CRYPTREC
Cryptography Research and Evaluation Commitees

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

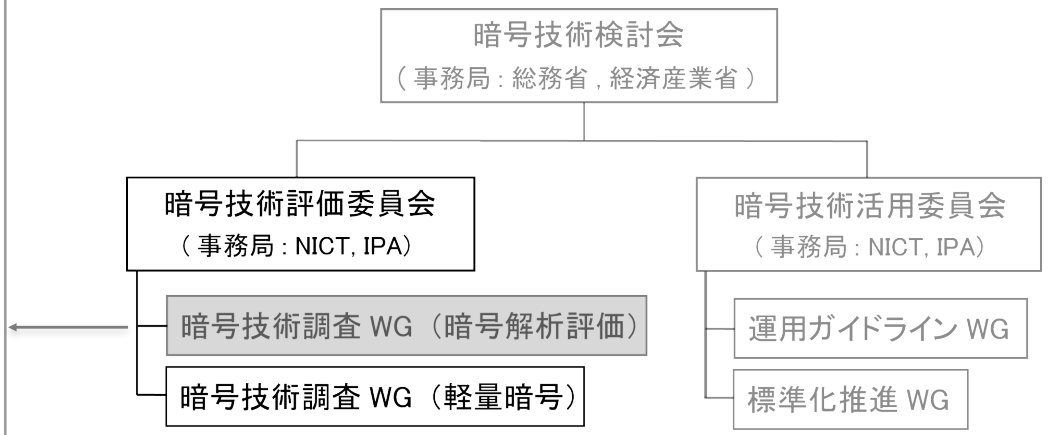
Institute of Mathematics for Industry
Kyushu University

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。

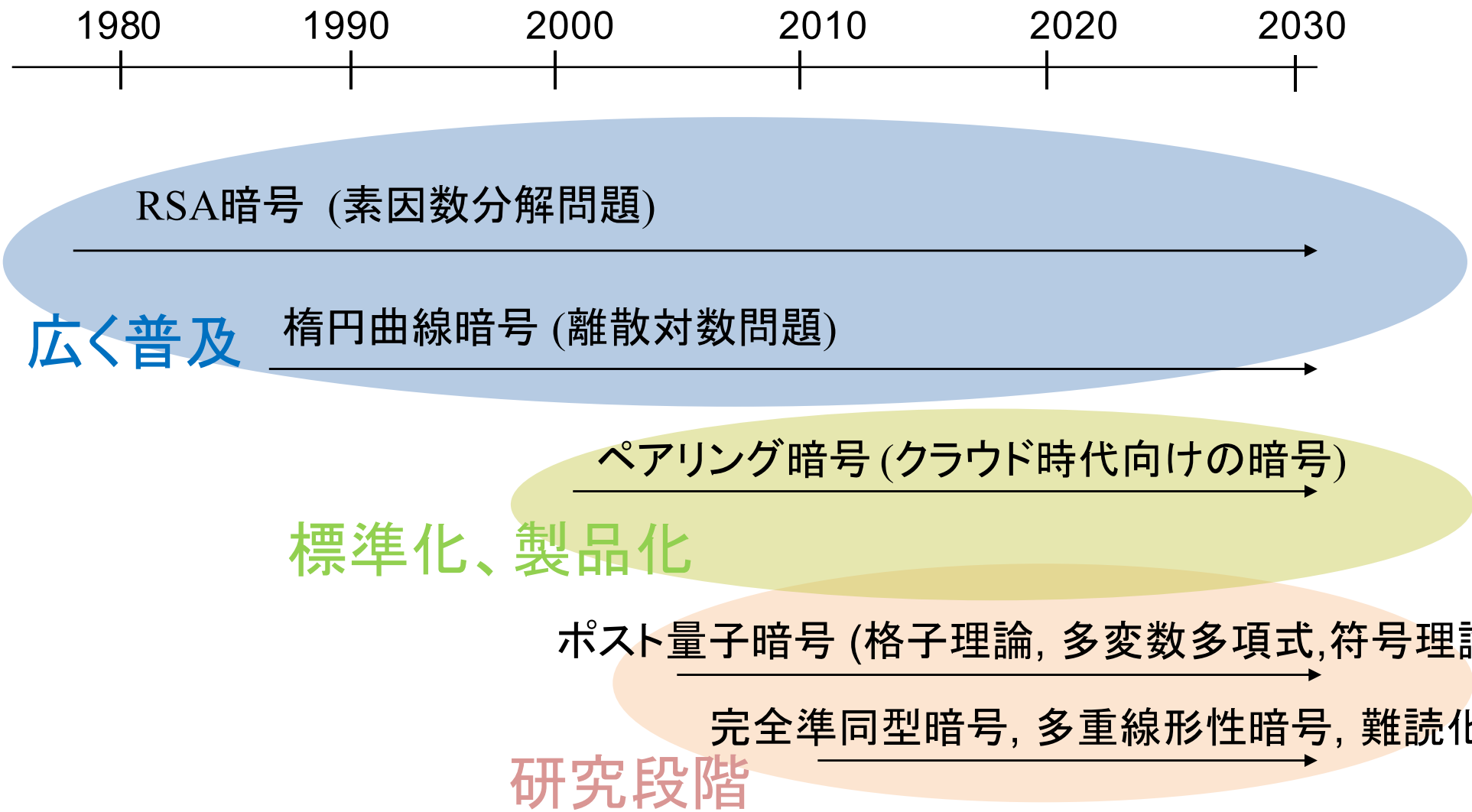
主査：高木 剛（九州大学）
委員：青木 和麻呂(NTT)
委員：石黒 司(KDDI研究所)*
委員：太田 和夫（電気通信大学）
委員：草川 恵太(NTT)
委員：國廣 昇（東京大学）
委員：下山 武司（富士通研究所）
委員：安田 雅哉（富士通研究所）

*2013年度まで



CRYPTREC
Cryptography Research and Evaluation Commitees

公開鍵暗号の歴史



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
- より詳細な内容については、CRYPTREC Report をご覧下さい。

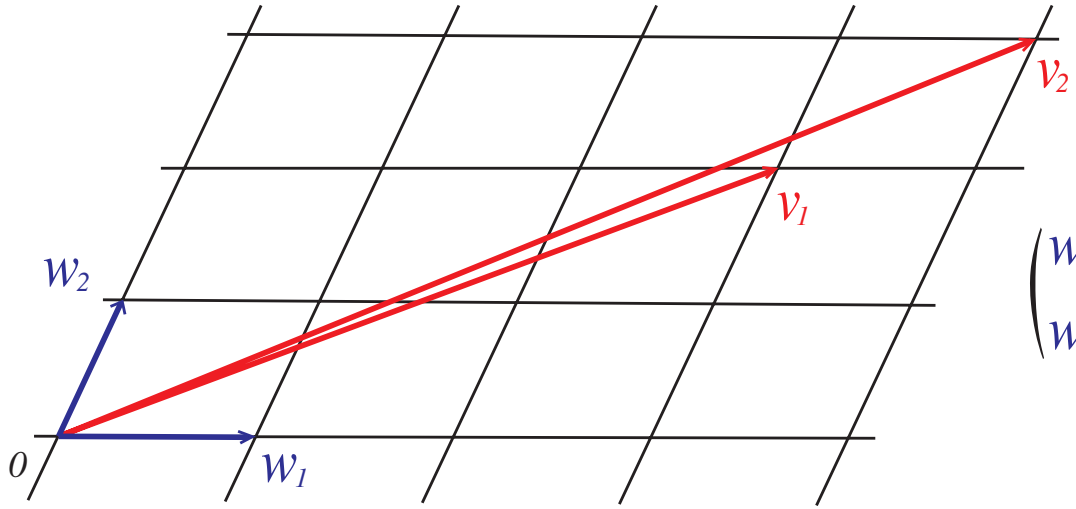
調査レポートの概要

章	執筆者	数学的問題	内容
第2章	石黒委員	最短ベクトル問題(SVP)	• SVPに関する一般的な概説
第3章	下山・安田委員	LWE問題	• 公開鍵方式からの帰着、証明の有無、追加の問題・制約など • 攻撃や量子アルゴリズム ➢ General な攻撃との関係 ➢ 固有の攻撃 ➢ 量子アルゴリズムとの関係
第4章	草川委員	LPN問題	
第5章	國廣委員	ACD問題	

SVP(Shortest Vector Problem)

最短ベクトル問題

- 格子上のベクトルの中で長さが最小となる非零ベクトルを探索する問題
- 大きな次元の格子では最短ベクトルを求めることは非常に難しい。



$$\begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

求解アルゴリズム

- SVPは、(条件付きで)NP困難であることが示されている(Ajtai 1998)。
- SVPを解くアルゴリズムとしてさまざまな求解アルゴリズムが提案されている。
  - 格子基底簡約アルゴリスム
    - LLL(Lenstra-Lenstra-Lovász)
    - BKZ(Block Korkin-Zolotarev)
  - 篩アルゴリズム
    - Gauss Sieve(Micciancio-Voulgaris)
  - 列挙アルゴリズム
    - Extreme Pruning Enumeration(Gama-Nguyen-Regev)
  - ボロノイセルアルゴリズム
    - Micciancio-Voulgaris

計算機実験

- ダルムシュタット工科大学のWebサイト上にSVPに関するコンテストが実施されている。日本の研究者も多く参加している。
- SVP Challenge (http://www.latticechallenge.org/svp-challenge/)
  - ランダムに与えられた格子基底に対してSVPを解き、より大きな次元、より短いベクトルを求める。
- Lattice Challenge (http://www.latticechallenge.org/)
  - 与えられた格子基底について近似版SVPを解き、より大きな次元、より短いベクトルを求める。
- Ideal Lattice Challenge

  (http://www.latticechallenge.org/ideallattice-challenge/)
  - 暗号で用いられることが多いイデアル格子に対するSVP、近似版SVPを解く。

LWE(Learning With Errors)問題

LWE問題とは

- 秘密情報に関するランダムな線形な近似値の列が与えられたときに、その秘密情報を復元する問題のこと。与えられた誤差の度合いが問題を難しくする。
  - 例：秘密情報(s_1, s_2, s_3, s_4)に関する線形近似値の列

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

- 類似なものとして、環(ring)の上で定義されたring-LWE問題がある。

LWE問題のアプリケーション

- 暗号技術の様々な分野に応用することが可能
  - 公開鍵暗号
    - Regev(2005), Kawachi−Tanaka−Xagawa(2007) など
    - Peikert−Waters(2008), Peikert(2009)
  - 紛失通信(Oblivious Transfer)
    - Peikert−Vaikuntanathan−Waters(2008)
  - IDベース暗号
    - Gentry−Peikert−Vaikuntanathan(2008), Cash−Hofheinz−Kiltz−Peikert(2010) など
  - 漏洩に耐性がある(Leakage-resilient)暗号
    - Akavia−Goldwaser−Vaikuntanathan(2009), Applebaum−Cash−Peikert−Sahai(2009) など
  - 完全準同型(Fully homomorphic)暗号
    - Smart−Vercauteren(2011), Brakerski−Gentry−Vaikuntanathan(2012) など

LWE問題の困難性

- 理論的な評価
  - 既知の中で最良のアルゴリズムでも、指数時間アルゴリズムである。（量子アルゴリズムを用いた場合でも難しい。）
  - GapSVP$_\gamma$問題やSIVP$_\gamma$問題に関するある仮定のもとで、LWE問題は困難であることが知られている。
- 攻撃実験的な評価
  - Distinguishing Attack (Micciancio−Regev 2007)
  - Decoding Attack (Lindner−Peikert 2011)

LWE問題まとめ

- 現時点では、効率的に解くことは困難であると予想されている。
- 現在までに完全準同型暗号スキームをはじめとした、様々な公開鍵暗号スキームのベースがこの問題をベースとして提案されており、今後も安全な暗号を構成する上で重要な要素となると考えられる。
- 現在までに知られている最良アルゴリズムは指数時間の計算量を持っている。ただし、実際の LWE 問題をベースとした暗号スキームの構成の際には、既存の解読アルゴリズムに対し耐性を持つようにパラメータ設定を行う必要があり、安全でかつ演算機能等の要件を満足するようなパラメータを選択するための、統一的な方法は知られておらず、今後の課題となっている。
- 今後は計算機実験に関する研究も非常に重要になると思われることから、安全性理論評価はもちろん攻撃実験評価の視点からも、今後の動向に注意する必要がある。

LPN (Learning Parity With Noise) 問題

LPN問題とは

- 基礎となる有限体としてGF(2)を用いた場合における、LWE問題に対応するもの。

LPN問題のアプリケーション

- LWE問題と同様に、暗号技術の様々な分野に応用することが可能
  - 擬似乱数生成器
    - Blum-Furst-Kearns-Lipton 1993
    - Fischer-Stern 1996
    - Appelbaum-Cash-Peikert-Sahai 2009
  - 共通鍵による両側認証
    - HBプロトコル(Hopper-Blum 2001)など
  - 共通鍵暗号
    - LPN-C(Gilbert-Robshaw-Seurin 2008)など
  - 署名
    - Fiat-Shamir変換によるもの
    - Full-Domain Hashによるもの
  - 公開鍵暗号
    - Alekhnovich暗号
    - McEliece暗号
    - Niederreiter暗号
  - 紛失通信
    - Dowsley-van de Graaf-Mueller-Quade-Nascimento 2012など

LPN問題の困難性

- 理論的な評価
  - LPN問題は、条件付きでNP困難であることが示されている。
  - 近似版LPN問題のNP困難性も示されている。
  - 現在のところ、多項式時間でLPN問題を解く量子アルゴリズムは提案されていない。
- 攻撃実験的な評価
  - BKWアルゴリズム(Blum-Kalai-Wasserman 2003)
  - 再線形化アルゴリズム(Arora-Ge 2011)
  - シンドローム復号問題として解くアルゴリズム

LPN問題まとめ

- 現時点では、誤り確率が十分大きい場合、効率的に解くことは困難であると予想されている。
- 共通鍵暗号や公開鍵暗号の分野で、多くの方式が提案されている。
- 利点：ハードウェア構成との相性が良い、誤差のサンプリングが容易である。欠点：鍵や暗号文のサイズが大きくなり易い、IDベース暗号や完全準同型暗号といった発展的な応用が少ない。
- 暗号方式のパラメータ設定の際には、既存の解読アルゴリズムに対し耐性を持つよう設定をする必要がある。
- アルゴリズムの高速化について盛んに研究されており、動向を注視する必要がある。
- 攻撃に用いられるアルゴリズムの研究は理論的なものが多く、攻撃実験報告は小さいパラメータに対して行ったものが多い。そのため、攻撃実験に関する研究もこれから非常に重要である。

ACD問題
(Approximate Common Divisor Problem)

ACD問題とは

- Nを既知の合成数とし、pをNの未知の素因数とするとき、与えられた整数aに対して、

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

を満たすxを求めること。

- Nが与えられない場合を、General ACD問題(GACD問題)と呼ぶ。区別のため、Nが与えられている場合を、Partial ACD問題(PACD問題)と呼ぶこともある。

ACD問題のアプリケーション

- 完全準同型暗号
  - 複数ACD問題をベースとする方式（van Dijk-Gentry-Halevi-Vaikuntanathan 2010）
  - Chinese Remainder Theoremを用いた、バッチ処理が可能な方式(Cheon-Coron-Kim-Lee-Lepoint-Tibouchi-Yun 2013)

ACD問題の困難性

- PACD問題の場合
  - N の素因数分解によるもの
  - 組み合わせ論に基づくアルゴリズム
    - 指数時間アルゴリズム（解の大きさに制限なし）（Chen–Nguyen 2011）
  - 格子理論に基づくアルゴリズム
    - 多項式時間アルゴリズム（解の大きさに制限あり）（Howgrave-Graham 2001）
- GACD問題の場合
  - 組み合わせ論に基づくアルゴリズム(Chen–Nguyen 2011)
  - 格子理論に基づくアルゴリズム(Howgrave-Graham 2001, Cohn-Heninger 2011)
  - 最短ベクトルに埋め込む方法（van Dijk-Gentry-Halevi-Vaikuntanathan 2010）

ACD問題まとめ

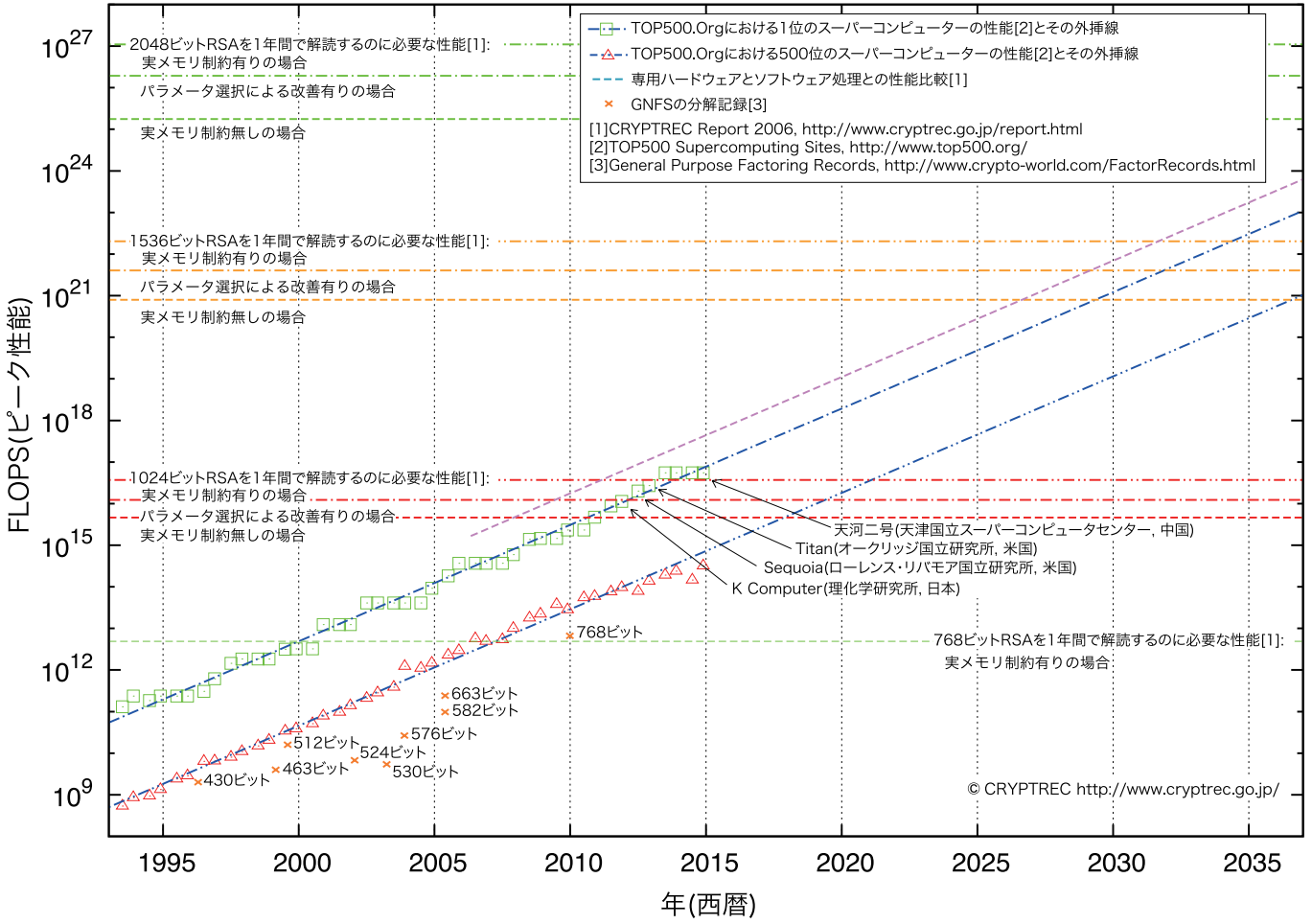
- 現時点においては、効率的に解くことは困難であると予想されている。
  - 法に対して、解がある制限よりも小さいときには、多項式時間で解くことができるが、解が十分大きいときには，解を求めることができない。
- 最近、提案されたアルゴリズム(Chen-Nguyen、2011年)は、暗号の提案時には考慮されていなかった攻撃であり、実際に、提案論文で書かれた推奨パラメータのいくつかは，解読されることが示されているため、今後の研究の動向に注視する必要がある。
- ACD 問題に関連した問題co-ACD 問題(Cheon ら、2014年)は、当初の想定よりも弱いことが明らかになっている。これらの結果は、ごく最近に示されたものであり、今後の研究の動向に注視する必要がある。

素因数分解問題
(Integer Factorization Problem)

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

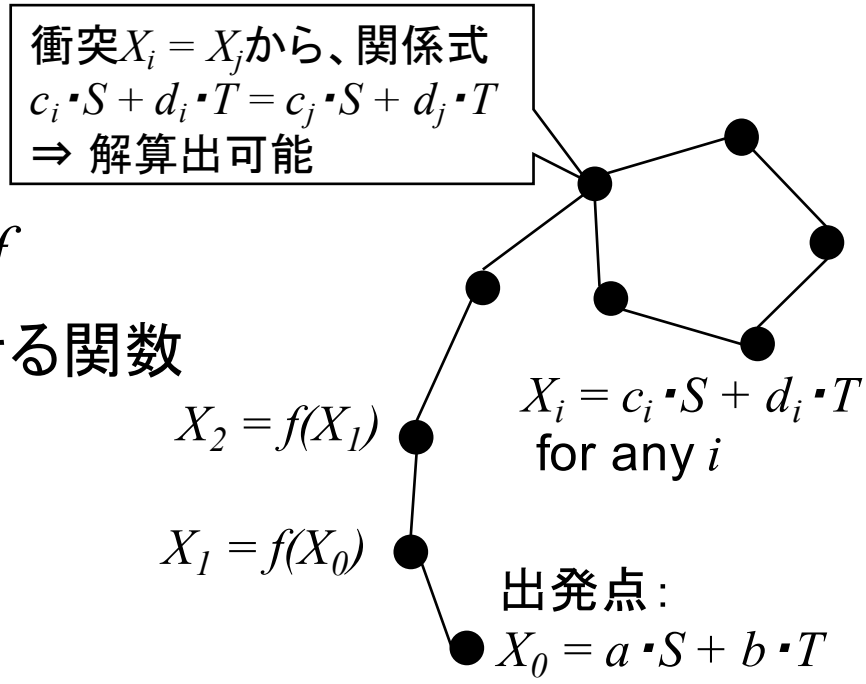


1年でふるい処理を完了するのに要求される処理能力の予測(2015年2月更新)
(CRYPTREC Report 2006, http://www.cryptrec.go.jp/report/c06_wat_final.pdf)

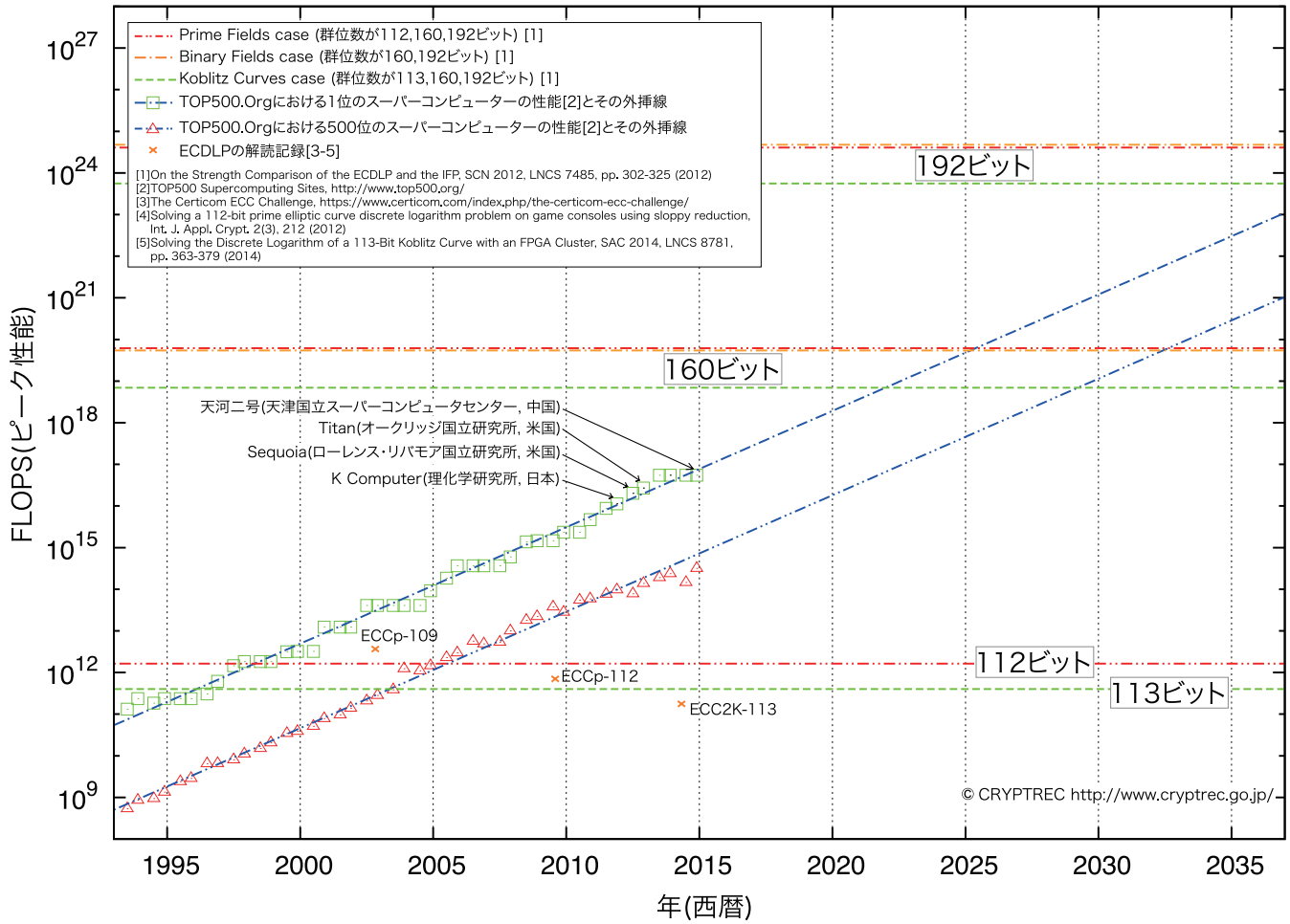
楕円曲線上の離散対数問題
(Elliptic Curve Discrete Logarithm Problem)

ポラード(Pollard)の ρ 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(2015年2月更新)
(CRYPTREC Report 2012, http://www.cryptrec.go.jp/report/c12_sch_web.pdf)

【参考】IFP vs ECDLP強度比較（安田らのSCN2012の表8からの引用）

- GNFSメモリ制限なしとの比較

IFPのビットサイズ	ECDLPのビットサイズ		
	素体の場合	標数2の場合	コブリッツ曲線の場合
512	87	87	92
768	113	113	118
894	124	124	129
1024	133	134	139
1308	153	154	159
1413	160	160	166
1536	168	168	174
2048	195	196	202
2671	224	224	231
3241	247	247	254

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

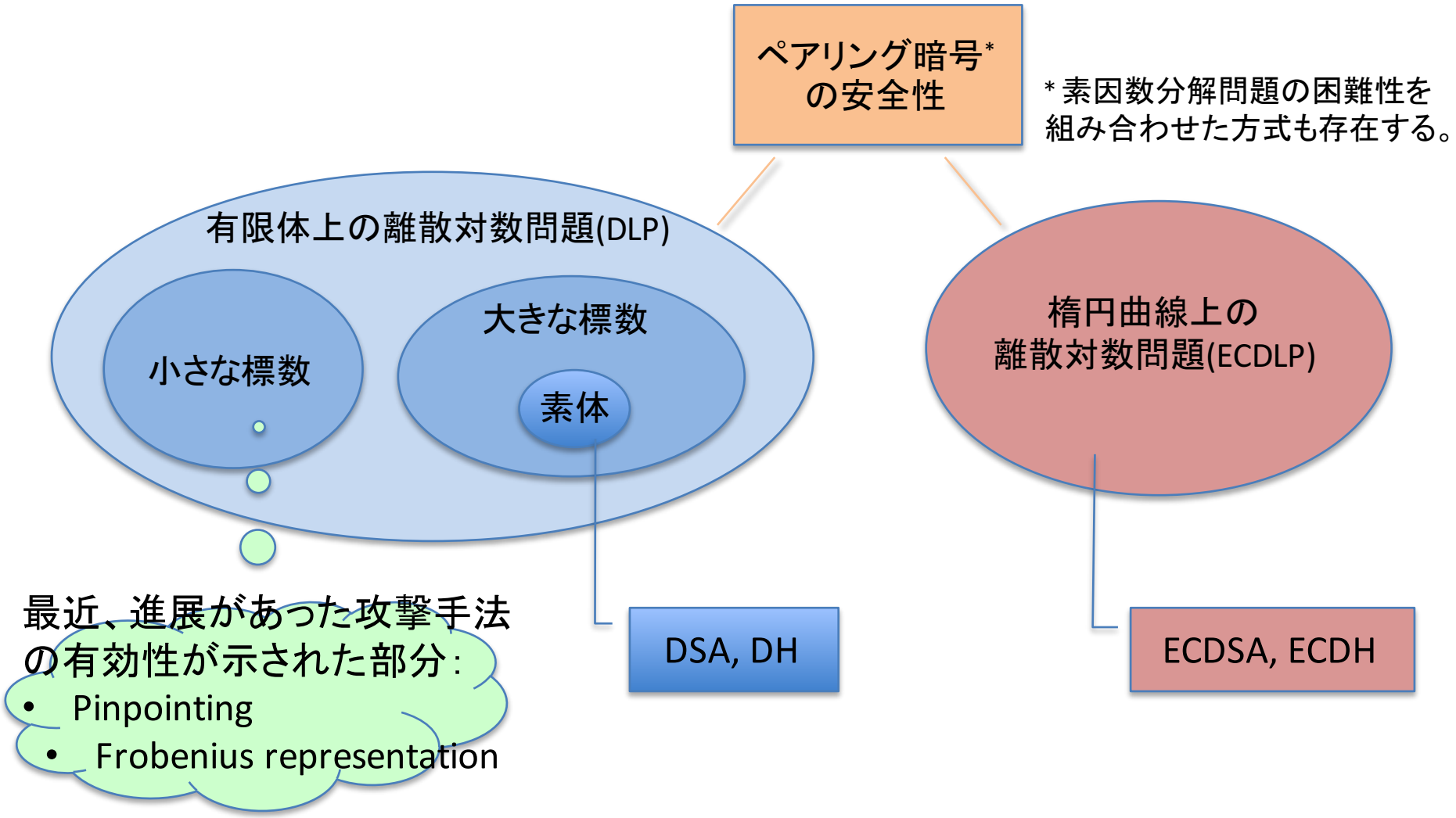
指数計算法

- 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
- 小さな標数の拡大体の場合は、関数体篩法が有効。
  - ペアリング実装例が多数、報告されてきた。
    - IDベース暗号に関する調査報告書(2008年度作成)の第3章
  - 関数体篩法は近年研究が活発になっている。
  - 特殊数体篩法の分解記録との類似性。

ペアリング暗号の安全性



標数が2又は3である有限体上のDLPに関する記録

年月	有限体	ビットサイズ	CPU時間	記録者名
1992	$GF(2^{401})$	401	114000	Gordon, McCurley
2001.09	$GF(2^{521})$	521	2000	Joux, Lercier
2001	$GF(2^{607})$	607	> 200000	Thomé
2005.09	$GF(2^{613})$	613	26000	Joux, Lercier
2012.06	$GF(3^{6\cdot 97})$	923	895000	Hayashi et al.
2013.02	$GF(2^{2\cdot 7\cdot 127})$	1778*	220	Joux
2013.02	$GF(2^{3\cdot 73})$	1971*	3132	Göloğlu et al.
2013.03	$GF(2^{4\cdot 3\cdot 5\cdot 17})$	4080*	14100	Joux
2013.04	$GF(2^{809})$	809	19300	The Caramel Group
2013.04	$GF(2^{3\cdot 3^2\cdot 5\cdot 17})$	6120*	750	Göloğlu et al.
2013.05	$GF(2^{3\cdot 3\cdot 257})$	6168*	550	Joux
2014.01	$GF(3^{6\cdot 137})$	1303	888	Adj et al.
2014.01	$GF(2^{2\cdot 3^5\cdot 19})$	9234*	398000	Granger et al.
2014.01	$GF(2^{2^2\cdot 3\cdot 367})$	4404	52000	Granger et al.
2014.09	$GF(3^{5\cdot 479})$	3796	8600	Joux, Pierrot
2014	$GF(3^{6\cdot 163})$	1551	1201	Adj et al.
2014.10	$GF(2^{1279})$	1279	35040	Kleinjung

表中の*はKummer extension又はtwisted Kummer extensionの性質が適用されたことを意味する。

ペアリング暗号で利用される小さな標数の有限体

- 拡大次数の大きさと部分体の大きさの比などに関連するため、計算量の評価は複雑。
  - 有限体ごとに評価する必要がある。
- 計算機実験からの結論
  - $GF(3^{6\cdot 137})$ や$GF(3^{6\cdot 163})$ の場合が解かれている。
    - $l \leqq 163$ である有限体$GF(3^{6\cdot l})$ 上のDLPは現実的な時間内で解読可能と見込まれる。
  - $GF(2^{2^2\cdot 3\cdot 367})$ の場合が解かれている。
    - $l \leqq 367$ である有限体$GF(2^{12\cdot l})$ と$GF(2^{4\cdot l})$ 上のDLPは現実的な時間内で解読可能と見込まれる。
- より詳細な内容については、CRYPTREC Report をご覧ください。

Thank you!