first multilinear map candidate GGH13 was proposed, Garg, Gentry, Sahai and Waters introduced the intriguing and powerful new notion of *witness encryption*, and showed how it can be realized from multilinear maps [GGSW13]. A witness encryption scheme is defined with respect to a certain NP language L, and consists of two efficient algorithms: $\mathsf{Encrypt}(1^\lambda, x, m)$ takes as input a security parameter, a string x and a message m, and outputs a ciphertext c; $\mathsf{Decrypt}(c, w)$ takes as input a ciphertext c and a string w, and outputs either a message m' or $\perp$. Correctness states that if x is an instance of L and w is a witness of $x \in L$, then $\mathsf{Decrypt}(\mathsf{Encrypt}(1^\lambda, x, m), w)$ outputs the same message m with probability 1. Soundness security states that the encryptions of distinct messages with respect to a string $x \notin L$ are indistinguishable.

In other words, witness encryption makes it possible to encrypt messages with respect to an instance x of the language L, and one can decrypt a ciphertext if one knows a witness to the fact that $x \in L$. Security does *not* imply that knowing a witness is necessary to decrypt in general. But depending on the language L, it may be the case that instances and non-instances are computationally indistinguishable without a witness (consider e.g. the language of Diffie–Hellman pairs over a DDH group), and soundness then implies a form of semantic security with respect to adversary who do not know the witness.

Witness encryption is a powerful notion; it implies strong forms of identity-based encryption, and even ABE for all circuits in an essentially black-box way [GGSW13]. The original instantiation was based on a hardness assumption that mimicked the construction very closely, but constructions based on less ad hoc assumptions were later proposed as well [GLW14, AJN+16].

Functional encryption. The notion of *functional encryption* is a far-reaching generalization of ABE introduced by Boneh, Sahai and Waters [BSW11]. In a functional encryption scheme defined with respect to a functionality $F\colon K \times X \to \{0,1\}^*$, a user secret key sk_k is associated with an element k the set K, and if a ciphertext c is an encryption of $x \in X$, the decryption algorithm applied to sk_k and c returns $F(k,x)$. For example, ciphertext-policy ABE is the special case when elements k of K are sets of attributes, elements of X consist of a pair (m,f) of a message and a predicate, and the functionality $F(k,x)$ evaluates to m if $f(k)$ is true and to $\perp$ otherwise.

A number of special cases of functional encryption have been described in the context of pairing-based cryptography, such as predicate encryption for inner-products [KSW08, OT09], spatial encryption [Ham11] and functional encryption for inner-product functionalities [ABDP15, BJK15], but they tend to be limited to functionalities that are "bilinear" in some sense.[1]

In contrast, one of the first results to emerge as a consequence of multilinear maps was a construction of functional encryption for all circuits [GGH+13b]. That construction is in fact based on the *indistinguishability obfuscator* proposed in the same paper (see below), so it relies on multilinear maps only in an indirect way in some sense. However, other instantiations based directly on multilinear maps (i.e. without obfuscation) have later been described, starting with the scheme of Garg, Gentry, Halevi and Zhandry [GGHZ16].

Indistinguishability obfuscation. Perhaps the most impressive result that followed the GGH13 multilinear map candidate was the description by Garg et al. [GGH+13b] of a possible construction of *indistinguishability obfuscation* for all circuits. Program obfuscation, roughly speaking, aims at making it possible to publish programs whose functionality depends on some secrets in such a way that even the source code of the program will not reveal those secrets. They are, in some sense, hidden in plain sight.

[1] More general notions have also been achieved over lattices, such as leveled predicate encryption for circuits [GVW15], and even some strong forms of functional encryption for circuits with a single-bit output [GKP+13]. Those notions, however, are weaker than the functional encryption schemes achieved from multilinear maps.

Strong forms of obfuscation can be achieved for very limited classes of functionalities using standard cryptographic techniques. For example, one can publish the source code of a program that checks if its input is equal to a secret password (a so-called "point function") without revealing that password: simply put in the program the image of the password under some one-way function. But being able to do the same with much more general classes of function is immensely powerful: for example, it allows to convert any symmetric key encryption scheme to public-key (just publish as "public key" the obfuscated encryption algorithm with an embedded symmetric key).

Unfortunately, as part of their study of various notions of obfuscation, Barak et al. found that the most natural notion of program obfuscation ("black-box obfuscation") is in fact impossible to achieve for general programs [BGI+01, BGI+10]. However, they also introduced weaker notions for which they could not obtain an impossibility result, including indistinguishability obfuscation, which Goldwasser and Rothblum later showed to be, in a precise technical sense, the *best possible* obfuscation [GR07].

An indistinguishability obfuscator $\mathcal{O}$ for a class $\mathscr{C}$ of circuits is a circuit transformation which is functionality-preserving (i.e. for a circuit $C \in \mathscr{C}$, $\mathcal{O}(C)$ is another circuit which agrees with C on all inputs) and guarantees that for two circuits $C_1, C_2 \in \mathscr{C}$ that are functionally equivalent (i.e. agree on all inputs), then $\mathcal{O}(C_1)$ and $\mathcal{O}(C_2)$ are computationally indistinguishable. Note that it is not immediately clear what that notion could be useful for: for example, since point functions associated with distinct passwords are inequivalent, there is no guarantee that applying an indistinguishability obfuscator to such a function will hide the password.

Nevertheless, most readers of Barak et al. and Goldwasser–Rothblum would probably have assumed that an impossibility result for indistinguishability obfuscation to be a lot more likely than an instantiation, so Garg et al.'s construction [GGH+13b] came as a great surprise. Moreover, their paper demonstrated that the notion is in fact actually extremely powerful, since it was sufficient to achieve the long-awaited construction of functional encryption. Following their work, a number of papers, such as [SW14], developed more systematic techniques to use indistinguishability obfuscation, and it is now understood to be powerful enough to construct, in the words of Bitansky and Vaikuntanathan, "almost any known cryptographic object." [BV15]

Relations between some of these notions. It is interesting to note that the more powerful notions described above, namely functional encryption and indistinguishability obfuscation, turn out to be essentially *equivalent*, and also equivalent to multilinear maps.

More precisely, as we have said, indistinguishability obfuscation (together with some standard primitives like PRFs) implies (compact, multibit) functional encryption for all circuits [GGH+13b], even with adaptive security [Wat15] (and in fact, there is a generic conversion from selective to adaptive security [ABSV15]). Conversely, (compact, multibit) functional encryption for all circuits is sufficient to achieve indistinguishability obfuscation [AJ15, BV15]. In fact, recent candidate constructions of indistinguishability obfuscation such as [LV16, Lin16, AS16] have used some form of functional encryption as an intermediate building block.

In addition, it is now known that if n-linear maps satisfying certain DDH-like security notions exist for some sufficiently large constant n (the current record is $n = 5$, obtained by Lin in [Lin16] and Ananth and Sahai in [AS16]), then indistinguishability obfuscation/function encryption exist as well. And conversely, Albrecht et al. have shown that indistinguishability obfuscation (again together with standard primitives like homomorphic encryption and NIZK) is enough to construct multilinear maps [AFH+16].

This means that constructing multilinear maps, functional encryption and indistinguishability obfuscation are equivalent goals, and future constructions could be obtained from any of those primitives.

1.5 Attacks against multilinear map constructions

If secure, we have seen that candidate constructions of multilinear maps have very interesting consequences in cryptography (and we have only touched upon a few among many). The actual security picture is far from clear, however.

Indeed, attacks have been demonstrated against all constructions so far, and we describe a number of them in details in Chapter 3. The current situation is that, due to a long series of attacks [CHL+15, CLT14, CGH+15, CFL+16, HJ16, CLLT16a], multiparty Diffie–Hellman key exchange is broken over all of the proposed candidates. In addition, a number of attacks have been demonstrated against several constructions of indistinguishability obfuscation [MSZ16a, CGH16, ADGM16, CLLT17], but not all schemes are broken yet.

We can also mention that GGH13 and CLT13 are both broken in classical subexponential time and quantum polynomial time. In the case of CLT13, it is because it relies on the hardness of factoring. In the case of GGH13, it is a consequence of recent progress on the cryptanalysis of some ideal lattice assumptions in the presence of very small noise [ABD16].

Chapter 2

Definitions and Constructions

2.1 Multilinear maps

2.1.1 The Boneh–Silverberg setting

Boneh and Silverberg introduced the notion of multilinear maps in a cryptographic setting [BS03]. The definition they adopted for their purposes was touched upon in §1.2. We recall it more formally below.

Definition 1. *Let $\mathbb{G}$ and $\mathbb{G}_T$ be cyclic groups (denoted additively), and $e\colon \mathbb{G}^\kappa \to \mathbb{G}_T$ a mapping for some integer $\kappa \geq 1$. We say that e is a* κ-linear map *(or simply a* multilinear map*) when the following conditions hold:*

1. *$\mathbb{G}$ and $\mathbb{G}_T$ are of the same prime order;*
2. *for any $a_1, \ldots, a_\kappa \in \mathbb{Z}$ and $g_1, \ldots, g_\kappa \in \mathbb{G}$, we have*

$$e(a_1 \cdot g, \ldots, a_\kappa \cdot g) = a_1 \cdots a_\kappa \cdot e(g, \ldots, g);$$

3. *if g is a generator of $\mathbb{G}$, then $e(g, \ldots, g)$ is a generator of $\mathbb{G}_T$.*

2.1.2 Efficient algorithms

Boneh and Silverberg called a multilinear map as above a *cryptographic multilinear map* when the groups $\mathbb{G}$ and $\mathbb{G}_T$ admit efficient group operations, when the map e itself is efficiently computable, and when the scheme satisfies some notion of security like the hardness of discrete logarithms in $\mathbb{G}$. Since efficiency and security are asymptotic notions, they can only make sense with respect to some instance generation algorithm.

Following [GGH12], one can capture these notions (minus the security, which can be definitely independently by a suitable game) by saying that a *multilinear map scheme* is a tuple of algorithms $(\mathsf{InstGen}, \mathsf{add}, \mathsf{neg}, \mathsf{EncTest}, \mathsf{map})$ for instance generation, group operations, membership testing and multilinear pairing, which can be described as follows.

Instance generation. $\mathsf{InstGen}(1^\lambda, 1^\kappa)$ is an efficient randomized algorithm that takes as input the security parameter λ and the multilinearity degree κ, and outputs a description of the groups $\mathbb{G}$ and $\mathbb{G}_T$, their order q, a description of the multilinear map $e\colon \mathbb{G}^\kappa \to \mathbb{G}_T$, and a string $g \in \{0,1\}^*$ encoding a generator of $\mathbb{G}$. The tuple $(\mathbb{G}, \mathbb{G}_T, q, e)$ is denoted by pp.

Membership testing. $\mathsf{EncTest}(\mathsf{pp}, b, x)$ is an efficient, deterministic algorithm that takes as input the parameters pp, a bit b and a string $x \in \{0,1\}^*$ and decides whether x is a valid representation of an element of $\mathbb{G}$ (resp. $\mathbb{G}_T$) when $b = 0$ (resp. $b = 1$). It is assumed that representations are unique, so we simply denote validity by membership: $x \in \mathbb{G}$ (resp. $x \in \mathbb{G}_T$).

Group operations. $\mathsf{add}(\mathsf{pp}, b, x, y)$ is efficient, deterministic, and returns $x + y$ when $b = 0$ and x and y are both elements of $\mathbb{G}$ (resp. $b = 1$ and $x, y \in \mathbb{G}_T$). Note that this is sufficient to efficiently compute $a \cdot x$ for $a \in \mathbb{Z}_q$ by double-and-add. Similarly, $\mathsf{neg}(\mathsf{pp}, b, x)$ computes $-x$.

Multilinear map. $\mathsf{map}(\mathsf{pp}, x_1, \ldots, x_\kappa)$ is efficient, deterministic, and returns the target group element $e(x_1, \ldots, x_\kappa) \in \mathbb{G}_T$.

2.1.3 Symmetry vs. asymmetry

The multilinear maps describe above are *symmetric* in the sense that all the source group are the same (or equivalently, are efficiently isomorphic). It is straightforward to extend the definition to multilinear maps of the form $e\colon \mathbb{G}_1 \times \cdots \times \mathbb{G}_\kappa \to \mathbb{G}_T$ where the groups $\mathbb{G}_i$ are all of the same prime order, but there does not necessarily exist efficient isomorphisms between them. That setting occurs frequently with elliptic curves (for type II and type III pairings in the sense of [GPS08]), and has been described for multilinear maps by Rothblum [Rot13].

2.2 Graded encoding schemes

As discussed in §1.3, the functionality achieved by constructions such as [GGH13a] and [CLT13a] differ from the Boneh–Silverberg definition above in at least two important aspects:

- contrary to the Boneh–Silverberg setting where elements of the source group are combined in one go to form an element of the target group, encodings are arranged in several levels, and one can pair elements at level i and level j to obtain an element at level $i + j$, and so on several times;
- a single "exponent" can be represented at a given level by many different encodings.

The corresponding notion is captured by the definition of a graded encoding system, and its algorithmic description, as presented below.

2.2.1 Graded encoding system

We recall the formal definition of a *κ-graded encoding system* from [GGH13a]. For simplicity we only consider the symmetric case below. See [GGH12, Appendix A] for the description

of a more general framework that can handle asymmetric multilinear maps and gradings with respect to more complicated monoids.

Definition 2. *A* κ-graded encoding system *for a ring* R *is a system of sets* $\mathscr{S} = \{S_v^{(\alpha)} \in \{0,1\}^* : v \in \mathbb{N}, \alpha \in R\}$*, with the following properties:*

1. *For every* $v \in \mathbb{N}$*, the sets* $\{S_v^{(\alpha)} : \alpha \in R\}$ *are disjoint.*
2. *There are binary operations* $+$ *and* $-$ *(on* $\{0,1\}^*$*) such that for every* $\alpha_1, \alpha_2 \in R$*, every* $v \in \mathbb{N}$*, and every* $u_1 \in S_v^{(a_1)}$ *and* $u_2 \in S_v^{(a_2)}$*, it holds that* $u_1 + u_2 \in S_v^{(\alpha_1+\alpha_2)}$ *and* $u_1 - u_2 \in S_v^{(\alpha_1-\alpha_2)}$ *where* $\alpha_1 + \alpha_2$ *and* $\alpha_1 - \alpha_2$ *are addition and subtraction in* R*.*
3. *There is an associative binary operation* $\times$ *(on* $\{0,1\}^*$*) such that for every* $\alpha_1, \alpha_2 \in R$*, every* v_1, v_2 *with* $0 \leq v_1 + v_2 \leq \kappa$*, and every* $u_1 \in S_{v_1}^{(\alpha_1)}$ *and* $u_2 \in S_{v_2}^{(\alpha_2)}$*, it holds that* $u_1 \times u_2 \in S_{v_1+v_2}^{(\alpha_1 \cdot \alpha_2)}$ *where* $\alpha_1 \cdot \alpha_2$ *is multiplication in* R*.*

2.2.2 Efficient procedures

We also recall the definition of the procedures for manipulating encodings. As previously we consider only the symmetric case.

Instance generation. The randomized $\mathsf{InstGen}(1^\lambda, 1^\kappa)$ takes as inputs the parameters λ and κ, and outputs $(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}})$, where pp is a description of a κ-Graded Encoding System as above, and $\mathbf{p}_{\mathrm{zt}}$ is a zero-test parameter.

Ring sampler. The randomized $\mathsf{samp}(\mathsf{pp})$ outputs a "level-zero encoding" $a \in S_0^{(\alpha)}$ for a nearly uniform element $\alpha \in_R R$. Note that the encoding a does not need to be uniform in $S_0^{(\alpha)}$.

Encoding. The (possibly randomized) $\mathsf{enc}(\mathsf{pp}, i, a)$ takes as input a level-zero encoding $a \in S_0^{(\alpha)}$ for some $\alpha \in R$ and a level $i \leq \kappa$, and outputs a level-i encoding $u \in S_i^{(\alpha)}$ for the same α.

Rerandomization. The randomized $\mathsf{reRand}(\mathsf{pp}, i, u)$ re-randomizes encodings relative to the same level i. Specifically, given an encoding $u \in S_v^{(\alpha)}$, it outputs another encoding $u' \in S_v^{(\alpha)}$. Moreover for any two $u_1, u_2 \in S_v^{(\alpha)}$, the output distributions of $\mathsf{reRand}(\mathsf{pp}, i, u_1)$ and $\mathsf{reRand}(\mathsf{pp}, i, u_2)$ are nearly the same.

Addition and negation. Given pp and two encodings relative to the same level, $u_1 \in S_i^{(\alpha_1)}$ and $u_2 \in S_i^{(\alpha_2)}$, we have $\mathsf{add}(\mathsf{pp}, u_1, u_2) \in S_i^{(\alpha_1+\alpha_2)}$ and $\mathsf{neg}(\mathsf{pp}, u_1) \in S_i^{(-\alpha_1)}$. Below we write $u_1 + u_2$ and $-u_1$ as a shorthand for applying these procedures.

Multiplication. For $u_1 \in S_i^{(\alpha_1)}$ and $u_2 \in S_j^{(\alpha_2)}$, we have $\mathsf{mul}(\mathsf{pp}, u_1, u_2) = u_1 \times u_2 \in S_{i+j}^{(\alpha_1 \cdot \alpha_2)}$.

Zero-testing. The procedure $\mathsf{isZero}(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}}, u)$ outputs 1 if $u \in S_\kappa^{(0)}$ and 0 otherwise.

Extraction. The procedure extracts a random function of ring elements from their level-κ encoding. Namely $\mathsf{ext}(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}}, u)$ outputs $s \in \{0,1\}^\lambda$, such that:

1. For any $\alpha \in R$ and $u_1, u_2 \in S_\kappa^{(\alpha)}$, $\mathsf{ext}(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}}, u_1) = \mathsf{ext}(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}}, u_2)$.
2. The distribution $\{\mathsf{ext}(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}}, u) : \alpha \in_R R, u \in S_\kappa^{(\alpha)}\}$ is nearly uniform over $\{0,1\}^\lambda$.

2.2.3 Approximate graded encodings

As pointed out in [GGH13a], actual constructions only achieve a slightly relaxed definition of isZero and ext, where isZero can still output 1 even for some non-zero encoding u with negligible probability, and ext can extract different outputs when applied to encodings of the same elements, also with negligible probability. See [GGH12, §2.2.2 and A.2] for the corresponding definitions.

2.3 Security definitions: the example of Diffie–Hellman key exchange

The sheer number of subtly or wildly different hardness assumptions used for security proofs in the field of pairing-based cryptography has been the object of many comments, for better or worse [Boy08, KM10]. Unsurprisingly, the more convoluted setting of multilinear maps and graded encoding schemes has seen the use of an even broader range of potential hard problems (see e.g. the discussion in [LV16, §1] for a discussion of the particular case of obfuscation candidates). It seems difficult, at this stage, to point to a particular security definition that could be singled out as the *correct* desirable security goal when trying to construct multilinear maps.

Nevertheless, one simple security definition has been emphasized in a number of construction papers, including [GGH13a, CLT13a, LSS14, CLT15], namely the graded encoding analogue of the decisional Diffie–Hellman assumption. Since it is so common, we recall it here, and add a few comments afterwards discussing the place of that assumption within the literature.

2.3.1 The graded decisional Diffie–Hellman problem

In their original paper [GGH13a], Garg et al. introduced the *graded decisional Diffie–Hellman* assumption (GDDH) as a security goal for graded encoding scheme. It is defined as follows (this is the definition from [LSS14], which looks slightly different from the one in [GGH13a, CLT13a], but is easily seen to be equivalent as long as reRand behaves correctly).

Consider the following procedure, parametrized by λ and κ:

1. Run $\mathsf{InstGen}(1^\lambda, 1^\kappa)$ to obtain $(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}})$.
2. Sample $a_j \leftarrow \mathsf{samp}(\mathsf{pp})$ for $0 \le j \le \kappa$.
3. Compute $u_j \leftarrow \mathsf{reRand}(\mathsf{pp}, 1, \mathsf{enc}(\mathsf{pp}, 1, a_j))$ for $0 \le j \le \kappa$.
4. Sample $b \leftarrow \mathsf{samp}(\mathsf{pp})$.

5. Compute the product encoding $u^* = a_0 \cdot \prod_{j=1}^{\kappa} u_i$ of the u_j's by repeated application of the mul procedure (encoding at level κ).
6. Set $v^{(0)} = \mathsf{reRand}(\mathsf{pp}, \kappa, u^*)$.
7. Set $v^{(1)} = \mathsf{reRand}(\mathsf{pp}, \kappa, \mathsf{enc}(\mathsf{pp}, \kappa, b))$.
8. Pick a bit β uniformly at random and set $v \leftarrow v^{(\beta)}$.

The GDDH assumption asserts that an efficient adversary receiving as input the values $(p^*, \mathbf{p}_{\mathsf{zt}}, u_0, \ldots, u_\kappa, v)$ can only guess the bit β with an advantage negligible in the security parameter λ.

Clearly, the GDDH assumption implies that the N-party key exchange protocol defined below is passively secure.

$\mathsf{Setup}(1^\lambda, 1^N)$. Output $(\mathsf{pp}, \mathbf{p}_{\mathsf{zt}}) \leftarrow \mathsf{InstGen}(1^\lambda, 1^\kappa)$ as the public parameter, with $\kappa = N-1$.

$\mathsf{Publish}(\mathsf{pp}, i)$. Each party i samples a random $c_i \leftarrow \mathsf{samp}(\mathsf{pp})$ as a secret value, and publishes as the public value the corresponding level-1 encoding, computed as $c'_i \leftarrow \mathsf{reRand}(\mathsf{pp}, 1, \mathsf{enc}(\mathsf{pp}, 1, c_i))$.

$\mathsf{KeyGen}(\mathsf{pp}, \mathbf{p}_{\mathsf{zt}}, i, c_i, \{c'_j\}_{j \neq i})$. Each party i computes $\tilde{c}_i = c_i \cdot \prod_{j \neq i} c'_j$, and uses the extraction routine to locally compute the common secret $s \leftarrow \mathsf{ext}(\mathsf{pp}, \mathbf{p}_{\mathsf{zt}}, \tilde{c}_i)$.

2.3.2 Discussion

The GDDH assumption does capture the security of multiparty key exchange (almost tautologically so!), but may not otherwise be a particularly useful security definition. The hardness assumptions under which more interesting primitives like witness encryption (e.g. in [GGSW13]) and indistinguishability obfuscation (e.g. in [PST14]) have been shown to exist are usually considerably more intricate, and not much has been done over multilinear maps with Diffie–Hellman-like assumptions. As a recent result counter to that trend, albeit in the Boneh–Silverberg setting rather than over graded encoding schemes, one can mention the surprising construction by Lin of indistinguishability obfuscation from (subexponential) DDH over 5-linear maps [Lin16].

Another issue with the GDDH assumption is that, unfortunately, proposed multilinear candidates have turned out not to satisfy it: as we will see in the next chapter, attacks have been found against multiparty Diffie–Hellman over the graded encoding schemes from [GGH13a, CLT13a] and their variants! This is of course considered a serious problem. A silver lining, however, is that GDDH is not *as basic* a problem as it sounds.

Indeed, one particular feature of the multiparty Diffie–Hellman scheme as described above is that it relies on the possibility for all users to publicly generate and rerandomize their own encodings. In contrast, in many other schemes, including witness encryption and indistinguishability obfuscation, the ability to generate encodings of new values is only used by the same user that generates the system parameters. In those settings, it is thus possible to require secret information in enc and reRand, whereas only arithmetic

operations and zero-testing/extraction remain public procedures. This leads to the definition of what Albrecht et al. call *secret-key graded encoding schemes* [ACLL15], which tend to be much more difficult to attack than Diffie–Hellman key exchange. Nevertheless, attacks have indeed been found in that setting as well (e.g. against constructions of indistinguishability obfuscation [CGH+15, MSZ16a, CLLT17]), as we will see in the next chapter.

2.4 A concrete instantiation: the CLT13 graded encoding scheme

The graded encoding schemes from [GGH13a] and [CLT13a] are very similar to each other, but a thorough presentation of GGH13 requires somewhat more background material, especially on algebraic number theory and Gaussian sampling on lattices. Therefore, for simplicity's sake, we only give a complete description of the CLT13 scheme. We refer back to §1.3 above for a conceptual-level description of GGH13, and to §2.4.3 below for a short rundown of the main differences between GGH13 and CLT13.

2.4.1 The shape of CLT13 encodings

In the "integer-based" scheme of [CLT13a], a level-k encoding of a short integer vector $\mathbf{m} = (m_i) \in \mathbb{Z}^n$ is an integer c such that for all $1 \leq i \leq n$:

$$c \equiv \frac{r_i \cdot g_i + m_i}{z^k} \pmod{p_i} \tag{2.1}$$

where the r_i's are ρ-bit random integers (specific to the encoding c), with the following secret parameters: the p_i's are η-bit prime integers, the g_i's are α-bit primes, and the denominator z is a random (invertible) integer modulo $x_0 = \prod_{i=1}^{n} p_i$. The integer c is therefore well-defined modulo x_0, where x_0 is made public. Since the p_i's must remain secret, the user cannot encode the vectors $\mathbf{m} \in \mathbb{Z}^n$ by CRT directly from (2.1); instead one includes in the public parameters a set of ℓ level-0 encodings x'_j of random vectors $\mathbf{a}_j \in \mathbb{Z}^n$, and the user can generate a random level-0 encoding by computing a random subset sum of those x'_j's.

From (2.1) we see that each integer m_i is actually defined modulo g_i. Therefore, the CLT13 scheme encodes vectors $\mathbf{m}$ from the ring $R = \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$.

2.4.2 Detailed description of CLT13

System parameters. The main parameters are the security parameter λ and the required multilinearity level $\kappa \leq \text{poly}(\lambda)$. Based on λ and κ, we choose the vector dimension n, the bit-size η of the primes p_i, the bit-size α of the primes g_i, the maximum bit-size ρ of the randomness used in encodings, and various other parameters that will be specified later; the constraints that these parameters must satisfy are described in the next section. For integers z, p we denote the reduction of z modulo p by $(z \bmod p)$ or $[z]_p$ with $-p/2 < [z]_p \leq p/2$.

Instance generation. $(\mathsf{pp}, \mathbf{p}_{\mathsf{zt}}) \leftarrow \mathsf{InstGen}(1^\lambda, 1^\kappa)$. This algorithm generates n secret random η-bit primes p_i and computes $x_0 = \prod_{i=1}^n p_i$. It then generates a random invertible integer z modulo x_0, n random α-bit prime integers g_i, and a secret matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}^{n\times\ell}$, where each component a_{ij} is randomly generated in $[0, g_i) \cap \mathbb{Z}$. It also generates an integer y, three sets of integers $\{x_j\}_{j=1}^\tau$, $\{x'_j\}_{j=1}^\ell$ and $\{\Pi_j\}_{j=1}^n$, a zero-testing vector $\mathbf{p}_{\mathsf{zt}}$, and a seed s for a strong randomness extractor; the shape of these elements is detailed below in the respective algorithms where they intervene. The parameters $\mathsf{pp} = \left(n, \eta, \alpha, \rho, \beta, \tau, \ell, y, \{x_j\}_{j=1}^\tau, \{x'_j\}_{j=1}^\ell, \{\Pi_j\}_{j=1}^n, s\right)$ and $\mathbf{p}_{\mathsf{zt}}$ are finally output and made public.

Sampling level-zero encodings. $c \leftarrow \mathsf{samp}(\mathsf{pp})$. Recall that the parameters pp contain a set of ℓ integers x'_j, where each x'_j encodes at level-0 the column vector $\mathbf{a}_j \in \mathbb{Z}^n$ of the secret matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}^{n\times\ell}$. More precisely, the integers x'_j are generated by Chinese remaindering, subject to the condition that:

$$x'_j \equiv r'_{ij} \cdot g_i + a_{ij} \pmod{p_i} \quad \text{for } 1 \le j \le \ell, \tag{2.2}$$

where the r'_{ij}'s are randomly generated in $(-2^\rho, 2^\rho) \cap \mathbb{Z}$.

Using those values x'_j, the randomized sampling algorithm $\mathsf{samp}(\mathsf{pp})$ works as follows: it samples a random binary vector $\mathbf{b} = (b_j) \in \{0,1\}^\ell$ and outputs the level-0 encoding

$$c = \sum_{j=1}^{\ell} b_j \cdot x'_j \bmod x_0.$$

From Equation (2.2), this gives $c \equiv \left(\sum_{j=1}^\ell r'_{ij} b_j\right) \cdot g_i + \sum_{j=1}^\ell a_{ij} b_j \pmod{p_i}$. As required, the output c is a level-0 encoding:

$$c \equiv r_i \cdot g_i + m_i \pmod{p_i} \tag{2.3}$$

of some vector $\mathbf{m} = \mathbf{A} \cdot \mathbf{b} \in \mathbb{Z}^n$ which is a random subset-sum of the column vectors $\mathbf{a}_j$. The sizes of the reductions $[c]_{p_i}$ are then well controlled for all i:

$$|r_i \cdot g_i + m_i| \le \ell \cdot 2^{\rho+\alpha}.$$

A left-over hash lemma argument ensures that $\mathbf{m}$ will be statistically close to uniform over $R = \mathbb{Z}_{g_1} \times \cdots \times \mathbb{Z}_{g_n}$ for suitably chosen parameters. See [CLT13a] for details.

Encodings at higher levels. $c_k \leftarrow \mathsf{enc}(\mathsf{pp}, k, c)$. To allow encoding at higher levels, a level-one random encoding of the vector $\mathbf{1}$ was published as part of the public parameters pp. That value is an integer y is generated in such a way that:

$$y \equiv \frac{r_i \cdot g_i + 1}{z} \pmod{p_i}$$

for random integers $r_i \in (-2^\rho, 2^\rho) \cap \mathbb{Z}$.

Given a level-0 encoding c of $\mathbf{m} \in \mathbb{Z}^n$ as given by (2.3), a level-1 encoding of the same $\mathbf{m}$ can be obtained by computing $c_1 = c \cdot y \bmod x_0$. Indeed, we then have:

$$c_1 \equiv \frac{r_i^{(1)} \cdot g_i + m_i}{z} \pmod{p_i} \tag{2.4}$$

for some integers $r_i^{(1)}$, and we get $|r_i^{(1)} \cdot g_i + m_i| \leq \ell \cdot 2^{2(\rho+\alpha)}$ for all i. More generally to generate a level-k encoding we compute $c_k = c_0 \cdot y^k \bmod x_0$.

Note however that this element should not be published as is, since it would then be possible to go back to the lower-level encoding c by simply dividing by y, thus inverting the multilinear map. Instead the level-1 encoding c_1 should first be re-randomized into a new level-1 encoding c_1' for the same vector $\mathbf{m}$, but whose distribution is otherwise independent of the original c. This is done with the following algorithm.

Rerandomization. $c' \leftarrow \mathsf{reRand}(\mathsf{pp}, k, c)$. To allow rerandomization of encodings at level $k = 1$, the public parameters pp contain a set of n integers Π_j which are all level-1 random encodings of zero:

$$\Pi_j \equiv \frac{\varpi_{ij} \cdot g_i}{z} \pmod{p_i} \quad \text{for } 1 \leq j \leq n.$$

The matrix $\mathbf{\Pi} = (\varpi_{ij}) \in \mathbb{Z}^{n \times n}$ is a diagonally dominant matrix generated as follows: the non-diagonal entries are randomly and independently generated in $(-2^\rho, 2^\rho) \cap \mathbb{Z}$, while the diagonal entries are randomly generated in $(n2^\rho, n2^\rho + 2^\rho) \cap \mathbb{Z}$.

The parameters pp also contain a set of τ integers x_j, each one of which is a level-1 random encoding of zero:

$$x_j \equiv \frac{r_{ij} \cdot g_i}{z} \pmod{p_i} \quad \text{for } 1 \leq j \leq \tau,$$

and where the column vectors of the matrix $(r_{ij}) \in \mathbb{Z}^{n \times \tau}$ are randomly and independently generated in the half-open parallelepiped spanned by the columns of the previous matrix $\mathbf{\Pi}$. This somewhat complicated choice is made to ensure a proper rerandomization.

Given a level-1 encoding c_1 as given by (2.4), the procedure reRand rerandomizes it by adding a random subset-sum of the x_j's and a linear combination of the Π_j's:

$$c_1' = c_1 + \sum_{j=1}^{\tau} b_j \cdot x_j + \sum_{j=1}^{n} b_j' \cdot \Pi_j \bmod x_0 \tag{2.5}$$

where $b_j \leftarrow \{0, 1\}$, and $b_j' \leftarrow [0, 2^\mu) \cap \mathbb{Z}$. One of the main technical difficulties of the construction of [CLT13a] is the proof that the distribution of c_1' is nearly independent of the input c_1 (aside from the fact that both encodings correspond to the same vector $\mathbf{m}$). This is shown using a "left-over hash lemma over lattices". We refer to the original paper for details.

Adding and multiplying encodings. It is clear that one can homomorphically add encodings. Moreover the product of κ level-1 encodings u_i can be interpreted as an

encoding of the product. Namely, given level-one encodings u_j of vectors $\mathbf{m}_j \in \mathbb{Z}^n$ for $1 \le j \le \kappa$, with $u_j \equiv (r_{ij} \cdot g_i + m_{ij})/z \pmod{p_i}$, the product

$$u = \prod_{j=1}^{\kappa} u_j \bmod x_0$$

satisfies:

$$u \equiv \frac{\prod_{j=1}^{\kappa}(r_{ij} \cdot g_i + m_{ij})}{z^\kappa} \equiv \frac{r_i \cdot g_i + \left(\prod_{j=1}^{\kappa} m_{ij}\right) \bmod g_i}{z^\kappa} \pmod{p_i}$$

for some $r_i \in \mathbb{Z}$. This is a level-κ encoding of the vector $\mathbf{m}$ obtained by componentwise product of the vectors $\mathbf{m}_j$, as long as $\prod_{j=1}^{\kappa}(r_{ij} \cdot g_i + m_{ij}) < p_i$ for all i. When computing the product of κ level-1 encodings from reRand and one level-0 encoding from samp as in multiparty Diffie–Hellman key exchange, one can easily check that $|r_i| \le (4n^2 2^{\mu+\rho+\alpha})^\kappa \cdot \ell \cdot 2^{\rho+1}$ for all i.

Zero testing. $\mathsf{isZero}(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}}, u_\kappa) \stackrel{?}{=} 0/1$. Zero testing of top level encodings is carried out with the parameter $\mathbf{p}_{\mathrm{zt}}$ obtained as follows as part of instance generation. First, an integer matrix $\mathbf{H} = (h_{ij}) \in \mathbb{Z}^{n \times n}$ is randomly generated in such a way that $\mathbf{H}$ is invertible over $\mathbb{Z}$ and both $\|\mathbf{H}^T\|_\infty \le 2^\beta$ and $\|(\mathbf{H}^{-1})^T\|_\infty \le 2^\beta$, for some parameter β; here $\|\cdot\|_\infty$ is the operator norm on $n \times n$ matrices with respect to the ℓ^∞ norm on $\mathbb{R}^n$. A technique for generating such an $\mathbf{H}$ is presented in the appendix of [CLT13b]. Then, $\mathbf{p}_{\mathrm{zt}} \in \mathbb{Z}^n$ is computed as:

$$(\mathbf{p}_{\mathrm{zt}})_j = \sum_{i=1}^{n} h_{ij} \cdot \left(z^\kappa \cdot g_i^{-1} \bmod p_i\right) \cdot \prod_{i' \ne i} p_{i'} \bmod x_0. \tag{2.6}$$

To determine whether a level-κ encoding c is an encoding of zero or not, one computes the vector $\boldsymbol{\omega} = c \cdot \mathbf{p}_{\mathrm{zt}} \bmod x_0$ and tests whether $\|\boldsymbol{\omega}\|_\infty$ is small: $\mathsf{isZero}(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}}, c)$ returns 1 if $\|\boldsymbol{\omega}\| < x_0 \cdot 2^{-\nu}$ and 0 otherwise, for some parameter ν.

The authors of [CLT13a] show that suitable choices of β and ν can ensure that this zero-testing procedure is then correct for all encodings c whose noise coefficients are appropriately bounded.

Extraction. $sk \leftarrow \mathsf{ext}(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}}, c)$. To extract a random value depending only on the vector $\mathbf{m}$ encoded in a level-κ encoding c, one proceeds as follows: multiply it by the zero-testing parameter $\mathbf{p}_{\mathrm{zt}}$ modulo x_0, collect the ν most significant bits of each of the n components of the resulting vector, and apply a strong randomness extractor (using the seed s from pp). More formally:

$$\mathsf{ext}(\mathsf{pp}, \mathbf{p}_{\mathrm{zt}}, c) = \mathsf{Extract}_s\big(\mathsf{msbs}_\nu(c \cdot \mathbf{p}_{\mathrm{zt}} \bmod x_0)\big)$$

where msbs_ν extracts the ν most significant bits of the result. If two encodings c and c' encode the same $\mathbf{m} \in \mathbb{Z}^n$, one can show (using the precise result establishing the correctness of zero-testing) that $\|(c - c') \cdot \mathbf{p}_{\mathrm{zt}} \bmod x_0\|_\infty < x_0 \cdot 2^{-\nu-\lambda}$, and therefore we expect that $\boldsymbol{\omega} = c \cdot \mathbf{p}_{\mathrm{zt}} \bmod x_0$ and $\boldsymbol{\omega}' = c' \cdot \mathbf{p}_{\mathrm{zt}} \bmod x_0$ agree on their ν most significant bits, and therefore extract to the same value. And conversely if the encoded values are distinct. We refer to [CLT13a] for the nitty-gritty details.

2.4.3 Differences with GGH13

Recall from §1.3 that the graded encoding scheme from [GGH13a] is defined over the cyclotomic ring $R = \mathbb{Z}[\mathbf{x}]/(\mathbf{x}^m + 1)$, with respect to a certain principal ideal $I = \langle \mathbf{g} \rangle$ with secret, small generator $\mathbf{g}$. A vector $\mathbf{m} \in R$ with small coefficients is encoded at level k by an element of the form:

$$\mathbf{c}_k = \frac{\mathbf{m} + \mathbf{r} \cdot \mathbf{g}}{\mathbf{z}^k} \bmod q,$$

where $\mathbf{z}$ is the secret masking element. This is essentially the same as (2.1) above.

A crucial difference, however, is the shape of the zero-testing parameter. In GGH13, it is simply of the form:

$$\mathbf{p}_{\text{zt}} = \mathbf{h} \cdot \mathbf{z}^\kappa \cdot \mathbf{g}^{-1} \bmod q$$

with $\mathbf{h}$ small. Indeed, multiplying a level-κ encoding $\mathbf{c}_\kappa$ of $\mathbf{m}$ gives:

$$\mathbf{p}_{\text{zt}} \cdot \mathbf{c}_\kappa \equiv \mathbf{h} \cdot (\mathbf{m}\mathbf{g}^{-1} + \mathbf{r}) \bmod q$$

which is small when $\mathbf{m} = 0$, but large otherwise since $\mathbf{g}^{-1}$ is expected to be of full size modulo q.

Adopting a similar zero-testing element $p_{\text{zt}} = hz^\kappa/g \bmod x_0$ in the CLT13 setting, however, *does not work*. This is because multiplying that value with a level-κ encoding c_κ yields an integer modulo x_0 whose *reductions* modulo all of the prime factors p_i of x_0 are small. But since those prime factors must be kept secret, there is no way of checking that directly. This is the reason why the vector $\mathbf{p}_{\text{zt}}$ in CLT13 has the different shape (2.6), involving extra factors of the form $\prod_{j \neq i} p_j$.

Other differences between the GGH13 and CLT13 constructions mainly reside in the technical details of how various properties of the schemes (such as correct sampling and rerandomization) are proved in both settings. And of course, they have different properties in terms of security.

2.5 GGH15 and the graph-induced approach

As mentioned in §1.3, the third main construction of multilinear maps after [GGH13a] and [CLT13a] is due to Gorbunov, Gentry and Halevi [GGH15] and differs substantially from the previous constructions even in syntactic terms. The primitive that the authors achieve is not a graded-encoding scheme, but what they call a *graph-induced encoding scheme*. In what follows, we recall the definition of that primitive, and give a description of the scheme they propose.

2.5.1 Graph-induced encoding scheme

The primitive constructed in [GGH15] is parametrized by a certain directed acyclic graph, and encodings are associated to edges (or more precisely, paths of edges) on that graph. Encodings on the same path can be combined linearly, and multiplication is permitted between encodings if and only if their associated paths are adjacent. These properties

are captured by saying that a *graph-induced encoding scheme* is a tuple (PrmGen, InstGen, Sample, Enc, add, neg, mult, ZeroTest, Extract) of efficient algorithms described as follows. These procedures are subject to some technical correctness conditions for which we refer to [GGH15]; the paper also discusses possible variants that we do not address in this document.

Parameter generation. $\mathsf{PrmGen}(1^\lambda, G)$ takes as inputs the security parameter λ and the underlying directed graph G, and outputs the global system parameters gp, including in particular the graph G, a description of the plaintext ring R, and a distribution χ over R from which plaintexts are sampled.

Instance generation. $\mathsf{InstGen}(\mathsf{gp})$ takes as inputs the system parameters and outputs the secret and public parameters sp, pp.

Ring sampler. The randomized $\mathsf{Sample}(\mathsf{pp})$ algorithm outputs an element of the plaintext ring R sampled according to the distribution χ.

Encoding. $\mathsf{Enc}(\mathsf{sp}, p, \alpha)$ takes as input the *secret* parameters, a path $p = u \rightsquigarrow v$ and a ring element $\alpha \in R$ in the range of Sample, and outputs an encoding u_p of α according to the path p.

Addition, negation and multiplication. The arithmetic procedures $\mathsf{add}(\mathsf{pp}, u_p, u'_p)$, $\mathsf{neg}(\mathsf{pp}, u_p)$ and $\mathsf{mult}(\mathsf{pp}, u_p, u'_{p'})$ are deterministic and take as input the public parameters together with some encodings.

Negation takes an encoding u_p of some $\alpha \in R$ with respect to a path p, and returns an encoding of $-\alpha$ relative to the same path p. Addition takes encodings u_p, u'_p of some $\alpha, \alpha' \in R$ with respect to the same path p, and returns an encoding of $\alpha + \alpha'$ relative to p. Finally, multiplication takes encodings u_p, $u'_{p'}$ of $\alpha, \alpha' \in R$ with respect to paths p, p' which are consecutive (i.e. $p = u \rightsquigarrow v$ and $p' = v \rightsquigarrow w$), and returns an encoding of $\alpha \cdot \alpha'$ with respect to the composed path $u \rightsquigarrow w$.

Zero-testing. The procedure $\mathsf{ZeroTest}(\mathsf{pp}, u)$ is deterministic, and decides whether a given encoding u is an encoding of 0 or not.

Extraction. The procedure $\mathsf{Extract}(\mathsf{pp}, u)$ is deterministic, and returns a λ-bit string depending only on the underlying plaintext α of the encoding u.

2.5.2 The GGH15 instantiation

We now describe the candidate graph-induced encoding scheme proposed by Gentry et al. in [GGH15]. Their paper actually describes several variants; we focus here on the commutative, ring based version, which is the one they use to achieve multiparty Diffie–Hellman key exchange.

That scheme is defined over the cyclotomic ring $R = \mathbb{Z}[\mathbf{x}]/(\mathbf{x}^n + 1)$. Plaintexts are small elements s in that ring, sampled according to a Gaussian distribution χ. Public parameters consist in particular of row vectors $\mathbf{A}_v \in R_q^m$ (where $R_q = R/qR$) associated to the vertices v of the underlying graph. An encoding of s associated with a path $u \rightsquigarrow v$ in the graph is then a matrix $\mathbf{D} \in R^{m \times m}$ with small coefficients such that:

$$\mathbf{A}_u \cdot \mathbf{D} = s \cdot \mathbf{A}_v + \mathbf{E} \pmod{q}$$

for some small error vector $\mathbf{E} \in R^m$. Such encodings $\mathbf{D}$ can be generated given some secret trapdoor information generated along with the public vectors $\mathbf{A}_v$, using classical lattice techniques [GPV08, MP12]. Formally speaking, the graph-induced encoding procedures can thus be described as follows.

Parameter generation. $\mathsf{PrmGen}(1^\lambda, G)$ computes the system parameters gp, which consist of the graph G, the description of the cyclotomic ring R, the vector dimension m, the modulus q, the plaintext Gaussian distribution χ, a dispersion parameter σ used in trapdoor sampling, and the number of most significant bits t used for zero-testing and extraction.

Instance generation. $\mathsf{InstGen}(\mathsf{gp})$ uses the trapdoor sampling algorithm of Micciancio and Peikert [MP12] to generate the vectors $\mathbf{A}_v$ for all vertices v in the underlying graph G, together with the corresponding trapdoor information τ_v. The algorithm also samples a seed and some extra information for randomness extraction. The vectors $\mathbf{A}_v$ and the extraction information form the public parameters pp, whereas the trapdoors τ_v form the secret parameters sp.

Ring sampler. The randomized $\mathsf{Sample}(\mathsf{pp})$ simply samples an element $s \in R$ according to the Gaussian distribution χ.

Encoding. $\mathsf{Enc}(\mathsf{sp}, p, s)$: to sample an encoding for $s \in R$ along the path $p = u \rightsquigarrow v$, this algorithm first samples an error vector $\mathbf{E} \in R^m$ according to χ^m, and computes $\mathbf{V} = s \cdot \mathbf{A}_v + \mathbf{E}$. It then uses the trapdoor information τ_u and the Micciancio–Peikert algorithm [MP12] to obtain a small matrix $\mathbf{D} \in R_q^{m \times m}$ such that $\mathbf{D} \cdot \mathbf{A}_u = \mathbf{V}$ over R_q. This matrix $\mathbf{D}$ is the required encoding.

Addition, negation and multiplication. Addition, negation and multiplication are the corresponding operations directly on matrices. It is easy to see that they behave as expected. Indeed, in the case of addition, if $\mathbf{D}_1$ and $\mathbf{D}_2$ are encodings of s_1, s_2 relative to the same path $u \rightsquigarrow v$, so we can write:

$$\begin{aligned} \mathbf{A}_u \cdot \mathbf{D}_1 &= s_1 \cdot \mathbf{A}_v + \mathbf{E}_1 \pmod q \\ \mathbf{A}_u \cdot \mathbf{D}_2 &= s_2 \cdot \mathbf{A}_v + \mathbf{E}_2 \pmod q \end{aligned}$$

we obtain:

$$\mathbf{A}_u \cdot (\mathbf{D}_1 + \mathbf{D}_2) = (s_1 + s_2) \cdot \mathbf{A}_v + \mathbf{E}_1 + \mathbf{E}_2 \pmod q.$$

Similarly, two encodings $\mathbf{D}_1$ and $\mathbf{D}_2$ relative to path $u \rightsquigarrow v$ and $v \rightsquigarrow w$ can be multiplied to get an encoding relative to path $u \rightsquigarrow w$. Namely given:

$$\begin{aligned} \mathbf{A}_u \cdot \mathbf{D}_1 &= s_1 \cdot \mathbf{A}_v + \mathbf{E}_1 \pmod q \\ \mathbf{A}_v \cdot \mathbf{D}_2 &= s_2 \cdot \mathbf{A}_w + \mathbf{E}_2 \pmod q \end{aligned}$$

we obtain by multiplying the matrix encodings $\mathbf{D}_1$ and $\mathbf{D}_2$:

$$\begin{aligned} \mathbf{A}_u \cdot \mathbf{D}_1 \cdot \mathbf{D}_2 &= (s_1 \cdot \mathbf{A}_v + \mathbf{E}_1) \cdot \mathbf{D}_2 \pmod q \\ &= s_1 \cdot s_2 \cdot \mathbf{A}_w + s_1 \cdot \mathbf{E}_2 + \mathbf{E}_1 \cdot \mathbf{D}_2 \pmod q \\ &= s_1 \cdot s_2 \cdot \mathbf{A}_w + \mathbf{E}' \pmod q \end{aligned}$$

for some new error vector $\mathbf{E}'$. Since s_1, $\mathbf{E}_1$, $\mathbf{E}_2$ and $\mathbf{D}_2$ have small coefficients, $\mathbf{E}'$ still has small coefficients (compared to q), and therefore the product $\mathbf{D}_1 \cdot \mathbf{D}_2$ is an encoding of $s_1 \cdot s_2$ for the path $u \rightsquigarrow w$.

Zero-testing. The procedure $\mathsf{ZeroTest}(\mathsf{pp}, \mathbf{D})$, for an encoding $\mathbf{D}$ relative to the path $u \rightsquigarrow v$, returns true if and only if $\|\mathbf{A}_u \cdot \mathbf{D}\| < q/2^{t+1}$. The justification of that procedure is that $\mathbf{A}_u \cdot \mathbf{D} = s \cdot \mathbf{A}_v + \mathbf{E}$ is small for $s = 0$, but not otherwise (because the matrix $\mathbf{A}_v$ itself is not small).

Extraction. The correctness of zero-testing shows that the t most significant bits of $\mathbf{D}$ depend only on the underlying plaintext s. Therefore, we can carry out the extraction procedure by applying a randomness extractor to those t bits.

Chapter 3

Overview of Known Attacks

3.1 Zeroizing attacks: breaking Diffie–Hellman key exchange over GGH13 and CLT13

3.1.1 Notation and attack goals

The GGH13 and CLT13 schemes share a very similar structure; here we summarize the common features that are used in the attacks:

- Each encoding is "associated" with the vector of small integers in the numerator. For GGH13 this is a 1-vector consisting of a single algebraic integer,and for CLT13 this is a vector of n integers in $\mathbb{Z}$. Below we write informally $u \sim (a_1, \ldots, a_n)$ to denote the fact that the encoding u is associated with the vector of a_i's. Roughly speaking, the goal of the attacks is to recover the vector $(a_j)_j$ from the encoding u. Recovering this vector (even if not in full) is usually considered a break of the scheme.
- An encoding of zero is associated with a vector divisible by the g_j's, namely $u \sim (g_j r_j)_j$ for some r_j's.
- Addition and multiplication of encodings acts entry-wise on the vector of integers in the numerator. Importantly, the addition and multiplication of these vectors is done *over the integers, with no modular reduction.* This is because a wrap-around in these operations is an error condition, and so the parameters are always set to ensure that it does not happen.
- If $u \sim (g_j r_j)_j$ is an encoding of zero at the top level, then applying the zero-test to u yields the integer $w = \sum_j r_j \rho_j$, where the r_j's are the multipliers from the numerator vector and the ρ_j's are system parameters independent of u.

  In other words, applying the zero-test to an encoding of zero yields the inner-product of the associated vector (without the g_j's) with a fixed secret vector. (In GGH13 this is the 1-vector (h), in CLT13 the vector is $(p_j^* h_j)_j$, where we denote $p_j^* = x_0/p_j = \prod_{i \neq j} p_i$). Importantly, here too the inner product is over the integers, with no modular reduction.

3.1.2 Weak-DL attack on GGH13 and the Hu–Jia attack

The first published attack against the GGH13 scheme appears in the original paper itself [GGH13a]. It considers the following setting. Suppose one gets a level-t encoding of zero $u_0 \sim (gr)$ and many other level-$(\kappa - t)$ encodings $u_m \sim (a_m)$. Multiplying u_0 by any of the u_m's yields a top-level encoding of zero $u_0 u_m \sim (gra_m)$, and applying the zero-test yields the algebraic integer $w_m = hra_m$. Note that this almost recovers the numerators a_m's; indeed we have them up to the common factor $h' = hr$.

If we also knew the ideal $I_g = gR$ that defines the plaintext space, then being able to recover the numerator up to a constant is enough to break many hardness assumptions. For example, given an encoded matrix we could compute its determinant (modulo I_g) up to a constant, which would tell us whether or not the encoded matrix has full rank.

Typically, however, the ideal I_g is not explicitly given. Even in that case, however, Garg et al. described how it can be recovered in certain cases using GCD computations. Roughly, we can use GCD to identify and remove the common factor h', thereby getting the a_m's themselves, except that these are all algebraic integers so we only have GCD in terms of their ideals. Recovering the ideal $I_a = aR$ is not always useful, e.g., if I_a and I_g are co-prime then knowing I_a does not tell us anything about our plaintext coset $a + I_g$. However if some of the u_i's are themselves encodings of zero, namely $a_i = gr_i$, then given enough ideals $I_{a_i} = gr_i R$ we could again use GCD calculations to recover the ideal I_g itself, and then use that knowledge to attack the non-zero encodings among the u_i's. This attack was called a "weak discrete-log attack" in [GGH13a]. It is easily seen to break the multilinear analogue of assumptions like subgroup membership: see [GGH13a, §4.2].

3.1.3 The zeroizing attack of Cheon et al.

In [CHL+15], Cheon, Han, Lee, Ryu and Stehlé describe a major extension of the GGH13 zeroizing attack, which can be used to *completely break* multiparty Diffie–Hellman key agreement over CLT13, and more generally any CLT13-based scheme in which a similar family of low-level encodings of zero are available. The attack recovers the factorization of x_0, and then all secret information.

To mount the zeroizing attack of Cheon et al. [CHL+15], one needs three sets of encoded inputs, which we denote by $\mathscr{A} = \{A_i : i = 1, \ldots, n\}$, $\mathscr{B} = \{B_0, B_1\}$, and $\mathscr{C} = \{C_j : j = 1, \ldots, n\}$ (with n the dimension of the numerator vectors). The A's are all random encoding of zeros, the B's are the target of the attack, and the C's are just helper encodings of random vectors. The levels of these encodings are such that multiplying $A_i \cdot B_\sigma \cdot C_j$ yields a top-level encoding of zero for any i, σ, j. Below we denote the numerator vectors associated with these encodings by

$$A_i \sim (g_1 r_{i,1}, \ldots, g_n r_{i,n}),\ B_\sigma \sim (b_{\sigma,1}, \ldots, b_{\sigma,n}),\ \text{and } C_j \sim (c_{j,1}, \ldots, c_{j,n}).$$

Multiplying $A_i \cdot B_\sigma \cdot C_j$ yields a top-level encoding of zero, associated with the vector $A_i \cdot B_\sigma \cdot C_j \sim (g_1 r_{i,1} b_{\sigma,1} c_{j,1}, \ldots, g_n r_{i,n} b_{\sigma,n} c_{j,n})$. Applying the zero-test we get a four-wise inner product, yielding the integer $w_\sigma[i,j] = \sum_{k=1}^{n} \rho_k r_{i,k} b_{\sigma,k} c_{j,k}$. We can write this four-wise

inner product in matrix form as

$$w_\sigma[i,j] = (r_{i,1} \ \dots \ r_{i,n}) \times \begin{pmatrix} \rho_1 b_{\sigma,1} & & \\ & \ddots & \\ & & \rho_n b_{\sigma,n} \end{pmatrix} \times \begin{bmatrix} c_{j,1} \\ \vdots \\ c_{j,n} \end{bmatrix},$$

and denote the vector on the left by $\mathbf{a}_i$, the matrix in the middle by B'_σ, and the vector on the right by $\mathbf{c}_j$. For a fixed σ, let i,j range over $1,\dots,n$. This yields an $n \times n$ matrix of integers $W_\sigma = [w_\sigma[i,j]]_{i,j} = A' \times B'_\sigma \times C'$, where A' has the $\mathbf{a}_i$'s for rows and C' has the $\mathbf{c}_j$'s for columns. Since the $r_{i,k}$'s, $b_{\sigma,k}$'s, $c_{j,k}$'s and ρ_k's are all random (small) quantities, then with high probability the matrices are all invertible (over the rationals). Having computed the matrices W_σ, the attacker now sets

$$W = W_0 \times W_1^{-1} = (A'B'_0C') \times (A'B'_1, C')^{-1} = A' \times (B'_0 \times {B'_1}^{-1}) \times {A'}^{-1}.$$

Observe now that $B^* = B'_0 \times {B'_1}^{-1}$ is a diagonal matrix with $b_{0,j}/b_{1,j}$ on the diagonal, and thus the eigenvalues of B^* are all the ratios $b_{0,j}/b_{1,j}$. And since W and B^* are similar matrices, then also the eigenvalues of W are the $b_{0,j}/b_{1,j}$'s. Hence once it computes W, the attacker can find its eigenvalues (over the rationals) and obtain all the ratios $b_{0,j}/b_{1,j}$.

These ratios may be enough by themselves to break some hardness assumptions, but for CLT13 it is possible to use them to factor x_0, thereby getting a complete break. Specifically, since each ratio is rational it can be written as $u/v = b_{0,j}/b_{1,j}$ with u,v co-prime integers. Recalling now that B_0, B_1 are two encodings at the same level (say, level t) with numerator vectors $(b_{0,1},\dots,b_{0,n})$ and $(b_{1,1},\dots,b_{1,n})$, respectively, we get that

$$uB_1 - vB_0 = [\mathrm{CRT}\,(ub_{1,1} - vb_{0,1}, \dots, ub_{1,n} - vb_{0,n})\,/z^t]_{x_0}.$$

This means that the j-th CRT component is $ub_{1,j} - vb_{0,j} = 0$, and with high probability the others are not, so we get $\gcd(x_0, uB_1 - vB_0) = p_j$.

3.1.4 The attack of Hu and Jia

The attack of Cheon et al. [CHL+15] relies crucially on the fact that CLT13 is defined over the integers, and on the fact that finding the factorization of x_0 suffices to break the scheme. These aspects have no counterpart in GGH13 setting, and therefore the attack does not apply (although it does apply to a *matrix variant* of GGH13: see [CGH+15]).

However, it turns out that the GGH13 version of multiparty Diffie–Hellman key exchange is *also* insecure. This was shown by Hu and Jia [HJ16], using another attack that expands upon the weak-DL attack above. One can sum up the attack as follows.

An eavesdropper in Diffie–Hellman key exchange sees encodings $u_i = e_i y + \rho_{i0}x_0 + \rho_{i1}x_1$, $0 \le i \le \kappa$, where x_0, x_0, y are level-1 encodings of $0,0,1$ respectively, and the e_i and ρ_{ij} are small. The secret derived by the parties is obtained from the most significant bits of $p_{\mathrm{zt}} \cdot \prod u_i$, or equivalently $h/g \cdot \prod e_i$.

The first step of Hu and Jia's attack is the weak-DL computation. Applying zero-testing to $u_i \cdot x_0 \cdot y^{\kappa-2}$, one gets:

$$v_i = p_{\mathrm{zt}} \cdot u_i \cdot x_0 \cdot y^{\kappa-2} \bmod q = e_i b_0 h + \xi_i g$$

for some small ξ_i (without modular reduction). Similarly, applying zero-testing to $x_0 \cdot y^{\kappa-1}$, one obtains:

$$\tilde{v} = p_{\text{zt}} \cdot x_0 \cdot y^{\kappa-1} \bmod q = b_0 h + \tilde{\xi} g$$

again without modular reduction. As a result, $\tilde{v}^{-1} \cdot v_i \equiv e_i \pmod{I_g}$, where I_g is the principal ideal generated by g, as above. If we denote by w_i a representative of $\tilde{v}^{-1} \cdot v_i \bmod I_g$, then the product:

$$\eta := \prod_{i=0}^{\kappa} w_i \equiv \prod_{i=0}^{\kappa} e_i \pmod{I_g}.$$

Thus, there exists some $\zeta_0 \in R$ such that $\eta = \prod e_i + \zeta g$. This element ζ, however, is not a priori small, so we cannot directly solve the problem by taking the most significant bits of η. Instead, Hu and Jia introduce some auxiliary zero-test values as follows:

$$X_i = p_{\text{zt}} \cdot x_1 x_i y^{\kappa-2} \bmod q = h(1+ag)^{\kappa-2} b_1 b_i g$$
$$Y = p_{\text{zt}} \cdot x_1 y^{\kappa-1} \bmod q = h(1+ag)^{\kappa-1} b_1 g.$$

Then $Y \cdot \eta$ is congruent to $Y \cdot \prod e_i$ modulo $b_1 g$, and since X_1 is a multiple of $b_1 g$, $\eta' = Y \cdot \eta \bmod X_0$ is also congruent to $Y \cdot \prod e_i$ modulo $b_1 g$. Thus:

$$y/x_1 \cdot \eta' \bmod q = p_{\text{zt}} \cdot y^{\kappa} \cdot \prod e_i + \zeta' \cdot (1+ag) \bmod q$$

for some small ζ'. Thus, we have computed $h/g \cdot \prod e_i +$ small error $\bmod q$, which breaks the Diffie–Hellman key exchange as required.

3.1.5 Other zeroizing attacks

Following the attack of Cheon et al. [CHL+15], several papers attempted to modify the CLT13 construction in order to protect against the attack. However, the modified variants turned out to be vulnerable to extensions of the same attack.

This includes in particular the "immunization technique" suggested by Boneh, Wu and Zimmerman [BWZ14] and the countermeasure proposed by Garg, Gentry, Halevi and Zhandry in [GGHZ14, §7], both of which can be broken by essentially extending the dimension of the matrices involved in Cheon et al.'s attack by a small factor, as described in [CLT14, CGH+15]. This also includes the CLT15 graded encoded scheme, proposed by Coron, Lepoint and Tibouchi in [CLT15], which was broken soon after it was published by Cheon, Fouque, Lee, Minaud and Ryu [CFL+16], again using a simple extension of Cheon et al.'s attack.

3.2 Graph-induced cryptanalysis: breaking GGH15 key exchange

Diffie–Hellman key exchange is also insecure over GGH15 multilinear maps. The protocol was broken by Coron, Lee, Lepoint and Tibouchi [CLLT16a], both in the basic case and when additional security defenses are implemented. Their attack also breaks the graph-induced variant of GGH13. We give a description of the basic attack below.

3.2.1 GGH15-based multiparty Diffie–Hellman

We first recall the structure of the multiparty Diffie–Hellman key exchange protocol over GGH15 [GGH15]. We consider the protocol with k users. As illustrated in Figure 3.1 for $k = 3$ users, each user i for $1 \leq i \leq k$ has a directed path of vectors $\mathbf{A}_{i,1}, \ldots, \mathbf{A}_{i,k+1}$, all sharing the same end-point $\mathbf{A}_0 = \mathbf{A}_{i,k+1}$. The i-th user will use the resulting chain to extract the session key. Each user i has a secret exponent s_i. Each secret exponent s_i will be encoded in each of the k chains; the encoding of s_i on the j-th chain for $j \neq i$ will be published, while the encoding of s_i on the i-th chain will be kept private by user i. Therefore on the i-th chain only user i will be able to compute the session key. The exponents s_i are encoded in a "round robin" fashion; namely the i-th secret s_i is encoded on the chain of user j at edge $\ell = i + j - 1$, with index arithmetic modulo k. Only the vectors $\mathbf{A}_{i,1}$ for $1 \leq i \leq k$ are made public to enable extraction of the session-key; the others are kept private.

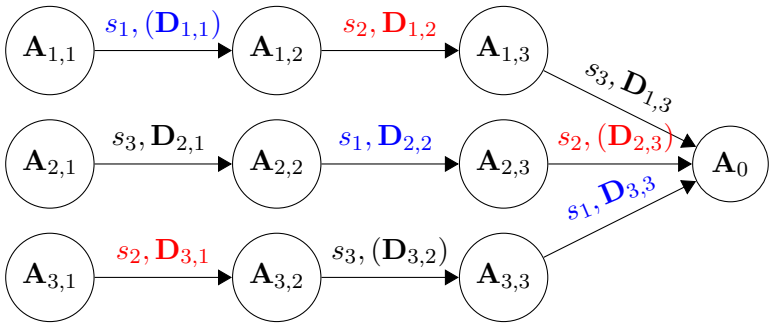


Figure 3.1: Graph of a key agreement between 3 parties for GGH15. The vertices contain random vectors $\mathbf{A}_{ij}$, and encodings are represented on the edges. Each party is represented by a different color, keeps the encoding in parenthesis secret and publishes the two other encodings.

3.2.2 The attack of Coron et al.

In [CLLT16a], Coron et al. show how an eavesdropper can recover the secret key derived by the parties in the previous protocol in polynomial time. The attack proceeds in two steps:

1. As a first step, the attacker will express one secret exponent s_1 as a linear combination of the other secret exponents $t_{1,\ell}$, using a variant of the attack of Cheon et al. [CHL+15]. However this does not immediately break the protocol, because the coefficients of the linear combination are not small.

2. In the second step, which can be seen as a generalization of the techniques of Hu and Jia [HJ16], the attacker will compute an equivalent of the private encoding of

User 1 from the previous linear combination, by correcting the error due to the large coefficients. This breaks the key-exchange protocol.

We now describe the first step in the particular case of 3 users, which illustrates the main ideas of the attack while avoiding some technical complications. We refer to [CLLT16a] for the whole details. In the 3-user case, we have the following relations:

$$\begin{aligned}
\mathbf{A}_{1,1}\cdot\mathbf{D}_{1,1} &= s_1\cdot\mathbf{A}_{1,2}+\mathbf{F}_{1,1} \pmod q\\
\mathbf{A}_{1,2}\cdot\mathbf{D}_{1,2} &= s_2\cdot\mathbf{A}_{1,3}+\mathbf{F}_{1,2} \pmod q\\
\mathbf{A}_{1,3}\cdot\mathbf{D}_{1,3} &= s_3\cdot\mathbf{A}_{0}+\mathbf{F}_{1,3} \pmod q\\
\mathbf{A}_{2,1}\cdot\mathbf{D}_{2,1} &= s_3\cdot\mathbf{A}_{2,2}+\mathbf{F}_{2,1} \pmod q\\
\mathbf{A}_{2,2}\cdot\mathbf{D}_{2,2} &= s_1\cdot\mathbf{A}_{2,3}+\mathbf{F}_{2,2} \pmod q\\
\mathbf{A}_{2,3}\cdot\mathbf{D}_{2,3} &= s_2\cdot\mathbf{A}_{0}+\mathbf{F}_{2,3} \pmod q\\
\mathbf{A}_{3,1}\cdot\mathbf{D}_{3,1} &= s_2\cdot\mathbf{A}_{3,2}+\mathbf{F}_{3,1} \pmod q\\
\mathbf{A}_{3,2}\cdot\mathbf{D}_{3,2} &= s_3\cdot\mathbf{A}_{3,3}+\mathbf{F}_{3,2} \pmod q\\
\mathbf{A}_{3,3}\cdot\mathbf{D}_{3,3} &= s_1\cdot\mathbf{A}_{0}+\mathbf{F}_{3,3} \pmod q
\end{aligned}
\qquad
\begin{aligned}
\mathbf{A}_{1,1}\cdot\mathbf{C}_{1,1,\ell} &= t_{1,\ell}\cdot\mathbf{A}_{1,2}+\mathbf{E}_{1,1,\ell} \pmod q\\
\mathbf{A}_{1,2}\cdot\mathbf{C}_{1,2,\ell} &= t_{2,\ell}\cdot\mathbf{A}_{1,3}+\mathbf{E}_{1,2,\ell} \pmod q\\
\mathbf{A}_{1,3}\cdot\mathbf{C}_{1,3,\ell} &= t_{3,\ell}\cdot\mathbf{A}_{0}+\mathbf{E}_{1,3,\ell} \pmod q\\
\mathbf{A}_{2,1}\cdot\mathbf{C}_{2,1,\ell} &= t_{3,\ell}\cdot\mathbf{A}_{2,2}+\mathbf{E}_{2,1,\ell} \pmod q\\
\mathbf{A}_{2,2}\cdot\mathbf{C}_{2,2,\ell} &= t_{1,\ell}\cdot\mathbf{A}_{2,3}+\mathbf{E}_{2,2,\ell} \pmod q\\
\mathbf{A}_{2,3}\cdot\mathbf{C}_{2,3,\ell} &= t_{2,\ell}\cdot\mathbf{A}_{0}+\mathbf{E}_{2,3,\ell} \pmod q\\
\mathbf{A}_{3,1}\cdot\mathbf{C}_{3,1,\ell} &= t_{2,\ell}\cdot\mathbf{A}_{3,2}+\mathbf{E}_{3,1,\ell} \pmod q\\
\mathbf{A}_{3,2}\cdot\mathbf{C}_{3,2,\ell} &= t_{3,\ell}\cdot\mathbf{A}_{3,3}+\mathbf{E}_{3,2,\ell} \pmod q\\
\mathbf{A}_{3,3}\cdot\mathbf{C}_{3,3,\ell} &= t_{1,\ell}\cdot\mathbf{A}_{0}+\mathbf{E}_{3,3,\ell} \pmod q
\end{aligned}$$

where all encodings $\mathbf{C}_{i,j,\ell}$ and $\mathbf{D}_{i,j}$ are public, except $\mathbf{D}_{1,1}$ which is private on Row 1, $\mathbf{D}_{2,3}$ is private on Row 2, and $\mathbf{D}_{3,2}$ is private on Row 3. The corresponding graph is illustrated in Figure 3.1. Note that on each row we have used the same index ℓ for $t_{1,\ell}$, $t_{2,\ell}$ and $t_{3,\ell}$, but on a given row one can obviously compute product of encodings for different indices.

In the first step of the attack, we show that we can express s_1 as a linear combinations of the $t_{1,\ell}$'s. For this we consider the rows 2 and 3, for which the encodings $\mathbf{D}_{2,2}$ and $\mathbf{D}_{3,3}$ corresponding to s_1 are public. In the remaining of the attack, we always consider a fixed index $\ell = 1$ for the encodings corresponding to $t_{3,\ell}$, and for simplicity we write $t_3 := t_{3,1}$, $\mathbf{C}_{1,3} := \mathbf{C}_{1,3,1}$, $\mathbf{C}_{2,1} := \mathbf{C}_{2,1,1}$ and $\mathbf{C}_{3,2} := \mathbf{C}_{3,2,1}$.

Since we always work with the same t_3, on Row 2 we define the product encodings $\hat{\mathbf{C}}_{2,2,\ell} := \mathbf{C}_{2,1}\cdot\mathbf{C}_{2,2,\ell}$, and on Row 3 we define the product encodings $\hat{\mathbf{C}}_{3,2,\ell} := \mathbf{C}_{3,1,\ell}\cdot\mathbf{C}_{3,2}$; recall that we use a fixed index for t_3. Therefore we can write:

$$\begin{aligned}
\mathbf{A}_{2,1}\cdot\hat{\mathbf{C}}_{2,2,\ell} &= t_{1,\ell}\cdot t_3\cdot\mathbf{A}_{2,3}+\hat{\mathbf{E}}_{2,2,\ell} \pmod q\\
\mathbf{A}_{2,3}\cdot\mathbf{C}_{2,3,\ell} &= t_{2,\ell}\cdot\mathbf{A}_{0}+\mathbf{E}_{2,3,\ell} \pmod q\\
\mathbf{A}_{3,1}\cdot\hat{\mathbf{C}}_{3,2,\ell} &= t_{2,\ell}\cdot t_3\cdot\mathbf{A}_{3,3}+\hat{\mathbf{E}}_{3,2,\ell} \pmod q\\
\mathbf{A}_{3,3}\cdot\mathbf{C}_{3,3,\ell} &= t_{1,\ell}\cdot\mathbf{A}_{0}+\mathbf{E}_{3,3,\ell} \pmod q
\end{aligned}
\tag{3.1}$$

for some small error vectors $\hat{\mathbf{E}}_{2,2,\ell}$ and $\hat{\mathbf{E}}_{3,2,\ell}$.

For simplicity of notations, we first consider a fixed index i for the encodings corresponding to $t_{1,i}$, and we write $t_1 := t_{1,i}$, $\hat{\mathbf{C}}_{2,2} := \hat{\mathbf{C}}_{2,2,i}$ and $\mathbf{C}_{3,3} := \mathbf{C}_{3,3,i}$. Similarly we consider a fixed index j for the encodings corresponding to $t_{2,j}$ and we write $t_2 := t_{2,j}$, $\mathbf{C}_{2,3} := \mathbf{C}_{2,3,j}$ and $\hat{\mathbf{C}}_{3,2} := \hat{\mathbf{C}}_{3,2,j}$. We use similar notations for the corresponding error vectors.

All previous equations hold modulo q only. To get a result over R instead of only modulo q, we compute the difference between two rows, for the same product of secret

exponents. More precisely, we compute:

$$\begin{aligned}\omega &= \mathbf{A}_{2,1} \cdot \hat{\mathbf{C}}_{2,2} \cdot \mathbf{C}_{2,3} - \mathbf{A}_{3,1} \cdot \hat{\mathbf{C}}_{3,2} \cdot \mathbf{C}_{3,3} \qquad (3.2)\\ &= t_1 \cdot t_3 \cdot t_2 \cdot \mathbf{A}_0 + t_1 \cdot t_3 \cdot \mathbf{E}_{2,3} + \hat{\mathbf{E}}_{2,2} \cdot \mathbf{C}_{2,3}\\ &\quad - t_2 \cdot t_3 \cdot t_1 \cdot \mathbf{A}_0 - t_2 \cdot t_3 \cdot \mathbf{E}_{3,3} - \hat{\mathbf{E}}_{3,2} \cdot \mathbf{C}_{3,3}\\ &= t_1 \cdot t_3 \cdot \mathbf{E}_{2,3} + \hat{\mathbf{E}}_{2,2} \cdot \mathbf{C}_{2,3} - t_2 \cdot t_3 \cdot \mathbf{E}_{3,3} - \hat{\mathbf{E}}_{3,2} \cdot \mathbf{C}_{3,3}\,. \qquad (3.3)\end{aligned}$$

Namely the latter equation holds over R (and not only modulo q) because all the terms in (3.3) have small coefficients; namely the only term $t_1 \cdot t_2 \cdot t_3 \cdot \mathbf{A}_0$ with large coefficients modulo q is canceled when doing the subtraction.

We have that ω is a vector of dimension m. Now an important step is to restrict ourselves to the first component of ω. Namely in order to apply the same technique as in Cheon et al.'s attack, we would like to express ω as the product of two vectors, where the left vector corresponds to User 1 and the right vector corresponds to User 2. However due to the "round-robin" fashion of exponent encodings, for this we would need to swap the product $\hat{\mathbf{E}}_{3,2} \cdot \mathbf{C}_{3,3}$ appearing in (3.3), since $\hat{\mathbf{E}}_{3,2}$ corresponds to User 2 while $\mathbf{C}_{3,3}$ corresponds to User 1; this cannot be done if we consider the full vector ω. By restricting ourselves to the first component of ω, the product $\hat{\mathbf{E}}_{3,2} \cdot \mathbf{C}_{3,3}$ becomes a simple scalar product that can be swapped; namely the scalar product of $\hat{\mathbf{E}}_{3,2}$ by the first column vector $\mathbf{C}'_{3,3}$ of the matrix $\mathbf{C}_{3,3}$. We obtain the scalar:

$$\omega = t_1 \cdot t_3 \cdot E_{2,3} + \hat{\mathbf{E}}_{2,2} \cdot \mathbf{C}'_{2,3} - t_2 \cdot t_3 \cdot E_{3,3} - \mathbf{C}'_{3,3} \cdot \hat{\mathbf{E}}_{3,2}$$

where $\mathbf{C}'_{2,3}$ and $\mathbf{C}'_{3,3}$ are the first column vectors of $\mathbf{C}_{2,3}$ and $\mathbf{C}_{3,3}$ respectively, both of dimension m; similarly $E_{2,3}$ and $E_{3,3}$ are the first components of $\mathbf{E}_{2,3}$ and $\mathbf{E}_{3,3}$ respectively.

We can now write ω as the scalar product of 2 vectors, the left one corresponding only to User 1, and the right one corresponding only to User 2:

$$\omega = \begin{bmatrix} t_1 & \hat{\mathbf{E}}_{2,2} & E_{3,3} & \mathbf{C}'_{3,3} \end{bmatrix} \cdot \begin{bmatrix} t_3 \cdot E_{2,3} \\ \mathbf{C}'_{2,3} \\ -t_2 \cdot t_3 \\ -\hat{\mathbf{E}}_{3,2} \end{bmatrix}.$$

Note that the two vectors in the product have dimension $2m + 2$.

As in the attack of Cheon et al. [CHL+15], we can now extend ω to a matrix by considering many left row vectors and many right column vectors. However instead of a square matrix as in Cheon et al.'s attack, we consider a rectangular matrix with $2m + 3$ rows and $2m + 2$ columns. In (3.2), this is done by considering $2m + 3$ public encodings $\hat{\mathbf{C}}_{2,2,i}$ and $\mathbf{C}_{3,3,i}$ corresponding to User 1, and similarly $2m + 2$ encodings $\mathbf{C}_{2,3,j}$ and $\hat{\mathbf{C}}_{3,2,j}$ corresponding to User 2, for $1 \leq i \leq 2m + 3$ and $1 \leq j \leq 2m + 2$. More precisely we compute as previously over R the following matrix elements, restricting ourselves to the first component:

$$(\mathbf{W})_{ij} = \mathbf{A}_{2,1} \cdot \hat{\mathbf{C}}_{2,2,i} \cdot \mathbf{C}'_{2,3,j} - \mathbf{A}_{3,1} \cdot \hat{\mathbf{C}}_{3,2,j} \cdot \mathbf{C}'_{3,3,i} \qquad (3.4)$$

and as previously we can write:

$$(\mathbf{W})_{ij} = \begin{bmatrix} t_{1,i} & \hat{\mathbf{E}}_{2,2,i} & E_{3,3,i} & \mathbf{C}'_{3,3,i} \end{bmatrix} \cdot \begin{bmatrix} t_3 \cdot E_{2,3,j} \\ \mathbf{C}'_{2,3,j} \\ -t_{2,j} \cdot t_3 \\ -\hat{\mathbf{E}}_{3,2,j} \end{bmatrix} .$$

We obtain a $(2m+3) \times (2m+2)$ matrix $\mathbf{W}$ with:

$$\mathbf{W} = \underbrace{\begin{bmatrix} & \cdots & \\ t_{1,i} & \hat{\mathbf{E}}_{2,2,i} \quad E_{3,3,i} \quad \mathbf{C}'_{3,3,i} & \\ & \cdots & \end{bmatrix}}_{\mathbf{A}} \cdot \underbrace{\begin{bmatrix} & t_3 \cdot E_{2,3,j} & \\ \vdots & \mathbf{C}'_{2,3,j} & \vdots \\ & -t_{2,j} \cdot t_3 & \\ & -\hat{\mathbf{E}}_{3,2,j} & \end{bmatrix}}_{\mathbf{B}}$$

where the matrix $\mathbf{A}$ has $2m+3$ rows vectors, each of dimension $2m+2$, and the matrix $\mathbf{B}$ has $2m+2$ column vectors, each of dimension $2m+2$; hence $\mathbf{B}$ is a square matrix.

By doing linear algebra, we can find a vector $\mathbf{u}$ over R of dimension $2m+3$ such that $\mathbf{u} \cdot \mathbf{W} = 0$, which gives:

$$(\mathbf{u} \cdot \mathbf{A}) \cdot \mathbf{B} = 0 .$$

Heuristically with good probability the matrix $\mathbf{B}$ is invertible, which implies:

$$\mathbf{u} \cdot \mathbf{A} = 0 .$$

Since the first column of the matrix $\mathbf{A}$ is the column vector given by the $t_{1,i}$'s, such vector $\mathbf{u}$ gives a linear relation among the secret exponents $t_{1,i}$.

Moreover, since the encodings $\mathbf{D}_{2,2}$ and $\mathbf{D}_{3,3}$ corresponding to s_1 are public, we can express s_1 as a linear combination of the $t_{1,i}$'s, over R. Namely we can define as previously the product encoding $\hat{\mathbf{D}}_{2,2} := \mathbf{C}_{2,1} \cdot \mathbf{D}_{2,2}$, with:

$$\mathbf{A}_{2,1} \cdot \hat{\mathbf{D}}_{2,2} = s_1 \cdot t_3 \cdot \mathbf{A}_{2,3} + \hat{\mathbf{F}}_{2,2} \pmod{q}$$

for some small error vector $\hat{\mathbf{F}}_{2,2}$, and we can now compute the same $(\mathbf{W})_{ij}$ as in (3.4) but with $\hat{\mathbf{D}}_{2,2}$ and $\mathbf{D}'_{3,3}$ instead of $\hat{\mathbf{C}}_{2,2,i}$ and $\mathbf{C}'_{3,3,i}$, where $\mathbf{D}'_{3,3}$ is the first column of $\mathbf{D}_{3,3}$. More precisely, we compute for all $1 \leq j \leq 2m+2$:

$$\omega_j = \mathbf{A}_{2,1} \cdot \hat{\mathbf{D}}_{2,2} \cdot \mathbf{C}'_{2,3,j} - \mathbf{A}_{3,1} \cdot \hat{\mathbf{C}}_{3,2,j} \cdot \mathbf{D}'_{3,3}$$

which gives as previously:

$$\omega_j = \begin{bmatrix} s_1 & \hat{\mathbf{F}}_{2,2} & F_{3,3} & \mathbf{D}'_{3,3} \end{bmatrix} \cdot \begin{bmatrix} t_3 \cdot E_{2,3,j} \\ \mathbf{C}'_{2,3,j} \\ -t_{2,j} \cdot t_3 \\ -\hat{\mathbf{E}}_{3,2,j} \end{bmatrix} .$$

This implies that we can replace any row vector $[t_{1,i}\ \hat{\mathbf{E}}_{2,2,i}\ E_{3,3,i}\ \mathbf{C}'_{3,3,i}]$ in the matrix $\mathbf{A}$ by the row vector:

$$[s_1\ \ \hat{\mathbf{F}}_{2,2}\ \ F_{3,3}\ \ \mathbf{D}'_{3,3}] \tag{3.5}$$

where $\mathbf{D}'_{3,3}$ is the first column of $\mathbf{D}_{3,3}$, and $F_{3,3}$ is the first component of $\mathbf{F}_{3,3}$. Using the previous technique, we can therefore obtain a linear relation between s_1 and the $t_{1,i}$'s over R. More precisely, with overwhelming probability, such a relation can be put in the form:

$$\mu \cdot s_1 = \sum_{i=1}^{2m+2} \lambda_i \cdot t_{1,i} \tag{3.6}$$

with $\mu \in \mathbb{Z}$ and $\lambda_1, \ldots, \lambda_{2m+2} \in R$. Indeed, we obtain such a relation by computing the kernel of the matrix analogous to $\mathbf{W}$ above in echelon form over the fraction field of R, which gives the kernel of the corresponding matrix $\mathbf{A}$ (assuming that $\mathbf{B}$ is invertible). Unless a minor of that matrix vanishes, which happens with only negligible probability, this gives a relation where the coefficient of s_1 is 1 and the other coefficients are in the fraction field $R \otimes_{\mathbb{Z}} \mathbb{Q}$ of R. By clearing denominators, we get an expression of the form (3.6).

Then, by considering exactly one additional $t_{1,i}$ (say $t_{1,2m+3}$) and carrying out the same computations with indices $i = 2, \ldots, 2m+3$ instead of $i = 1, \ldots, 2m+2$, we get a second relation:

$$\nu \cdot s_1 = \sum_{i=2}^{2m+3} \lambda'_i \cdot t_{1,i}\,.$$

If the integers μ and ν are relatively prime, which happens with significant probability, we can apply Bézout's identity to obtain a linear relation in R where the coefficient of s_1 is 1:

$$s_1 = \sum_{i=1}^{2m+3} \alpha_i \cdot t_{1,i}, \tag{3.7}$$

which completes this first attack step and our description.

3.3 Attacks on obfuscation

We conclude this chapter by a short discussion of proposed attacks against constructions of indistinguishability obfuscation. Since a precise description of the constructions themselves exceeds the scope of this document, we simply give a very rough idea of what the attacks can achieve and of their limitations, without any attempt to provide technical details, for which we refer to the corresponding papers.

3.3.1 Attacks against obfuscation over CLT13

Candidate constructions of indistinguishability obfuscation from multilinear maps (aside from more recent techniques via functional encryption) can be broadly divided into two types: one the one hand, obfuscation for *branching programs*, that rely on Barrington's

theorem to obfuscate circuits, and on the other hand, circuit-obfuscation constructions, that work directly on circuits. Limited attacks exist on both types of schemes when instantiated over CLT13.

Attacks on branching program obfuscation. Recall that a branching program is a collection of pairs $\mathbf{A}_{i,0}, \mathbf{A}_{i,1}$, $1 \leq i \leq t$, of $d \times d$ square matrices together with some input assignment function $\mathsf{inp}\colon \{1,\ldots,t\} \to \{1,\ldots,n\}$. It computes the Boolean function on n inputs bits given by:

$$f(x_1,\ldots,x_n) = \begin{cases} 1 & \text{if } \prod_{i=1}^{t} \mathbf{A}_{i,x_{\mathsf{inp}(i)}} = \mathbf{I}_d \\ 0 & \text{otherwise} \end{cases}.$$

Roughly speaking, branching program obfuscation candidates such as the one described by Garg et al. in [GGH+13b] work by taking such a branching program, randomizing it using Kilian's technique, increasing the dimension of the matrices with some diagonal padding, and then encoding the expanded randomized matrices element-wise using a multilinear map.

In [CGH+15], Coron et al. showed that such a construction provides the necessary data to apply the attack of Cheon et al. [CHL+15] in the particular case when the branching program has a *decomposable structure*, i.e. when the successive matrices can be divided into three groups, each depending on a different subset of input bits. This attack does not apply to actual obfuscation candidates, however, because the branching programs produced by Barrigton's theorem never have the required decomposable structure.

However, Coron, Lee, Lepoint and Tibouchi [CLLT16b, CLLT17] later showed how to dramatically expand the scope of this attack, and make it practically relevant to an actual obfuscation candidates when applied to a large class of functions. The key idea of their attack is the observation that the order of matrices in a branching program can be rearranged in an essentially arbitrary way by taking tensor products, at the cost of increasing the dimension. This can be used to force branching programs into a decomposition suitable to apply the previous attack, at least if the blow-up in matrix dimension is not too large.

As a result, they were able to break the original candidate obfuscator from [GGH+13b] when instantiated over CLT13 multilinear maps, as well as the so-called *single-input* versions of many subsequent candidate obfuscators, including [MSW14, AGIS14, PST14, BGK+14, BMSZ16], again over CLT13. A surprising feature of the attack of [CLLT16b, CLLT17] is that, assuming the existence of certain classes of pseudorandom functions computed by branching programs of short length, it can also break the obfuscator described in [GMM+16], which is proved secure in the *weak multilinear map model*, a model that was believed to capture all known classes of attacks on multilinear map constructions.

The attack of [CLLT16b, CLLT17] can only target functions satisfying a property called input-partionability, however. And soon after the attack was made public, Fernando, Rasmussen and Sahai proposed a generic countermeasure to protect against all attacks of that nature [FRS16]. It works by adding to the input of all functions a "signature structure" that prevents input-partionability.

Attacks on circuit-obfuscation. Coron et al. [CGH+15] also showed that the attack of Cheon et al. can be extended to partially break the circuit-obfuscation schemes of Zimmerman [Zim15] and Applebaum–Brakerski [AB15]. More precisely, the two papers present a "simple" scheme (which is essentially the same in both papers) and more advanced variants (which differ between the two papers). Coron et al. target the simple scheme, and show that an attack similar to Cheon at al.'s can be applied to that scheme when obfuscating simple enough circuits, such as point functions.

Note that this simple scheme uses so-called "composite-order" multilinear maps, which cannot be instantiated over GGH13, so a CLT13-based instantiation is the only possible concrete instantiation of that scheme known so far, and it is partially broken. However, the more advanced versions are not shown to be vulnerable.

3.3.2 Attacks against obfuscation over GGH13 and GGH15

Setting aside obfuscation candidates relying on composite order multilinear maps (which cannot be instantiated over GGH13), the first attack against indistinguishability obfuscators over GGH13 was the *annihilation attack* introduced by Miles, Sahai and Zhandry in [MSZ16a]. It is conceptually different from zeroizing attacks.

The attack targets a family of obfuscator that Miles et al. describe axiomatically, and that captures in particular the constructions from [MSW14, AGIS14, PST14, BGK+14, BMSZ16]. One way of describing the general idea of the attack is to note that the zero-testing values ω_i arising from the evaluation a given branching program are ring elements that can be expressed as polynomials $\sum_j f_{ij}(r_1, \ldots, r_\ell)g^j$ on the error factors r_k involved in encodings. And for a different but functionally equivalent branching program, one will find polynomials $f'_{ij} \neq f_{ij}$ in general. One can then for instance distinguish between two different but functionally equivalent branching programs by finding a polynomial relation Q between the $f_{i,0}$'s (i.e. $Q(f_{1,0}, \ldots, f_{m,0}) = 0$). Indeed, such a relation will ensure that $Q(\omega_1, \ldots, \omega_m)$ is always in the ideal I_g for the first branching program, whereas this will typically happen with only negligible probability for the second branching program, for which the polynomial relation does not hold.

The attack of [MSZ16a] even applies to the dual-input versions of the schemes mentioned above over GGH13. However, several subsequent multilinear map constructions have been proved to be secure against this class of attack [GMS16, MSZ16b].

More recently, several extensions of the attack of [MSZ16a] have been proposed. Chen, Gentry and Halevi [CGH16] show how to break the original obfuscation candidate of Garg et al. [GGH+13b] over GGH13 using annihilation attacks. They also combine the annihilation technique with the attack of [CLLT16a] to break the construction of obfuscation over GGH15 multilinear maps [GGH15]. Like [CLLT17], however, these attacks are limited to input partitionable functions, and can thus be thwarted using the techniques of [FRS16]. One can also mention the work of Apon et al. [ADGM16], which introduces an efficiently testable condition for breaking obfuscation over GGH13 using annihilation attacks, and uses it to attack a larger class of branching programs than [MSZ16a]. The constructions that are provably secure against annihilation attacks [GMS16, MSZ16b] remain unaffected, however.

Chapter 4

Conclusions and Perspectives

4.1 Status of multilinear map-based primitives

We present a snapshot of the current security status of major primitives based on multilinear maps at the time of this writing. The situation is likely to evolve rapidly, however. For an up-to-date overview of current results, we refer the reader to Martin Albrecht's excellent resource entitled "Are Graded Encoding Schemes Broken Yet?" [Alb16].

Multiparty Diffie–Hellman key exchange. Over all proposed multilinear map candidates, multiparty Diffie–Hellman key exchange is broken. Over CLT13 multilinear maps, it was broken by Cheon et al. [CHL+15], and later attempts to protect against the attack [BWZ14, GGHZ14, CLT15] were also broken by extensions of that attack [CLT14, CGH+15, CFL+16]. Over GGH13 multilinear maps, it was broken by Hu and Jia [HJ16], and that attack also applies to the optimized versions proposed in [LSS14, ACLL15]. Finally, over GGH15 multilinear maps, it was broken by Coron et al. [CLLT16a].

Indistinguishability obfuscation. Attacks have been demonstrated against *some* candidate constructions of indistinguishability obfuscation over each of GGH13, CLT13 and GGH15, but *not everything* is broken. More precisely, the annihilation attack of Miles, Sahai and Zhandry [MSZ16a] and its extensions [CGH16, ADGM16] broke almost all indistinguishability obfuscators over GGH13 existing at the time, but later on, constructions were proposed that are provably secure against it [GMS16, MSZ16b]. The zeroizing attack of Coron et al. [CLLT16b, CLLT17] broke almost all indistinguishability obfuscators over CLT13 existing at the time in the *single-input* setting. However, dual-input constructions are unaffected. Moreover, the attack only affects input-partitionable functionalities, and can thus be thwarted using the generic countermeasure of Fernando, Rasmussen and Sahai [FRS16]. Finally, Chen, Gentry and Halevi [CGH16] obtained an attack indistinguishability obfuscation over GGH15 [GGH15]. However, this attack also applies to input-partitionable functionalities only, and is thus thwarted by [FRS16].

Other primitives. No specific cryptanalytic work so far has examined the security of other multilinear map-based primitives like witness encryption. However, a reasonable expectation is that constructions relying on *secret-key* graded encodings, like witness encryption, are likely to behave similarly to indistinguishability obfuscation, whereas constructions relying on *public-key* encodings, like some constructions of ABE, are likely to fall prey to the same kind of attacks as Diffie–Hellman key exchange.

Note also that indistinguishability obfuscation is sufficient to obtain provably secure multilinear maps [AFH+16], so theoretically speaking, as long as indistinguishability obfuscation exists, everything, including multiparty Diffie–Hellman, can be instantiated securely. Of course, the efficiency of such a giant pyramid construction is guaranteed to be atrocious.

4.2 Future prospects

As we have seen, the whole multilinear map edifice is standing on shaky ground, and its security situation is quite precarious. Further progress on the cryptanalytic side is likely, and could easily bring about the unravelling of the last few remaining candidate constructions of indistinguishability obfuscation. And even if one believes that those schemes will stay secure, it is fair to say that the current situation, in which we have to rely on multilinear map constructions that were found to not even satisfy their original, basic security definition, is unsatisfactory. Progress is also being made on the construction side, however, and it could ultimately yield to much more solid foundations. This could come from several directions.

Indistinguishability obfuscation. The conditions needed to obtain indistinguishability obfuscation are becoming less and less stringent. Although early candidate constructions required multilinear maps with polynomially large degrees satisfying very strong security assumptions, this has recently been reduced to conservative assumptions over n-linear maps for n as low as 5 [Lin16, AS16]. If n could be reduced further, one might eventually be able to dispense with multilinear maps altogether and obtain everything from pairings.

Functional encryption. Compact functional encryption for relatively limited classes of functions would also suffice to obtain indistinguishability obfuscation and hence everything else. And current techniques are not very far off from achieving it from LWE [GKP+13, GVW15].

New multilinear maps. Since low-degree multilinear maps are now known to suffice for indistinguishability obfuscation, and hence essentially all applications, geometry-based techniques, which were originally ruled out by Boneh and Silverberg, might be usefully revisited, as has been done on a few occasions [RH09].

In any event, the field of multilinear maps can certainly expect many interesting developments in the months and years to come.

Bibliography

[AB15] Benny Applebaum and Zvika Brakerski. Obfuscating circuits via composite-order graded encoding. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 528–556, Warsaw, Poland, March 23–25, 2015. Springer, Heidelberg, Germany.

[ABD16] Martin R. Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretched NTRU assumptions - cryptanalysis of some FHE and graded encoding schemes. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part I*, volume 9814 of *LNCS*, pages 153–178, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Heidelberg, Germany.

[ABDP15] Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval. Simple functional encryption schemes for inner products. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 733–751, Gaithersburg, MD, USA, March 30 – April 1, 2015. Springer, Heidelberg, Germany.

[ABSV15] Prabhanjan Ananth, Zvika Brakerski, Gil Segev, and Vinod Vaikuntanathan. From selective to adaptive security in functional encryption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 657–677, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[ACLL15] Martin R. Albrecht, Catalin Cocis, Fabien Laguillaumie, and Adeline Langlois. Implementing candidate graded encoding schemes from ideal lattices. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 752–775, Auckland, New Zealand, November 30 – December 3, 2015. Springer, Heidelberg, Germany.

[ADGM16] Daniel Apon, Nico Döttling, Sanjam Garg, and Pratyay Mukherjee. Cryptanalysis of indistinguishability obfuscations of circuits over GGH13. Cryptology ePrint Archive, Report 2016/1003, 2016. http://eprint.iacr.org/2016/1003.

[AFH+16] Martin R. Albrecht, Pooya Farshim, Dennis Hofheinz, Enrique Larraia, and Kenneth G. Paterson. Multilinear maps from obfuscation. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 446–473, Tel Aviv, Israel, January 10–13, 2016. Springer, Heidelberg, Germany.

[AGIS14] Prabhanjan Vijendra Ananth, Divya Gupta, Yuval Ishai, and Amit Sahai. Optimizing obfuscation: Avoiding Barrington's theorem. In Gail-Joon Ahn, Moti Yung, and Ninghui Li, editors, *ACM CCS 14*, pages 646–658, Scottsdale, AZ, USA, November 3–7, 2014. ACM Press.

[AJ15] Prabhanjan Ananth and Abhishek Jain. Indistinguishability obfuscation from compact functional encryption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 308–326, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[AJN+16] Prabhanjan Ananth, Aayush Jain, Moni Naor, Amit Sahai, and Eylon Yogev. Universal constructions and robust combiners for indistinguishability obfuscation and witness encryption. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 491–520, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Heidelberg, Germany.

[Alb16] Martin Albrecht. Are graded encoding schemes broken yet? Regularly updated webpage, 2016. http://malb.io/are-graded-encoding-schemes-broken-yet.html.

[AS16] Prabhanjan Ananth and Amit Sahai. Projective arithmetic functional encryption and indistinguishability obfuscation from degree-5 multilinear maps. Cryptology ePrint Archive, Report 2016/1097, 2016. http://eprint.iacr.org/2016/1097.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55, Santa Barbara, CA, USA, August 15–19, 2004. Springer, Heidelberg, Germany.

[BDOP04] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 506–522, Interlaken, Switzerland, May 2–6, 2004. Springer, Heidelberg, Germany.

[BF03] Dan Boneh and Matthew K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[BGI+01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 1–18, Santa Barbara, CA, USA, August 19–23, 2001. Springer, Heidelberg, Germany.

[BGI+10] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. *Journal of the ACM*, 59(2):6:1–6:48, 2010.

[BGK+14] Boaz Barak, Sanjam Garg, Yael Tauman Kalai, Omer Paneth, and Amit Sahai. Protecting obfuscation against algebraic attacks. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 221–238, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany.

[BGN05] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In Joe Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 325–341, Cambridge, MA, USA, February 10–12, 2005. Springer, Heidelberg, Germany.

[BJK15] Allison Bishop, Abhishek Jain, and Lucas Kowalczyk. Function-hiding inner product encryption. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 470–491, Auckland, New Zealand, November 30 – December 3, 2015. Springer, Heidelberg, Germany.

[BLS04] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, September 2004.

[BMSZ16] Saikrishna Badrinarayanan, Eric Miles, Amit Sahai, and Mark Zhandry. Post-zeroizing obfuscation: New mathematical tools, and the case of evasive circuits. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 764–791, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany.

[Boy08] Xavier Boyen. The uber-assumption family (invited talk). In Steven D. Galbraith and Kenneth G. Paterson, editors, *PAIRING 2008*, volume 5209 of *LNCS*, pages 39–56, Egham, UK, September 1–3, 2008. Springer, Heidelberg, Germany.

[BS03] Dan Boneh and Alice Silverberg. Applications of multilinear forms to cryptography. *Contemporary Mathematics*, 324:71–90, 2003.

[BSW11] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 253–273, Providence, RI, USA, March 28–30, 2011. Springer, Heidelberg, Germany.

[BV15] Nir Bitansky and Vinod Vaikuntanathan. Indistinguishability obfuscation from functional encryption. In Venkatesan Guruswami, editor, *56th FOCS*, pages 171–190, Berkeley, CA, USA, October 17–20, 2015. IEEE Computer Society Press.

[BWZ14] Dan Boneh, David J. Wu, and Joe Zimmerman. Immunizing multilinear maps against zeroizing attacks. Cryptology ePrint Archive, Report 2014/930, 2014. http://eprint.iacr.org/2014/930.

[CCK+13] Jung Hee Cheon, Jean-Sébastien Coron, Jinsu Kim, Moon Sung Lee, Tancrède Lepoint, Mehdi Tibouchi, and Aaram Yun. Batch fully homomorphic encryption over the integers. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 315–335, Athens, Greece, May 26–30, 2013. Springer, Heidelberg, Germany.

[CFL+16] Jung Hee Cheon, Pierre-Alain Fouque, Changmin Lee, Brice Minaud, and Hansol Ryu. Cryptanalysis of the new CLT multilinear map over the integers. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 509–536, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany.

[CGH+15] Jean-Sébastien Coron, Craig Gentry, Shai Halevi, Tancrède Lepoint, Hemanta K. Maji, Eric Miles, Mariana Raykova, Amit Sahai, and Mehdi Tibouchi. Zeroizing without low-level zeroes: New MMAP attacks and their limitations. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 247–266, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[CGH16] Yilei Chen, Craig Gentry, and Shai Halevi. Cryptanalyses of candidate branching program obfuscators. Cryptology ePrint Archive, Report 2016/998, 2016. http://eprint.iacr.org/2016/998.

[CHL+15] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the multilinear map over the integers. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 3–12, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany.

[CLLT16a] Jean-Sébastien Coron, Moon Sung Lee, Tancrède Lepoint, and Mehdi Tibouchi. Cryptanalysis of GGH15 multilinear maps. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 607–628, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Heidelberg, Germany.

[CLLT16b] Jean-Sébastien Coron, Moon Sung Lee, Tancrède Lepoint, and Mehdi Tibouchi. Zeroizing attacks on indistinguishability obfuscation over CLT13. Cryptology ePrint Archive, Report 2016/1011, 2016. http://eprint.iacr.org/2016/1011.

[CLLT17] Jean-Sébastien Coron, Moon Sung Lee, Tancrède Lepoint, and Mehdi Tibouchi. Zeroizing attacks on indistinguishability obfuscation over CLT13. In *PKC 2017*, LNCS. Springer, Heidelberg, Germany, 2017. To appear.

[CLT13a] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 476–493, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany.

[CLT13b] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. Cryptology ePrint Archive, Report 2013/183, 2013. http://eprint.iacr.org/2013/183.

[CLT14] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Cryptanalysis of two candidate fixes of multilinear maps over the integers. Cryptology ePrint Archive, Report 2014/975, 2014. http://eprint.iacr.org/2014/975.

[CLT15] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. New multilinear maps over the integers. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 267–286, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[CS03] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, 33(1):167–226, 2003.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[ElG85] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.

[FRS16] Rex Fernando, Peter M. R. Rasmussen, and Amit Sahai. Preventing CLT zeroizing attacks on obfuscation. Cryptology ePrint Archive, Report 2016/1070, 2016. http://eprint.iacr.org/2016/1070.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 169–178, Bethesda, MD, USA, May 31 – June 2, 2009. ACM Press.

[GGH12] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. Cryptology ePrint Archive, Report 2012/610, 2012. http://eprint.iacr.org/2012/610.

[GGH13a] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 1–17, Athens, Greece, May 26–30, 2013. Springer, Heidelberg, Germany.

[GGH+13b] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional

encryption for all circuits. In *54th FOCS*, pages 40–49, Berkeley, CA, USA, October 26–29, 2013. IEEE Computer Society Press.

[GGH+13c] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. Attribute-based encryption for circuits from multilinear maps. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 479–499, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany.

[GGH15] Craig Gentry, Sergey Gorbunov, and Shai Halevi. Graph-induced multilinear maps from lattices. In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *TCC 2015, Part II*, volume 9015 of *LNCS*, pages 498–527, Warsaw, Poland, March 23–25, 2015. Springer, Heidelberg, Germany.

[GGHZ14] Sanjam Garg, Craig Gentry, Shai Halevi, and Mark Zhandry. Fully secure attribute based encryption from multilinear maps. Cryptology ePrint Archive, Report 2014/622, 2014. http://eprint.iacr.org/2014/622.

[GGHZ16] Sanjam Garg, Craig Gentry, Shai Halevi, and Mark Zhandry. Functional encryption without obfuscation. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part II*, volume 9563 of *LNCS*, pages 480–511, Tel Aviv, Israel, January 10–13, 2016. Springer, Heidelberg, Germany.

[GGSW13] Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th ACM STOC*, pages 467–476, Palo Alto, CA, USA, June 1–4, 2013. ACM Press.

[GKP+13] Shafi Goldwasser, Yael Tauman Kalai, Raluca A. Popa, Vinod Vaikuntanathan, and Nickolai Zeldovich. Reusable garbled circuits and succinct functional encryption. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th ACM STOC*, pages 555–564, Palo Alto, CA, USA, June 1–4, 2013. ACM Press.

[GLW14] Craig Gentry, Allison B. Lewko, and Brent Waters. Witness encryption from instance independent assumptions. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 426–443, Santa Barbara, CA, USA, August 17–21, 2014. Springer, Heidelberg, Germany.

[GMM+16] Sanjam Garg, Eric Miles, Pratyay Mukherjee, Amit Sahai, Akshayaram Srinivasan, and Mark Zhandry. Secure obfuscation in a weak multilinear map model. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part II*, volume 9986 of *LNCS*, pages 241–268, Beijing, China, October 31 – November 3, 2016. Springer, Heidelberg, Germany.

[GMS16] Sanjam Garg, Pratyay Mukherjee, and Akshayaram Srinivasan. Obfuscation without the vulnerabilities of multilinear maps. Cryptology ePrint Archive, Report 2016/390, 2016. http://eprint.iacr.org/2016/390.

[GPS08] Steven D. Galbraith, Kenneth G. Paterson, and Nigel P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008.

[GPSW06a] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 06*, pages 89–98, Alexandria, Virginia, USA, October 30 – November 3, 2006. ACM Press. Available as Cryptology ePrint Archive Report 2006/309.

[GPSW06b] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. Cryptology ePrint Archive, Report 2006/309, 2006. http://eprint.iacr.org/2006/309.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206, Victoria, British Columbia, Canada, May 17–20, 2008. ACM Press.

[GR07] Shafi Goldwasser and Guy N. Rothblum. On best-possible obfuscation. In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 194–213, Amsterdam, The Netherlands, February 21–24, 2007. Springer, Heidelberg, Germany.

[GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432, Istanbul, Turkey, April 13–17, 2008. Springer, Heidelberg, Germany.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 75–92, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany.

[GVW13] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *45th ACM STOC*, pages 545–554, Palo Alto, CA, USA, June 1–4, 2013. ACM Press.

[GVW15] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Predicate encryption for circuits from LWE. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 503–523, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[Ham11] Mike Hamburg. Spatial encryption. Cryptology ePrint Archive, Report 2011/389, 2011. http://eprint.iacr.org/2011/389.

[HJ16] Yupu Hu and Huiwen Jia. Cryptanalysis of GGH map. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 537–565, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany.

[Jou04] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. *Journal of Cryptology*, 17(4):263–276, September 2004.

[KM10] Neal Koblitz and Alfred Menezes. The brave new world of bodacious assumptions in cryptography. *Notices of the American Mathematical Society*, 57:357–365, 2010.

[KSW08] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 146–162, Istanbul, Turkey, April 13–17, 2008. Springer, Heidelberg, Germany.

[Lin16] Huijia Lin. Indistinguishability obfuscation from DDH on 5-linear maps and locality-5 PRGs. Cryptology ePrint Archive, Report 2016/1096, 2016. http://eprint.iacr.org/2016/1096.

[LSS14] Adeline Langlois, Damien Stehlé, and Ron Steinfeld. GGHLite: More efficient multilinear maps from ideal lattices. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 239–256, Copenhagen, Denmark, May 11–15, 2014. Springer, Heidelberg, Germany.

[LV16] Huijia Lin and Vinod Vaikuntanathan. Indistinguishability obfuscation from DDH-like assumptions on constant-degree graded encodings. In Irit Dinur, editor, *57th FOCS*, pages 11–20, New Brunswick, NJ, USA, October 9–11, 2016. IEEE Computer Society Press.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 700–718, Cambridge, UK, April 15–19, 2012. Springer, Heidelberg, Germany.

[MSW14] Eric Miles, Amit Sahai, and Mor Weiss. Protecting obfuscation against arithmetic attacks. Cryptology ePrint Archive, Report 2014/878, 2014. http://eprint.iacr.org/2014/878.

[MSZ16a] Eric Miles, Amit Sahai, and Mark Zhandry. Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over GGH13. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 629–658, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Heidelberg, Germany.

[MSZ16b] Eric Miles, Amit Sahai, and Mark Zhandry. Secure obfuscation in a weak multilinear map model: A simple construction secure against all known attacks. Cryptology ePrint Archive, Report 2016/588, 2016. http://eprint.iacr.org/2016/588.

[MVO93] Alfred Menezes, Scott A. Vanstone, and Tatsuaki Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39:1639–1646, 1993.

[NR04] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *Journal of the ACM*, 51(2):231–262, 2004.

[OT09] Tatsuaki Okamoto and Katsuyuki Takashima. Hierarchical predicate encryption for inner-products. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 214–231, Tokyo, Japan, December 6–10, 2009. Springer, Heidelberg, Germany.

[Pai99] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 223–238, Prague, Czech Republic, May 2–6, 1999. Springer, Heidelberg, Germany.

[PRV12] Periklis A. Papakonstantinou, Charles W. Rackoff, and Yevgeniy Vahlis. How powerful are the DDH hard groups? Cryptology ePrint Archive, Report 2012/653, 2012. http://eprint.iacr.org/2012/653.

[PST14] Rafael Pass, Karn Seth, and Sidharth Telang. Indistinguishability obfuscation from semantically-secure multilinear encodings. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 500–517, Santa Barbara, CA, USA, August 17–21, 2014. Springer, Heidelberg, Germany.

[RAD78] Ron L. Rivest, Leonard M. Adleman, and Michael L. Dertouzos. On data banks and privacy homomorphisms. In Richard A. DeMillo, editor, *Foundations of Secure Computation*, pages 169–180. Academic Press, 1978.

[RH09] Wayne Raskind and Ming-Deh Huang. A multilinear generalization of the Tate pairing. Talk at the Fq9 conference, University College Dublin, July 2009. https://maths.ucd.ie/~gmg/Fq9Talks/Raskind.pdf.

[Rot13] Ron Rothblum. On the circular security of bit-encryption. In Amit Sahai, editor, *TCC 2013*, volume 7785 of *LNCS*, pages 579–598, Tokyo, Japan, March 3–6, 2013. Springer, Heidelberg, Germany.

[Sch91] Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.

[SW05] Amit Sahai and Brent R. Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany.

[SW14] Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: deniable encryption, and more. In David B. Shmoys, editor, *46th ACM STOC*, pages 475–484, New York, NY, USA, May 31 – June 3, 2014. ACM Press.

[vDGHV10] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 24–43, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany.

[Wat15] Brent Waters. A punctured programming approach to adaptively secure functional encryption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 678–697, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[Zim15] Joe Zimmerman. How to obfuscate programs directly. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 439–467, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany.

付録５

学会等での主要攻撃論文発表等一覧

目次

1. 具体的な暗号の攻撃に関する発表 156
2. Eurocrypt 2016 の発表 159
2.1. Eurocrypt 2016 の発表(1 日目) 159
2.2. Eurocrypt 2016 の発表(2 日目) 159
2.3. Eurocrypt 2016 の発表(3 日目) 159
3. Crypto 2016 の発表 160
3.1. Crypto 2016 の発表(2 日目) 160
3.2. Crypto 2016 の発表(3 日目) 160
3.3. Crypto 2016 の発表(4 日目) 161
4. FDTC 2016 の発表 162
5. CHES 2016 の発表 162
5.1. CHES 2016 の発表(1 日目) 162
5.2. CHES 2016 の発表(2 日目) 163
5.3. CHES 2016 の発表(3 日目) 163
6. PROOFS 2016 の発表 163
7. IWSEC 2016 の発表 164
7.1. IWSEC 2016 の発表(2 日目) 164
8. ACM CCS 2016 の発表 164
8.1. ACM CCS 2016 の発表(1 日目) 164
9. Asiacrypt 2016 の発表 165
9.1. Asiacrypt 2016 の発表(1 日目) 165
9.2. Asiacrypt 2016 の発表(2 日目) 165
9.3. Asiacrypt 2016 の発表(3 日目) 166
10. CT-RSA 2017 の発表 166
10.1. CT-RSA 2017 の発表(1 日目) 166
10.2. CT-RSA 2017 の発表(3 日目) 166
11. FSE 2017 の発表 167
11.1. FSE 2017 の発表(1 日目) 167
11.2. FSE 2017 の発表(2 日目) 167
11.3. FSE 2017 の発表(3 日目) 168
12. PKC 2017 の発表 168
12.1. PKC 2017 の発表(2 日目) 168

1. 具体的な暗号の攻撃に関する発表

表 1 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 1 具体的な暗号の攻撃に関する発表

公開鍵暗号		頁
	Provably Weak Instances of Ring-LWE Revisited [Eurocrypt 2016]	―
	Faster Algorithms for Solving LPN [Eurocrypt 2016]	―
☆	New Complexity Trade-Offs for the (Multiple) Number Field Sieve Algorithm in Non-Prime Fields [Eurocrypt 2016]	159
	Cryptanalysis of the New CLT Multilinear Maps over the Integers [Eurocrypt 2016]	―
	Cryptanalysis of GGH Map [Eurocrypt 2016]	―
	Recovering Short Generators of Principal Ideals in Cyclotomic Rings [Eurocrypt 2016]	―
	Improved Progressive BKZ Algorithms and their Precise Cost Estimation by Sharp Simulator [Eurocrypt 2016]	―
	Practical, Predictable Lattice Basis Reduction [Eurocrypt 2016]	―
	A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and Graded Encoding Schemes [Crypto 2016]	―
	A Practical Cryptanalysis of the Algebraic Eraser [Crypto 2016]	―
	Cryptanalysis of GGH15 Multilinear Maps [Crypto 2016]	―
	Annihilation Attacks for Multilinear Maps: Cryptanalysis of Indistinguishability Obfuscation over GGH13 [Crypto 2016]	―
☆	Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case [Crypto 2016]	160
☆	A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm [Asiacrypt 2016]	165
	On the Security of Supersingular Isogeny Cryptosystems [Asiacrypt 2016]	―
	Optimization of LPN Solving Algorithms [Asiacrypt 2016]	―
	Cryptographic applications of capacity theory: On the optimality of Coppersmith's method for univariate polynomials [Asiacrypt 2016]	―
	A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors [Asiacrypt 2016]	―
	Gauss Sieve Algorithm on GPUs [CT-RSA 2017]	―
★	A Tool Kit for Partial Key Exposure Attacks on RSA [CT-RSA 2017]	166
★	Improved Key Recovery Algorithms from Noisy RSA Secret Keys with Analog Noise [CT-RSA 2017]	166
★	On the Bit Security of Elliptic Curve Diffie-Hellman [PKC 2017]	168

☆	Extended Tower Number Field Sieve with Application to Finite Fields of Arbitrary Composite Extension Degree [PKC 2017]	169
	Provably Secure NTRU Instances over Prime Cyclotomic Rings [PKC 2017]	169
ブロック暗号		**頁**
	Provable Security Evaluation of Structures against Impossible Differential and Zero Correlation Linear Cryptanalysis [Eurocrypt 2016]	—
★	Polytopic Cryptanalysis [Eurocrypt 2016]	159
	Improved Differential-Linear Cryptanalysis of 7-round Chaskey with Partitioning [Eurocrypt 2016]	—
	Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1 [Eurocrypt 2016]	—
★	A 2^{70} Attack on the Full MISTY1 [Crypto 2016]	160
★	New Insights on AES-Like SPN Ciphers [Crypto 2016]	161
☆	Another View of the Division Property [Crypto 2016]	161
★	Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks [Crypto 2016]	161
☆	On the Division Property of SIMON48 and SIMON64 [IWSEC 2016]	164
☆	On the Practical (In-)Security of 64-bit Block Ciphers Collision Attacks on HTTP over TLS and OpenVPN [ACM CCS 2016]	164
☆	Message-Recovery Attacks on Feistel-Based Format Preserving Encryption [ACM CCS 2016]	164
☆	Nonlinear Invariant Attack - Practical Attack on Full SCREAM, iSCREAM, and Midori64 [Asiacrypt 2016]	165
	Trick or Tweak: On the (In)security of OTR's Tweaks [Asiacrypt 2016]	—
☆	Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers [Asiacrypt 2016]	166
	Impossible-Differential and Boomerang Cryptanalysis of Round-Reduced Kiasu-BC [CT-RSA 2017]	—
	Optimal Differential Trails in SIMON-like Ciphers [FSE 2017]	168
ストリーム暗号		**頁**
	Cryptanalysis of the FLIP Family of Stream Ciphers [Crypto 2016]	—
	Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha [FSE 2017]	168
ハッシュ関数／メッセージ認証コード		**頁**
★	Freestart collision for full SHA-1 [Eurocrypt 2016]	159
★	Breaking Symmetric Cryptosystems using Quantum Period Finding [Crypto 2016]	162
★	Linear Structures: Applications to Cryptanalysis of Round-Reduced Keccak [Asiacrypt 2016]	165
★	The first collision for full SHA-1 [https://shattered.io/]	28
	Weak Keys for AEZ, and the External Key Padding Attack [CT-RSA 2017]	—
☆	SymSum: Symmetric-Sum Distinguishers Against Round Reduced SHA3 [FSE 2017]	167

暗号利用モード／認証暗号		頁
	Universal Forgery and Key Recovery Attacks on ELmD Authenticated Encryption Algorithm [Asiacrypt 2016]	—
	Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes [Asiacrypt 2016]	—
	Conditional Cube Attack on Round-Reduced ASCON [FSE 2017]	167
	Cube-like Attack on Round-Reduced Initialization of Ketje Sr [FSE 2017]	167
サイドチャネル攻撃		**頁**
☆	Correlated Extra-Reductions Defeat Blinded Regular Exponentiation [CHES 2016]	162
☆	CacheBleed: A Timing Attack on OpenSSL Constant Time RSA [CHES 2016]	163
	Side-Channel Analysis Protection and Low-Latency in Action - case study of PRINCE and Midori [Asiacrypt 2016]	—
	Characterisation and Estimation of the Key Rank Distribution in the Context of Side Channel Evaluations [Asiacrypt 2016]	—
	Taylor Expansion of Maximum Likelihood Attacks for Masked and Shuffled Implementations [Asiacrypt 2016]	—
	Unknown-Input Attacks in the Parallel Setting: Improving the Security of the CHES 2012 Leakage-Resilient PRF [Asiacrypt 2016]	—
	A Tale of Two Shares: Why Two-Share Threshold Implementation Seems Worthwhile–and Why it is Not [Asiacrypt 2016]	—
	A Bounded-Space Near-Optimal Key Enumeration Algorithm for Multi-subkey Side-Channel Attacks [CT-RSA 2017]	—
	Ridge-Based Profiled Differential Power Analysis [CT-RSA 2017]	—
	My Traces Learn What You Did in the Dark: Recovering Secret Signals Without Key Guesses [CT-RSA 2017]	—
故障利用攻撃		**頁**
☆	Differential fault analysis of SHA3-224 and SHA3-256 [FDTC 2016]	162
☆	A Design Methodology for Stealthy Parametric Trojans and Its Application to Bug Attacks [CHES 2016]	163
その他の攻撃		**頁**
☆	Lucky Microseconds: A Timing Attack on Amazon's s2n Implementations of TLS [Eurocrypt 2016]	159
☆	An Analysis of OpenSSL's Random Number Generator [Eurocrypt 2016]	160
☆	Backdoors in Pseudorandom Number Generators: Possibility and Impossibility Results [Crypto 2016]	160
	Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem [Crypto 2016]	—
☆	Memory-Efficient Algorithms for Finding Needles in Haystacks [Crypto 2016]	161
	Efficiently Computing Data-Independent Memory-Hard Functions [Crypto 2016]	—
	Algebraic Security Analysis of Key Generation with Physical Unclonable Functions [PROOFS 2016]	163
	Cliptography: Clipping the Power of Kleptographic Attacks [Asiacrypt 2016]	—
☆	A New Algorithm for the Unbalanced Meet-in-the-Middle Problem [Asiacrypt 2016]	166

2. Eurocrypt 2016 の発表

2.1. Eurocrypt 2016 の発表(1 日目)

Polytopic Cryptanalysis [Eurocrypt 2016]

Tyge Tiessen

差分暗号解析は、2 つの平文の違いと各々の対応する暗号文の違いとの統計的な依存関係を利用しているが、その拡張としてより多くのテキストの相互依存関係を利用する多面的暗号解析を導入した。不可能差分解析に関しては従来よりも優位性があり、縮退版 DES、および縮退版 AES に関して部分的に既存攻撃を凌ぐ結果を得た。

2.2. Eurocrypt 2016 の発表(2 日目)

New Complexity Trade-Offs for the (Multiple) Number Field Sieve Algorithm in Non-Prime Fields [Eurocrypt 2016]

Palash Sarkar and Shashank Singh

位数 $Q=p^n$, $n>1$ の有限体における数体篩法(NFS: Number Field Sieve)の新しい多項式選択アルゴリズムを提案する。$p=L_Q(2/3, c_p)$, $c_p \in [3.39, 20.91]$の場合の NFS は、他の多項式選択アルゴリズムによる NFS/MNFS(Multiple NFS: 複数数体篩)よりも小さい計算量となる。本多項式選択アルゴリズムを使用した MNFS は本多項式選択アルゴリズムを使用した NFS よりも小さい計算量となる。$c_p \in (0, 1.12] \cup [1.45, 3.15]$の場合は、本多項式選択アルゴリズムを使用した MNFS の計算量は、Conjugation を使用した MNFS の計算量と同じであり、それ以外の場合は、本多項式選択アルゴリズムを使用した MNFS の計算量は、あらゆる既存方式よりも小さくなる。

Freestart collision for full SHA-1 [Eurocrypt 2016]

Marc Stevens, Pierre Karpman and Thomas Peyrin

SHA-1 のフリースタート衝突ペアが具体的に示された。64GPU クラスタによる 10 日間の計算、およそ $2^{57.5}$ 回の圧縮関数呼び出しが攻撃に必要であった。2005 年の理論的衝突攻撃のブレークスルー以来の進歩、特に Crypto 2015 における Karpman らの 76 段 SHA-1 をより高速化するテクニックを使い、また、Eurocrypt 2013 の Stevens の最適な攻撃条件を得る結果を利用した。著者らは、産業界に SHA-1 の利用を止めるよう勧告している。

2.3. Eurocrypt 2016 の発表(3 日目)

Lucky Microseconds: A Timing Attack on Amazon's s2n Implementations of TLS [Eurocrypt 2016]

Martin R. Albrecht and Kenneth G. Paterson

s2n は 2015 年 6 月にリリースされたアマゾンによる TLS プロトコルの実装である。リリース時には、3 つの外部評価とテストを実施したと発表されたが、CBC モード暗号スイートにおいてタイミング攻撃に弱く、設定によっては平文回復につながることが示された。攻撃

は 2 つの部分からなり、第 1 の部分は s2n に実装されている Lucky 13 対策に対しても有効となる新たな版の Lucky 13 攻撃であり、第 2 の部分は、Lucky 13 に対する付加的な対策として s2n に実装されたランダム化された遅延を扱っている。

An Analysis of OpenSSL's Random Number Generator [Eurocrypt 2016]

Falko Strenzke

OpenSSL 暗号ライブラリの乱数生成における様々な脆弱性が示された。エントロピーの低い状態ではその出力に低エントロピー秘密情報を漏らす。また、状態にエントロピーを付加する関数は有効に機能せず、結果として期待されるエントロピーレベルに到達しない。更に、設計の欠陥により正しく種が与えられたとしても意図された 256 ビットのセキュリティではなく、240 ビットのエントロピーに制限されてしまう。

3. Crypto 2016 の発表

3.1. Crypto 2016 の発表(2 日目)

Backdoors in Pseudorandom Number Generators: Possibility and Impossibility Results [Crypto 2016]

Jean Paul Degabriele, Kenneth G Paterson, Jacob C. N. Schuldt and Joanne Woodage

Dodis らによる落とし戸付疑似乱数生成の設定を見直し、これまで考えられていたよりも強力な落とし戸を仕込むことができることを示した。特に、一つの生成出力が与えられれば、ビッグブラザーは初期状態、即ちすべての出力を回復することができる落とし戸付疑似乱数生成の効率的な構成を与えた。また、Dodis らの ACM-CSS 2013 の意味における、入力を持つ頑強な落とし戸付疑似乱数生成を構成した。肯定的な結果としては、状態サイズに対して比較的大きな k に対しては、ビッグブラザーは k 個以上の適切にリフレッシュされた状態を回復することは不可能であることを示した。

A 2^{70} Attack on the Full MISTY1 [Crypto 2016]

Achiya Bar-On and Nathan Keller

64 ビットブロック暗号 MISTY1 に対する鍵回復攻撃が発表された。NTT の藤堂氏の結果を改良したものであり、解読計算量は約 2^{70} にまで下がっているが、解読に必要なデータ量は 2^{64} であり、まだ現実的な脅威とは言えない。本結果は事前にプレプリントで公表されており、CRYPTREC はホームページにて解読に必要なデータ量・計算量の表および「解読に必要なデータ量が膨大であることから現実的な脅威ではないと考えられる」という見解を公表済である。

3.2. Crypto 2016 の発表(3 日目)

Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case [Crypto 2016]

Taechan Kim and Razvan Barbulescu

離散対数問題解読における多項式選択ステップの改良により、解読計算量を削減できることを示した。対象とした基礎体は中程度の大きさの素数の拡大体であり、$Q=p^n$ に対して、数体篩法の場合、計算量を $L_Q(1/3, (96/9)^{1/3})$ から $L_Q(1/3, (48/9)^{1/3})$ に下げ、複数数体篩法の場合、$L_Q(1/3, 2.15)$ から $L_Q(1/3, 1.71)$ に下げた。CRYPTREC 暗号リストで利用している素体ではないため CRYPTREC に直接的な影響はないが、ペアリング暗号等の条件に当てはまる体を利用している場合には注意が必要である。

New Insights on AES-Like SPN Ciphers [Crypto 2016]

Bing Sun, Meicheng Liu, Jian Guo, Longjiang Qu and Vincent Rijmen

本論文では S-box と MDS 行列の両方を詳しく調べることにより AES 風 SPN 暗号の識別性質に注目し安全性に関する新しい洞察を記述する。選択暗号文攻撃モードにおいて、5 ラウンド AES はランダム置換と識別可能であることを示した。本結果は秘密鍵設定における縮退 AES に対する最も長い識別であり、AES に対する 5 ラウンド識別は、選択暗号文攻撃モードにおいてのみ可能であるため、選択平文攻撃モードにおける縮退 AES のセキュリティマージンは、選択暗号文攻撃モードのそれとは異なるかもしれない。

Another View of the Division Property [Crypto 2016]

Christina Boura and Anne Canteaut

パリティ集合の概念の導入により、Eurocrypt 2015 において藤堂により導入された division 性質に対する新しいアプローチを与える。初めに、この新しい概念により、任意階の division 性質を定式化し特徴づける。次に、division 性質を一般化したパリティ集合の性質を考慮することにより、ブロック暗号の識別を構成することを検討する。最後にこのタイプの攻撃に対する Sbox の耐性を分析し、Sbox とその逆の代数的正規化との関連を示し、この攻撃に対する Sbox の設計基準を示す。

3.3. Crypto 2016 の発表(4 日目)

Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks [Crypto 2016]

Patrick Derbez and Pierre-Alain Fouque

本論文では、非常に大きなクラスのブロック暗号ーバイト指向からビット指向、SPN、Feistel、Lai-Massey ブロック暗号ーに対する最良の中間一致および不可能差分総当たりを行う一般的なアルゴリズムを記述する。これまでのツールのように、暗号の最良差分／線型パスを見つけ、これらのパスを用いた攻撃は暗号解析者に委ねるのではなく、暗号と鍵スケジュールアルゴリズムを考慮することにより、自動的に最良の攻撃を見つけるツールである。本ツールにより、AES、mCRYPTON、SIMON、IDEA、KTANTAN、PRINCE、ZORRO 等多くの攻撃を改良した。本ツールは暗号設計者がより良い解析を得るために使うことができる。

Memory-Efficient Algorithms for Finding Needles in Haystacks [Crypto 2016]

Itai Dinur, Orr Dunkelman, Nathan Keller and Adi Shamir

指数的に多い $N=2^n$ のイベントの集まり(干し草の山)の中から、興味深いイベント(針)を探す問題、特に N の干し草がほぼ一様分布であり針が非常に高い確率 $p>>1/N$ の場合を考える。探索アルゴリズムがこの分布からサンプリングすることしかできない場合、このイベン

トを見つける既知の最良時間／空間トレードオフは O(M)空間が与えられた場合 O(1/Mp^2)時間を必要とする。本論文では分布がランダムな入力にある決定的関数 f を適用して定義される状況において、もっと速く針を探索するアルゴリズムを開発する。このような分布は N 個の頂点を持ち、ほとんどすべての頂点は O(1)の祖先を持つが、探している頂点は O(pN)の祖先を持つランダム有向グラフでモデル化される。一定の空間が与えられた場合に、NestedRho と名付けた新しい探索方式を提案する。新アルゴリズムは、1/N < p < 1 において、既知最良の O(1/p^2)アルゴリズムよりも速く、$N^{-0.75}$ < p < $N^{-0.5}$の任意の p に対して、√N 因子も時間計算量を改良する。より大きな空間がある場合、並行衝突探索アルゴリズムと組み合わせることに更に時間計算量を下げることができる。

Breaking Symmetric Cryptosystems using Quantum Period Finding [Crypto 2016]

Marc Kaplan, Gaetan Leurent, Anthony Leverrier and Maria Naya-Plasencia

本論文では、攻撃者が異なる量子状態の重ね合わせにおける暗号プリミティブを実装しているクエリにアクセスできる攻撃を考える。このモデルにおいて共通鍵暗号を攻撃するために、Simon のアルゴリズムと呼ばれる(最も単純な区間探索量子アルゴリズム)量子手続きの応用を検討する。いくつかの古典的な衝突探索に基づいた攻撃は Simon のアルゴリズムにより劇的に高速化される。古典設定においては衝突探索は Ω(2$^{n/2}$)問合せが必要だが、ある隠された周期で衝突が起こるときは、量子モデルでは O(n)問合せで発見される。このセキュリティモデルにおいては、最も広く使われている認証利用モードと認証暗号（例えば、CBC-MAC、PMAC、GMAC、GCM、OCB）は完全に解読されることを示す。本攻撃は多くの CAESAR 候補(CLOC、AEZ、COPA、OTR、POET、OMD、Minalpher)にも適用可能である。Simon のアルゴリズムはスライド攻撃にも適用することができ、古典的な共通鍵暗号解析テクニックの量子モデルにおける指数的高速化につながる。

4. FDTC 2016 の発表

Differential fault analysis of SHA3-224 and SHA3-256 [FDTC 2016]

Pei Luo, Yunsi Fei, Liwei Zhang and A. Adam Ding

米国ノースイースタン大学のグループによる、米国標準ハッシュ関数 SHA3 への差分故障解析であり、シングルバイト故障モデルの提案とそれによる効率的な攻撃方法を示した。SHA-3 のダイジェスト長{224,256,384,512}のうち、SHA3-384,SHA3-512 の差分故障利用攻撃は既に発表されていたが、SHA3-224,SHA3-256 は本発表が初 (SHA3-256 は推奨候補暗号リスト掲載の暗号)。

5. CHES 2016 の発表

5.1. CHES 2016 の発表(1 日目)

Correlated Extra-Reductions Defeat Blinded Regular Exponentiation [CHES 2016]

Margaux Dugardin, Sylvain Guilley, Jean-Luc Danger, Zakaria Najm and Olivier Rioul

エクストラリダクション（extra-reduction）をサイドチャンネル情報として、べき乗剰余を用いた非対称計算に対する新しい理論的かつ実用的なサイドチャネル攻撃を示した。この攻撃は、2 つの連続したモンゴメリモジュラ乗算演算のエクストラリダクション間に存在するバイアスを利用する。論文では RSA の実装への詳細適用が示されているが、ECC の実装へも適用可であるとしている。

5.2. CHES 2016 の発表（2 日目）

CacheBleed: A Timing Attack on OpenSSL Constant Time RSA [CHES 2016]

Yuval Yarom, Daniel Genkin and Nadia Heninger

キャッシュ・タイミング攻撃に耐性をもつソフトウェア実装のテクニックである“scatter-gather”実装に対して“CacheBleed”と名付けた新たなキャッシュ・タイミング攻撃を提案している。この攻撃は、インテル社によるマイクロプロセッサのマイクロアーキテクチャである“Sandy Bridge”マイクロアーキテクチャのキャッシュバック競合（cache-bank conflict）を利用する。インテル Xeon E5-2430 上で、OpenSSL バージョン 1.0.2f のモジュラ冪剰余ルーチンの“scatter-gather ”実装に対して攻撃を行い、4096 ビット RSA に対して 16000 回の復号処理を観測することでプライベート鍵の攻撃に成功した。

5.3. CHES 2016 の発表（3 日目）

A Design Methodology for Stealthy Parametric Trojans and Its Application to Bug Attacks [CHES 2016]

Samaneh Ghandali, Georg T., Daniel Holcomb and Christof Paar

追加のロジックを必要とせず、トランジスタレベルのパラメータを操作することで、特定のターゲット回路にハードウェアのステルス型トロイの木馬を導入する手法を示した。従来とは異なり、特定のシーケンスに対して故障を発生させるトリガーベースのトロイの木馬を初めて実現した。遺伝的アルゴリズムを用いてパス上の全てのゲートに遅延を分散させ、トリガー入力がなされた時にパス遅延フォルトが発生し、他の入力に対してはタイミング基準を満たす。32 ビット乗算回路にこのステルス型トロイの木馬を適用し、Biham らによって導入されたバグ攻撃を拡張し、ECDH 鍵合意プロトコルへの攻撃を示した。

6. PROOFS 2016 の発表

Algebraic Security Analysis of Key Generation with Physical Unclonable Functions [PROOFS 2016]

Matthias Hiller, Michael Pehl, Gerhard Kramer and Georg Sigl

Physical Unclonable Function (PUF) を用いた鍵生成方法について、秘密データとヘルパーデータの生成プロセスを表す統一的な代数的表現 (algebraic core) を導入した。これを用いてこれまで提案された PUF を用いた鍵生成手法を分析し、新たなセキュリティ設計基準を提示した。このセキュリティ設計基準を満たさないアプローチはアルゴリズムレベルで秘密漏えいを発生する。

7. IWSEC 2016 の発表

7.1. IWSEC 2016 の発表(2 日目)

On the Division Property of SIMON48 and SIMON64 [IWSEC 2016]

Zejun Xiang, Wentao Zhang and Dongdai Lin

SIMON に対する Division Property を用いた integral 解析について、ビット毎独立に検討することと左半分と右半分を全体として検討することのトレードオフ（つまりは、time-memory と distinguisher の正確性のトレードオフ）を実現する新手法を提案する。SIMON の状態を細かく区切り、循環シフトと AND 演算における division property の伝播を検討する。さらに、2 つの異なる状態を選び、division property の伝播における異なる状態の影響を検討する。その結果、異なる状態は integral distinguisher の長さの大きな差につながる循環シフトにおける division property の伝播に影響を与えることが分かった。本手法を SIMON に適用することで、著者らは SIMON48 及び SIMON64 について、藤堂らの結果より 1 ラウンド改良された 12 ラウンドの distinguisher を見つけている。

8. ACM CCS 2016 の発表

8.1. ACM CCS 2016 の発表(1 日目)

On the Practical (In-)Security of 64-bit Block Ciphers Collision Attacks on HTTP over TLS and OpenVPN [ACM CCS 2016]

Karthikeyan Bhargavan and Gaetan Leurent

128ビット以上のブロックサイズを持つAESが広く使われている一方、3DES や Blowfish などの 64ビットブロック暗号も TLS, SSL, および IPsec などのプロトコルの中でいまだ多くのアルゴリズムがサポートされている。特に CBC モードを用いて利用する場合、2^{32} ブロックのデータの暗号化を行うと衝突攻撃が無視できない確率で成功してしまうことは既知のことである。しかし、このような攻撃を実際に成功させるのは難しいであろうと考えられ、実際に具体的な影響のある衝突攻撃なども示されていなかった。この論文では、具体的に攻撃が成功することを実際に示した。攻撃には 785GBのデータを要し、時間にして19-38時間を要した。これらの攻撃の実現の容易さは、RC4 が使われている場合の攻撃の容易さに比べ、それほど大きなかい離はない。攻撃を回避するためには、64ビットブロック暗号を無効にする・送信する暗号文数が、攻撃者が攻撃に必要となる暗号文数となる前に鍵を更新するなどの案が提示されている。また、この攻撃を受けての各大手ベンダの対応なども紹介された。

Message-Recovery Attacks on Feistel-Based Format Preserving Encryption [ACM CCS 2016]

Mihir Bellare, Viet Tung Hoang and Stefano Tessaro

NIST standard により提唱されている Feistel タイプの共通鍵暗号を用いた Format

Preserving Encryption に対する generic attack を示した。攻撃に際しては、この論文で提示している message-recovery security の攻撃モデルに沿い、Formal Preserving Encryption で指定されている形式に沿って実装されている Feistel タイプの共通鍵暗号に対して、left-half attack, right-half attack, full recovery attack を行った。結果、distinguisher の存在を示すのみならず、message recovery が可能となる解析方法を示した。具体的に短いサイズの message(例えば, 4bit メッセージなど) であれば完全にメッセージを推定できるとしている。攻撃には、2^{21} のサンプル(FF1 NIST standard の場合)、 2^{25} のサンプル(FFT3 NIST standard の場合) を必要とする。この解析を回避するためには、送信対象となるメッセージのビット数に対してラウンド数を増やすことであるとしている。発表者らはすでに NIST にこの結果を報告しているとのこと。

9. Asiacrypt 2016 の発表

9.1. Asiacrypt 2016 の発表(1 日目)

A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm [Asiacrypt 2016]

Palash Sarkar and Shashank Singh

Kim らが扱っていない素数べき $Q=p^n$ の場合の拡張塔数体篩法を扱い、NFS の場合 $L_Q(1/3, (64/9)^{1/3})$、MNFS の場合 $L_Q(1/3, 1.88)$を得た。これまでの最小計算量は、それぞれ $L_Q(1/3, (96/9)^{1/3})$および $L_Q(1/3, 2.12)$であった。

Linear Structures: Applications to Cryptanalysis of Round-Reduced Keccak [Asiacrypt 2016]

Jian Guo, Meicheng Liu and Ling Song

ハッシュ関数 Keccak に対して、シンガポールの Guo らは、線型構造という技術を導入し、より少ない計算量で 4 段 Keccak の原像攻撃に成功したが、フルスペックの 24 段 Keccak の安全性を脅かすには至っていない。原像攻撃の計算量は、SHAKE128 の場合 2^{106}、KECCAK-224/256 の場合、各々$2^{213/251}$ である。

9.2. Asiacrypt 2016 の発表(2 日目)

Nonlinear Invariant Attack – Practical Attack on Full SCREAM, iSCREAM, and Midori64 [Asiacrypt 2016]

Yosuke Todo, Gregor Leander and Yu Sasaki

非線型不変攻撃という新しいタイプの攻撃を導入し、SCREAM、iSCREAM、Midori64 に適用した。これらの攻撃は少数の平文-暗号文ペアと最小限の計算コストしか使用しない。ベースとなるブロック暗号への非線型不変攻撃は、CBC モードや CTR モードでの暗号文単独攻撃に拡張される。ナンス尊重モデルにおいて認証暗号 SCREAM および iSCREAM の平文は暗号文のみから回復される。弱鍵モデルにおいて、Midori64-CBC 等で、単独暗号文攻撃により平文が回復される。

9.3. Asiacrypt 2016 の発表(3 日目)

A New Algorithm for the Unbalanced Meet-in-the-Middle Problem [Asiacrypt 2016]

Ivica Nikolić and Yu Sasaki

n ビットのアンバランスな関数のペア（一方はもう一方の R 倍コストがかかる）の衝突探索は、T を時間計算量、M を空間計算量、$N=2^n$ とした時、TM=N のトレードオフに従う良く知られた標準アルゴリズムにより解かれる中間一致問題の例である。アンバランス交互配置と van Oorschot-Wiener 並行衝突探索の 2 つのアイディアを組み合わせることにより、M が R 以下であれば、$T^2M=R^2N$ に従うアルゴリズムを構成する。本アルゴリズムは、アンバランスな衝突探索において空間計算量を削減する未解決問題を解決する。

Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers [Asiacrypt 2016]

Zejun Xiang, Wentao Zhang and Zhenzhen Bao

FSE 2016 において藤堂らはビットベースの division property による攻撃を SIMON32 に適用したが、時間・メモリ計算量が大きくなるため、32 ビット以下のブロック長の暗号にしか適用することができなかった。本論文では、混合整数線型計画法を拡張し、ブロックサイズが 32 ビット以上の暗号に適用する。SIMON、SIMECK、PRESENT、RECTANGLE、Lblock、TWINE に対して攻撃を行い、SIMON32, 48, 64, 96, 128 に対して各々14-, 16-, 18, 22-, 26- 段の整識別を見つけることができた。

10. CT-RSA 2017 の発表

10.1. CT-RSA 2017 の発表(1 日目)

A Tool Kit for Partial Key Exposure Attacks on RSA [CT-RSA 2017]

Atsushi Takayasu and Noboru Kunihiro

本論文では、RSA 暗号の鍵漏洩攻撃の一般的な攻撃シナリオを定式化し、そのシナリオに対する攻撃を示す。本攻撃は Ernst らの攻撃(Eurocrypt 2005)、高安-國廣(SAC 2014、ICISC 2014)等の最先端攻撃を特別な場合として含み、Sarkar-Maitra(ICISC)、HINEK(J. Math. Cryptology 2008)等の既知の最良攻撃を凌ぐ結果を与える。本結果は一般化や既存結果より良い結果を与えるのみならず、一般的なシナリオに沿っているため RSA 変形版の安全性解析ツールキットとして、Coppersmith 法を知らなくとも使うことができる。

10.2. CT-RSA 2017 の発表(3 日目)

Improved Key Recovery Algorithms from Noisy RSA Secret Keys with Analog Noise [CT-RSA 2017]

Noboru Kunihiro and Yuki Takahashi

離散的なノイズを含む RSA の秘密鍵から元の鍵を回復する問題を考える。CHES 2014 で提

案されたノイズを含むアナログデータから鍵を回復する 2 つのアルゴリズムの内の一つは、ノイズの分布が未知でも機能するが、特にノイズの分散がアンバランスの場合には最適ではない。本論文では、分布がアンバランスなアナログノイズから秘密鍵を回復する新しいアルゴリズムを提示する。初めに一般的なアルゴリズム、およびその成功条件を示し、次に、ノイズ分布の分散が事前にわかっているという条件のもとで、アンバランスなノイズ分布に適したアルゴリズムを構築する。本アルゴリズムの成功条件を明に示し、既知の結果よりも優れている、即ちより多くのノイズが含まれている場合でも鍵を回復することを示し、最適性も示す。更に分散の値を使わない鍵回復アルゴリズムを示す。本アルゴリズムは初めに観測データから EM アルゴリズムを利用してノイズ分布の分散を見積もり、見積もった分散を基に初めのアルゴリズムから鍵を回復する。より多くのノイズを含む場合に、既存のアルゴリズムよりも鍵回復に成功することを示す。

11. FSE 2017 の発表

11.1. FSE 2017 の発表(1 日目)

SymSum: Symmetric-Sum Distinguishers Against Round Reduced SHA3 [FSE 2017]

Dhiman Saha, Sukhendu Kuila and Dipanwita Roy Chowdhury

特別に構成された入力セットに対する SHA3 のメッセージダイジェストの合計に示される大変興味深い特性を示し、それらを用いて SHA3 ファミリーの新たな Distinguisher を提案した。“SymSum”と名付けられたこの Distinguisher は SHA3 の 9 段を識別し、従来知られていた Distinguisher である“ZeroSum”よりも 4 倍ほど優れている。

11.2. FSE 2017 の発表(2 日目)

Conditional Cube Attack on Round-Reduced ASCON [FSE 2017]

Zheng Li, Xiaoyang Dong and Xiaoyun Wang

認証暗号コンペである CAESAR において第 3 ラウンド候補に進んだ ASCON への攻撃である。これまで ASCON への攻撃としては、Differential-Linear 攻撃でフルスペック 12 段中 4/5 段まで、Cube-like 攻撃でフルスペック 12 段、中 5/6 段までの攻撃が知られていた。著者らは Huang らが提案した条件付きキューブ攻撃を一般化し、フルスペック 12 段中、7 段の攻撃まで成功した。鍵サイズ 128 ビットに対して 7 段で $2^{103.9}$ の計算時間で、更に弱鍵であれば 2^{77} の計算時間まで削減可能である。ただし、いずれもフルスペック 12 段の ASCON への脅威とは至っていない。

Cube-like Attack on Round-Reduced Initialization of Ketje Sr [FSE 2017]

Xiaoyang Dong, Zheng Li, Xiaoyun Wang and Ling Qin

Keccak ベースの認証暗号 Ketje Sr への Cube-like 攻撃を行った。Ketje Sr は、認証暗号コンペである CAESAR において第 3 ラウンド候補まで進んだ Ketje の第一推奨である。攻撃の結果、7 段の Ketje Sr v1 と v2（v2 は CAESAR の第 3 ラウンドコンペで示された版）に

対して、それぞれ 2^{117}、2^{97} の計算量で攻撃可能であることを示した（v1 より v2 の方が弱くなっている)。その他、Ketje Jr v1,v2 や Ketje Minor/Major v1,v2 などの攻撃も試みている。ただし、いずれもフルスペック 13 段に対しての脅威とは至っていない。

11.3. FSE 2017 の発表(3 日目)

Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha [FSE 2017]

Arka Rai Choudhuri and Subhamoy Maitra

Salsa は eSTREAM コンペに提案された 20 段／256 ビット鍵のストリーム暗号で、12 段の短縮版も存在する。ChaCha は Salsa の一つのバリアントで 20 段／256 ビット鍵のストリーム暗号であり、ChaCha20-Poly1305 AEAD が TLS1.3 で採用されようとしている。Salsa、ChaCha はこれまで各々20 段中、8 段、7 段までの攻撃が成功していたが、この論文ではある種の差分-線形攻撃によって解読成功段数は伸ばすことができていないが、解読に必要な計算時間の削減に成功した。

Optimal Differential Trails in SIMON-like Ciphers [FSE 2017]

Zhengbin Liu, Yongqiang Li and Mingsheng Wang

SIMON-like なブロック暗号の最適な差分軌跡（Trails）を探索するアルゴリズムを提案している。まず SIMON-like なラウンド関数の差分確率のより正確な上界を示した。これに基づき、松井による探索アルゴリズムを応用し、最適な差分軌跡の探索アルゴリズムを提案している。提案探索アルゴリズムにより、SIMON32/48/64/96/128 の 12/16/19/28/37 段の最適な差分軌跡（Differential trails）の確率を示した（各々、2^{-34}、2^{-50}、2^{-64}、2^{-96}、2^{-128}）。同様に SIMON のバリアントである SIMECK についての最適な差分軌跡の確率示すと共に、SIMON、SIMECK の差分（Differentials）の確率も示した。

12. PKC 2017 の発表

12.1. PKC 2017 の発表(2 日目)

On the Bit Security of Elliptic Curve Diffie–Hellman［PKC 2017］

Barak Shani

素体上で定義された楕円曲線の楕円 Diffie-Hellman 鍵交換プロトコルのビットセキュリティを初めて示した。Diffie-Hellman 鍵の x 座標の最上位ビットの約 5/6 を求める計算量と、鍵全体を求める計算量が同等であることを示した。また 5/6 の下位ビットについても同様の結果を示した。これらは楕円曲線 HNP(Elliptic curve Hidden Number Problem)より導かれる。また拡大体上の楕円曲線について既知の手法を改善し、Diffie-Hellman 鍵の x 座標または y 座標の 1 成分を（基礎体において）計算することは、鍵全体を求める計算量と同等であることを示した。

Extended Tower Number Field Sieve with Application to Finite Fields of Arbitrary Composite Extension Degree [PKC 2017]

Taechan Kim and Jinhyuck Jeong

Crypto 2016でKim、Barbulescuによって示されたexTNFS （Extended tower number field sieve）アルゴリズムの一般化を提案している。exTNFSは有限体F(Q)（p ： 素数, $Q=p^n$）に対しての離散対数問題を計算する最先端アルゴリズムであり、$n = \eta\kappa$、gcd（η, κ）＝1の時に適用されるが、一般化により最良の漸近複雑度を維持しつつ任意の合成数nに対して適用可能とした。nが合成数の時、離散対数をL_Q（1/3, 1.71）で計算できることを示した。これはAsiacrypt 2016でSarkar、Singhによって示されたnが2のべき乗の合成数の時の最速値L_Q（1/3, 1.88）より速くなっている。

Provably Secure NTRU Instances over Prime Cyclotomic Rings [PKC 2017]

Yang Yu, Guangwu Xu and Xiaoyun Wang

格子暗号 NTRUEncrypt は IEEE で標準化されているが、古典的な NTRUEncrypt は強力な安全性の保証がなかった。Eurocrypt 2011 で Stehlé と Steinfeld が NTRUEncrypt の変形を提案したが、環 Z［X］/（$X^n + 1$）の n が 2 のべき乗に限定される等の制限があった。この論文では環の選択に、より柔軟性をもつものとして、n を奇素数とする素数円環（Prime Cyclotomic Ring)、すなわち Z［X］/（$X^{n-1}+\cdots+ X + 1$）とし、標準モデルで IND-CPA の安全性をもつ変形 NTRUEncrypt を示した。

CRYPTREC Report 2016
(暗号技術評価委員会報告 CRYPTREC-RP-0002-2016)

発行日　2017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
（サイバー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
（技術本部 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