CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術評価委員会
暗号技術調査ワーキンググループ
（暗号解析評価）
活動報告

主査　高木 剛
九州大学
マス・フォア・インダストリ研究所
http://imi.kyushu-u.ac.jp/~takagi/

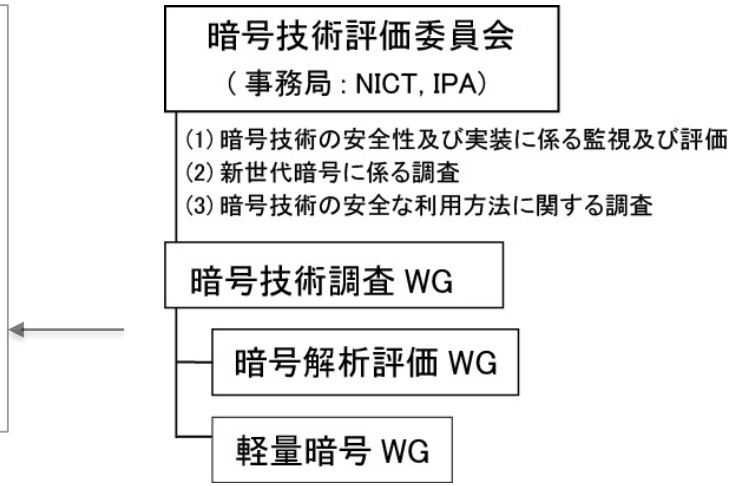
KYUSHU UNIVERSITY

Institute of Mathematics for Industry
Kyushu University

本ワーキンググループの目的

- 今日、公開鍵暗号の安全性をささえている数学的問題にはさまざまなものがある。
- このような数学的問題に関する調査を行うのが、本ワーキンググループの主目的である。

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



公開鍵暗号の歴史

RSA暗号 (素因数分解問題)

広く普及

楕円曲線暗号 (離散対数問題)

ペアリング暗号 (クラウド時代向けの暗号)

標準化、製品化

ポスト量子暗号 (格子理論, 多変数多項式,符号理論)

完全準同型暗号, 多重線形性暗号, 難読化

研究段階

2013～2014年度調査対象

- 現在、格子理論等において研究が進んでいるものの中から、代表的なものを選び、調査レポートを作成した。
  - 最短ベクトル問題(SVP, Shortest Vector Problem)
  - LWE(Learning With Errors)問題
  - LPN(Learning Parity with Noise)問題
  - ACD(Approximate Common Divisor)問題
- これらは、CRYPTRECシンポジウム2015にて紹介済み。

2015～2016年度調査対象

- 現在、下記の項目について近年の研究動向について調査する計画。
  - 多重線形写像及び難読化
  - 楕円曲線上の離散対数問題に対する指数計算法
  - その他
    - 予測図の更新

多重線形写像及び難読化
(multi linear map & obfuscation)

多重線形写像の将来性

さまざまな応用アプリケーションを実現し得る、
今後重要となる技術の一つと考えられる。

[応用例]

- **Obfuscation**
- One-round n-way DH key exchange protocol
- Verifiable pseudo random functions
- Unique Signature
- Witness Encryption
- Authenticated data structures
- Functional Encryption
- Efficient Aggregate and Verifiably Encrypted Signatures
- Efficient Broadcast encryption

など

難読化のアプリケーション と具体的構成

従来の暗号技術のみでは、
達成することが困難であった
アプリケーションを提供することが可能になる。
例えば、
〇ソフトウェアのバグ等に関するパッチを
　内部の処理を秘匿したまま安全に配布することが出来る
〇**複数**の仲間が**同時**に安全に鍵を共有することが出来る
など

具体的な構成方法などについて外部評価を実施
依頼先：**Sanjam Garg 准教授** (UCバークレー大学, 米国)
レポート詳細は、HP 参照
http://www.cryptrec.go.jp/estimation.html

多重線形写像の今後の課題

安全性の解析が求められている

- 安全性に求められる要件
- 攻撃モデル
- 具体的な構成方法の安全性証明

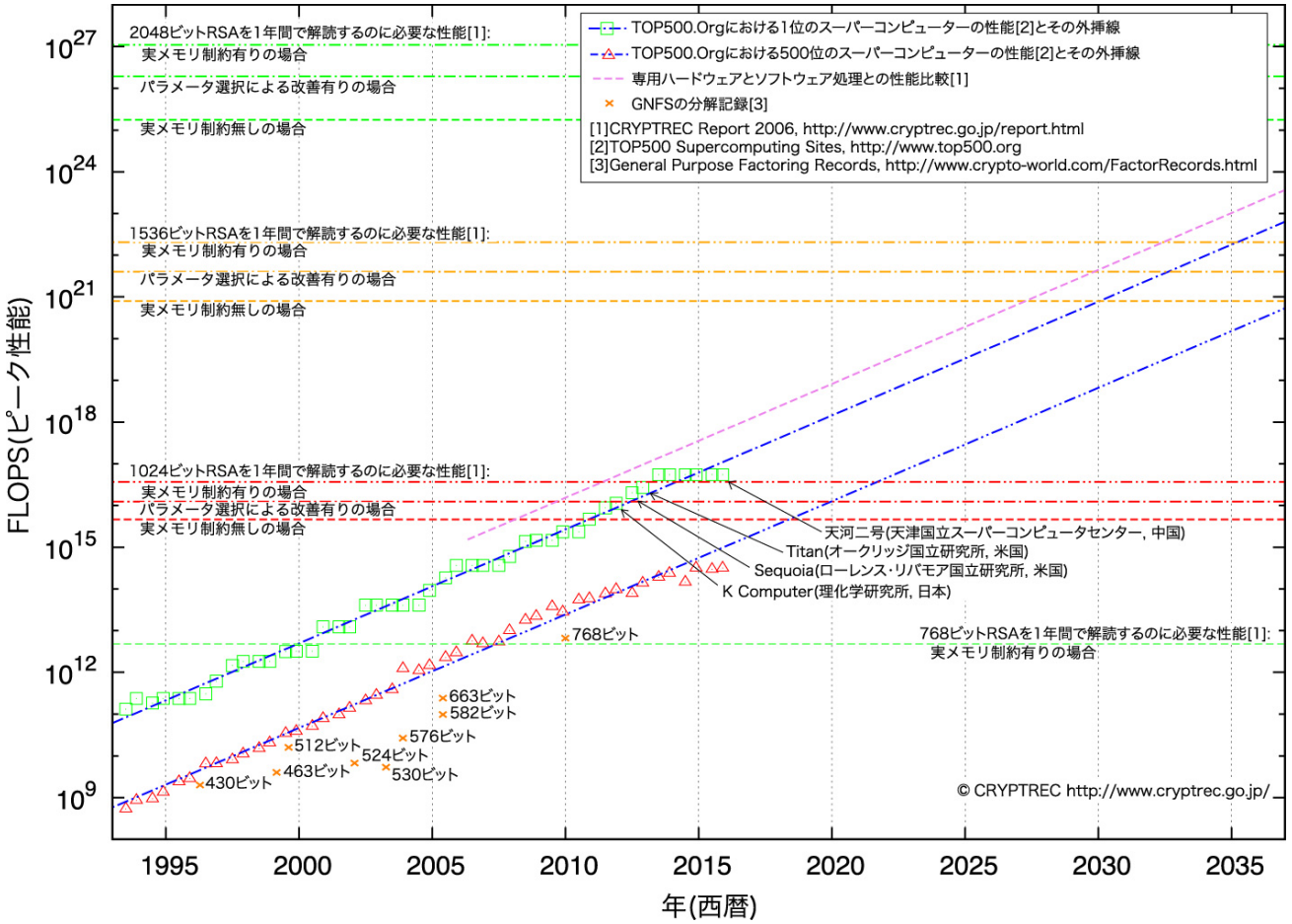
など

今年度引き続き検討を行う

一般数体ふるい法
General Number Field Sieve (GNFS)

- 現在知られている中で最良の素因数分解アルゴリズム
  - 準指数時間 $O\left(e^{(c+o(1))(\log N)^{1/3}(\log\log N)^{2/3}}\right)$
- 大きく分けると下記の過程に分かれる:
  - 多項式選択
  - 関係式収集(篩)（☜全体の中で支配的）
  - フィルタリング
  - 線形代数　　（☜全体の中で支配的）
  - 平方根の計算

素因数分解の解読推移と予測

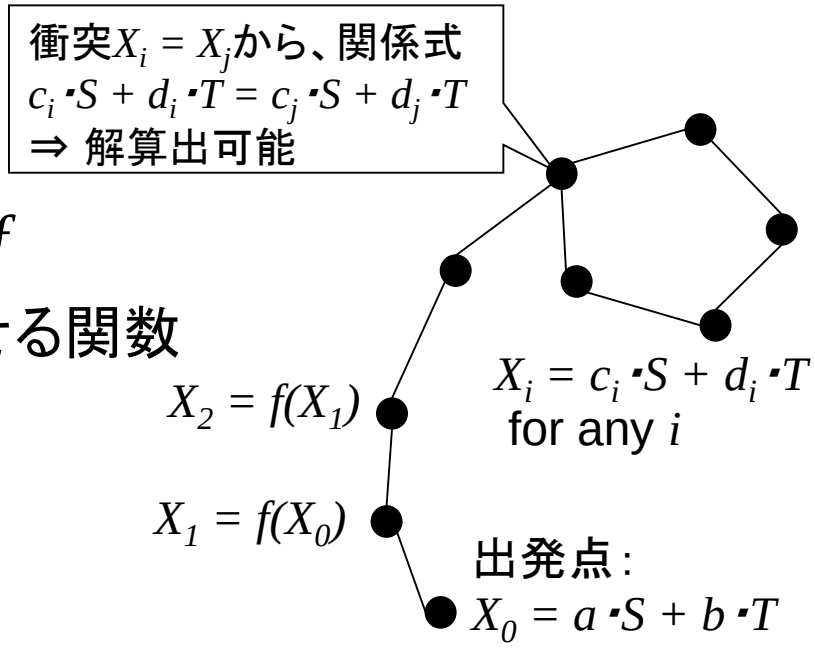


1年でふるい処理を完了するのに要求される処理能力の予測(2016年2月更新)
(CRYPTREC Report 2006, http://www.cryptrec.go.jp/report/c06_wat_final.pdf)

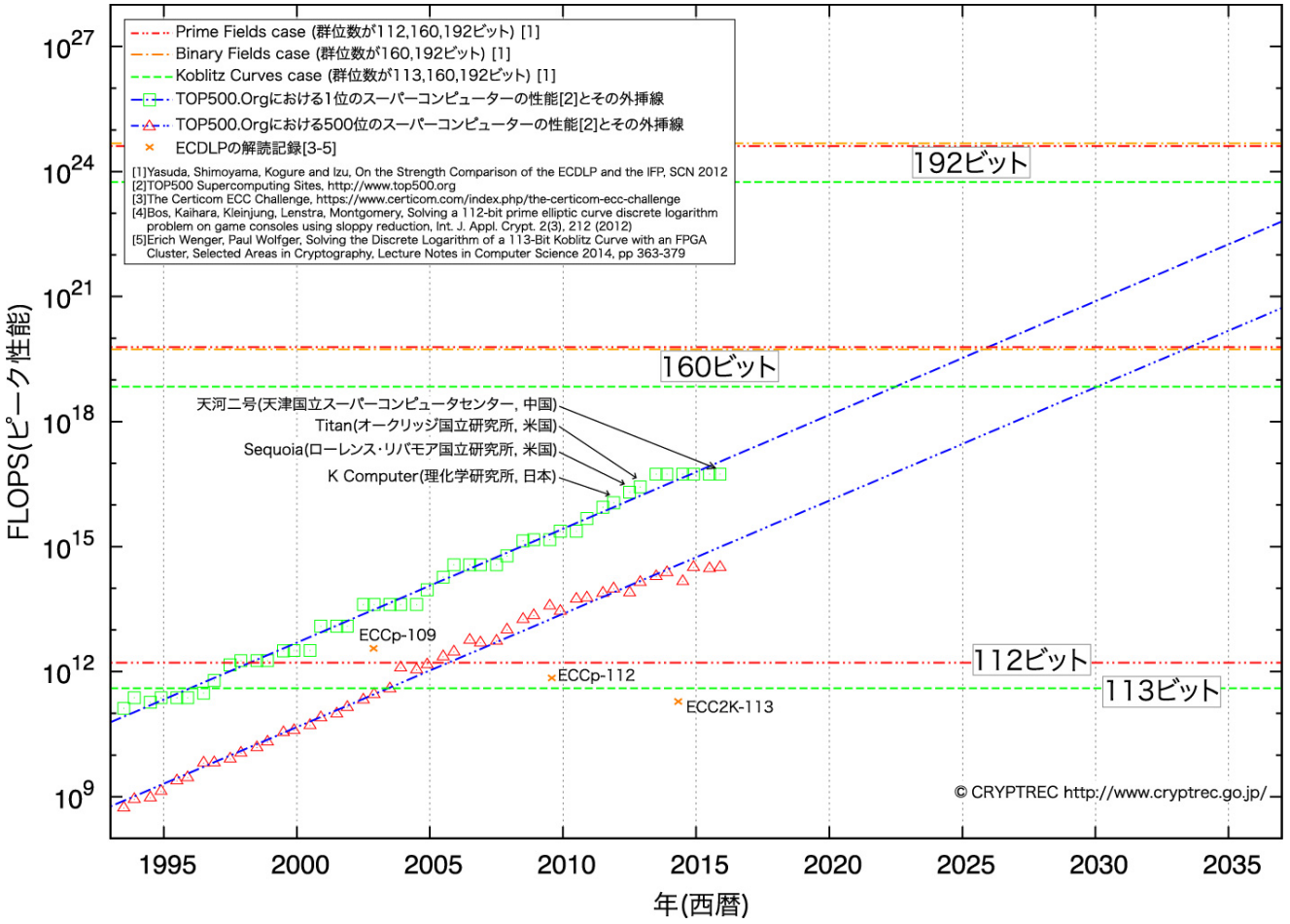
楕円曲線上の離散対数問題
(Elliptic Curve Discrete Logarithm Problem)

ポラード(Pollard)の ρ（ロー） 法

- 一般のECDLPに対する最良のアルゴリズム
  - (E, S, T)に対して、$T = dS$となる整数dを求めよ。
  - E: 位数 n の楕円曲線、S, T: E上の点
  - 指数時間　$O(\sqrt{n})$
- 反復計算
  - ρ 法実装で固定する関数 f
    - 解読計算量を大きく左右させる関数
  - ランダム関数が最適
    - 平均$\sqrt{\pi n/2}$−回の計算で衝突
      （birthday paradox）



解読計算量の見積もり



ρ 法でECDLPを1年で解くのに要求される処理能力の予測(2016年2月更新)
(CRYPTREC Report 2012, http://www.cryptrec.go.jp/report/c12_sch_web.pdf)

楕円曲線上の離散対数問題に対する指数計算法

- 楕円曲線上の点をFactor Baseと呼ばれる空間内の点の和で表すことにより、問題を線形代数の問題に帰着する一連の方法。
  - この種のアイディアは‘90年代から存在する。
  - 最近の論文では、Semaevが2004年に導入したsummation polynomialを用いた方法に基づいている。

楕円曲線上の離散対数問題に対する指数計算法(つづき)

- 点の和で表す問題は、多変数多項式の求解問題に帰着される。
  - 多変数多項式の求解問題やその計算量評価は、非常に難しい問題である。
  - グレブナー基底を使った計算量の評価が試みられている。
    - Petit and Quisquater, “On polynomial systems arising from a Weil descent,”ASIACRYPT 2012.
    - Huang, Kosters and Yeo, “Last Fall Degree, HFE, and Weil Descent Attacks on ECDLP,”CRYPTO 2015.
    - Petit, Kosters and Messeng, “Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields,”PKC 2016.

⇒ 今年度、近年の研究動向をまとめる予定。

有限体上の離散対数問題
(Discrete Logarithm Problem)

指数計算法

- 現在知られている中で最良の離散対数問題を解くアルゴリズムの枠組み（数体篩法、関数体篩法を含む）
  - 準指数時間 $O\left(e^{(c+o(1))(\log N)^{1/3}(\log\log N)^{2/3}}\right)$以下
- 大きく分けると下記の過程に分かれる:
  - パラメータ選択（多項式選択など）
  - 関係式収集(篩、Pinpointing など)
  - 線形代数
  - 小さい離散対数への還元

DLPの困難性

- 大きな標数の拡大体の場合は、数体篩法が有効。
  - DSA(NIST FIPS 186-4)やDH(NIST SP 800-56A)のパラメータ選択に該当
    - 現在のところ、素体上であれば安全。
  - 標数が特殊な構造をもっている場合は、その構造を利用して計算量を小さくすることが可能(特殊数体篩法)
    - 例:Kim & Barbulescu,"Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case," CRYPTO 2016.
- 小さな標数の拡大体の場合は、関数体篩法が有効。