CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術調査WG(計算機能力評価)活動報告

主査　高木 剛

九州大学

KYUSHU UNIVERSITY

マス・フォア・インダストリ研究所

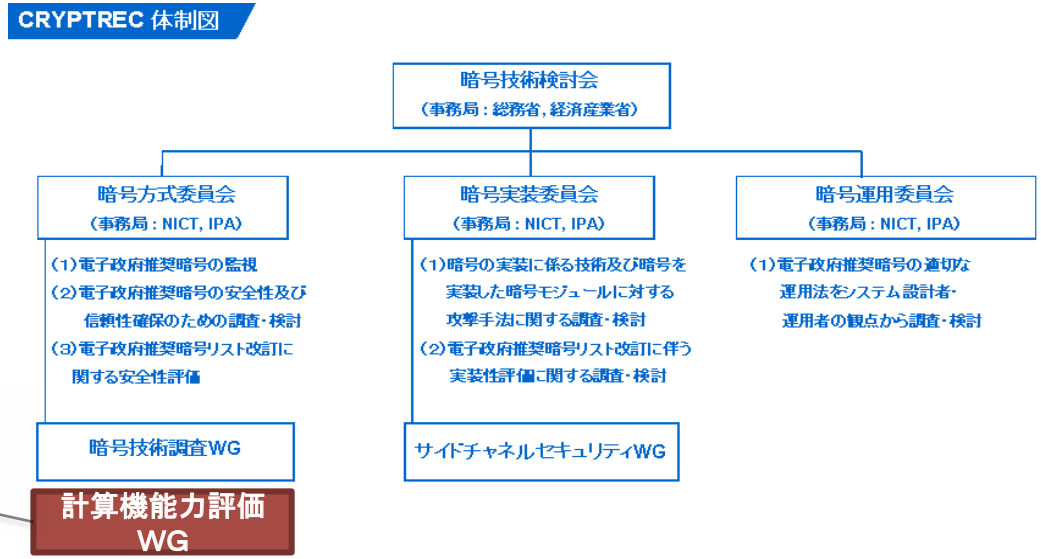
http://imi.kyushu-u.ac.jp/~takagi/

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：國廣 昇(東京大学)
委員：下山 武司(富士通研究所)



公開鍵暗号の歴史

RSA暗号（SSLなどで広く普及、素因数分解の困難性を安全性の根拠）

楕円曲線暗号（鍵長が短く、組み込みディバイスで利用）

ペアリング暗号（新たな暗号応用が構築可能）

ポスト量子暗号（符号理論、格子理論、多変数多項式など）

完全準同型暗号、多重線形性写像

素因数分解問題
(Integer Factorization Problem)

簡単な例(2次篩法)

- 分解したい数 n に対して、√n 近くの数を2乗して n を引くことで、
  $x^2 \equiv y^2 \bmod n$
  が成り立つ数 x, y を見つける。
- n = 3937の場合、
  $63^2 - n = 2^5$ ☜
  $64^2 - n = 3 \cdot 5^3$
  $65^2 - n = 2^5 \cdot 3^2$ ☜
  $66^2 - n = 419$
  $67^2 - n = 23 \cdot 3 \cdot 23$
  …
- ☜の部分を組み合わせると、
  $(63 \cdot 65)^2 \equiv (2^5 \cdot 3)^2 \bmod n$
- GCD$(63 \cdot 65 - 2^5 \cdot 3, n) = 31$
  $3937 / 31 = 127$

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

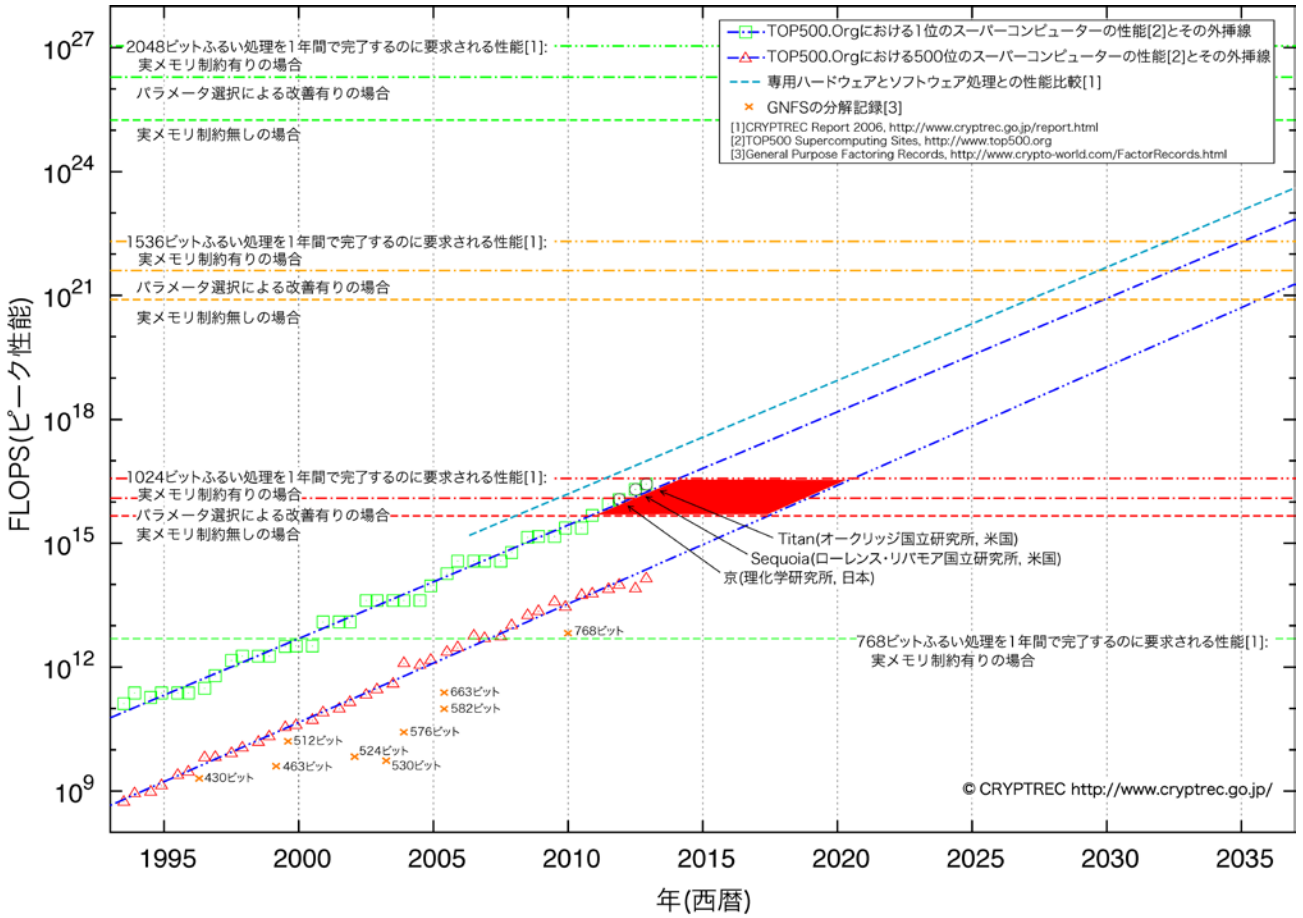
- 現在知られている中で最速な素因数分解アルゴリズム
  - 準指数時間 $O\left(e^{(c+o(1))(\log N)^{1/3}(\log\log N)^{2/3}}\right)$
- 大きく分けると下記の5つの過程に分かれる:
  - 多項式選択
  - 関係式収集(篩(ふるい)) （☜全体の中で支配的）
  - フィルタリング
  - 線形代数　　（☜全体の中で支配的）
  - 平方根の計算

素因数分解の解読世界記録

- 2010年1月、232桁、1500年×CPU、NTT青木ら

- 1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413
  =
  3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799489
  ×
  3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

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(2013年2月更新)
(CRYPTREC Report 2006, http://www.cryptrec.go.jp/report/c06_wat_final.pdf)

IFPに依存している方式に対する鍵長の選択指針

- RSAに関する選択指針
  - 現時点においては一般数体篩法が有効
    - 2048ビット以上が推奨
- Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST SP 800-131A(January 2011)では、
  - 1024ビット以上2048ビット未満の場合は
    - 「Acceptable through 2010, Deprecated from 2011 through 2013, Disallowed after 2013」
  - 2048ビット以上の場合は
    - 「Acceptable」

  とされている。

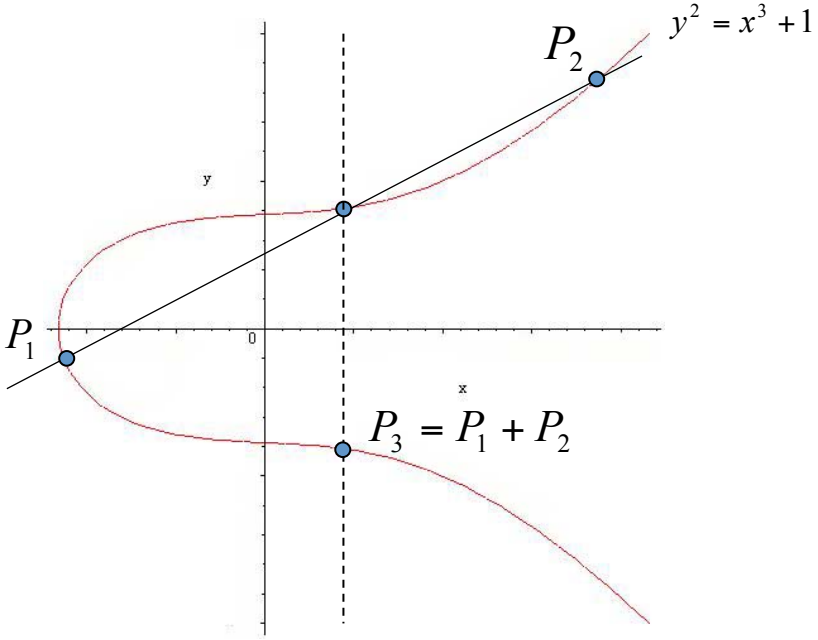
オープンソース実装例

- CADO-NFS
  - http://cado-nfs.gforge.inria.fr/
    - http://maths-people.anu.edu.au/~bai/paper/rsa704.txt
    - http://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2012-October/000098.html
- GGNFS
  - http://sourceforge.net/projects/ggnfs/

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

楕円曲線暗号

- $E(GF(p)):=\{(x,y) \in GF(p)^2 \mid y^2 = x^3+ax+b\} \cup \{\infty\}$は群構造を持つ

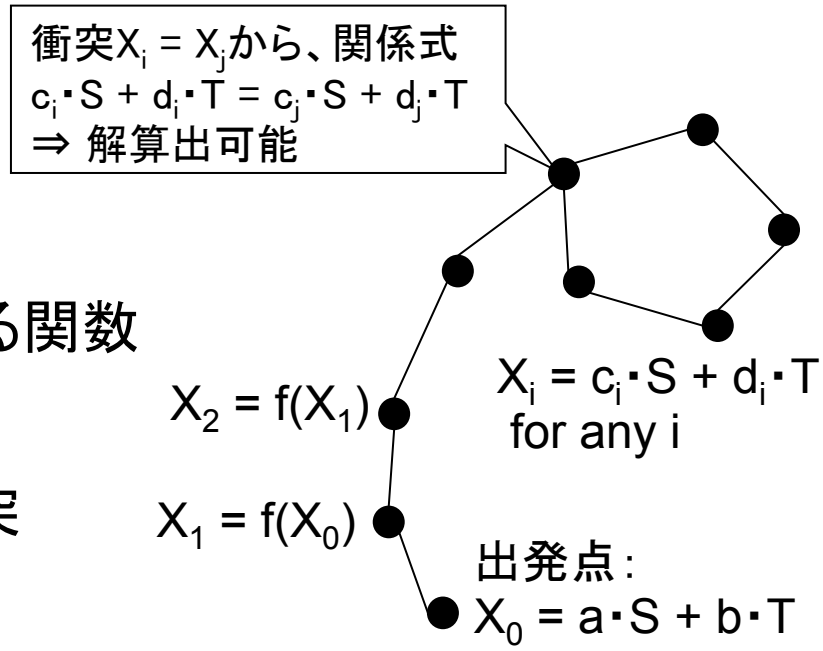


- 楕円曲線暗号の安全性　≒ 楕円曲線上の離散対数問題

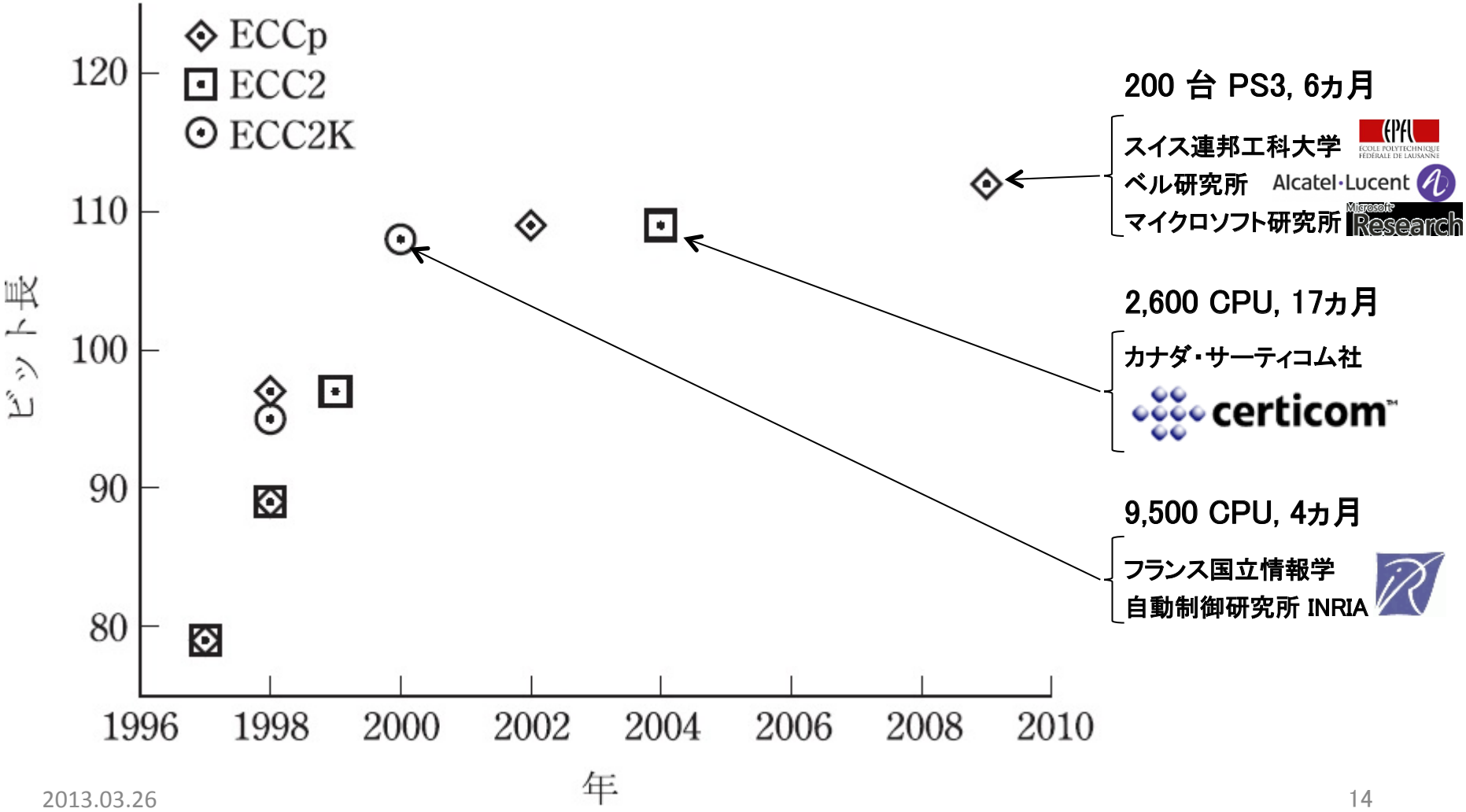
「dS = T を満たす秘密鍵 d を求めよ。」

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）



楕円曲線上の離散対数問題
解読世界記録の推移



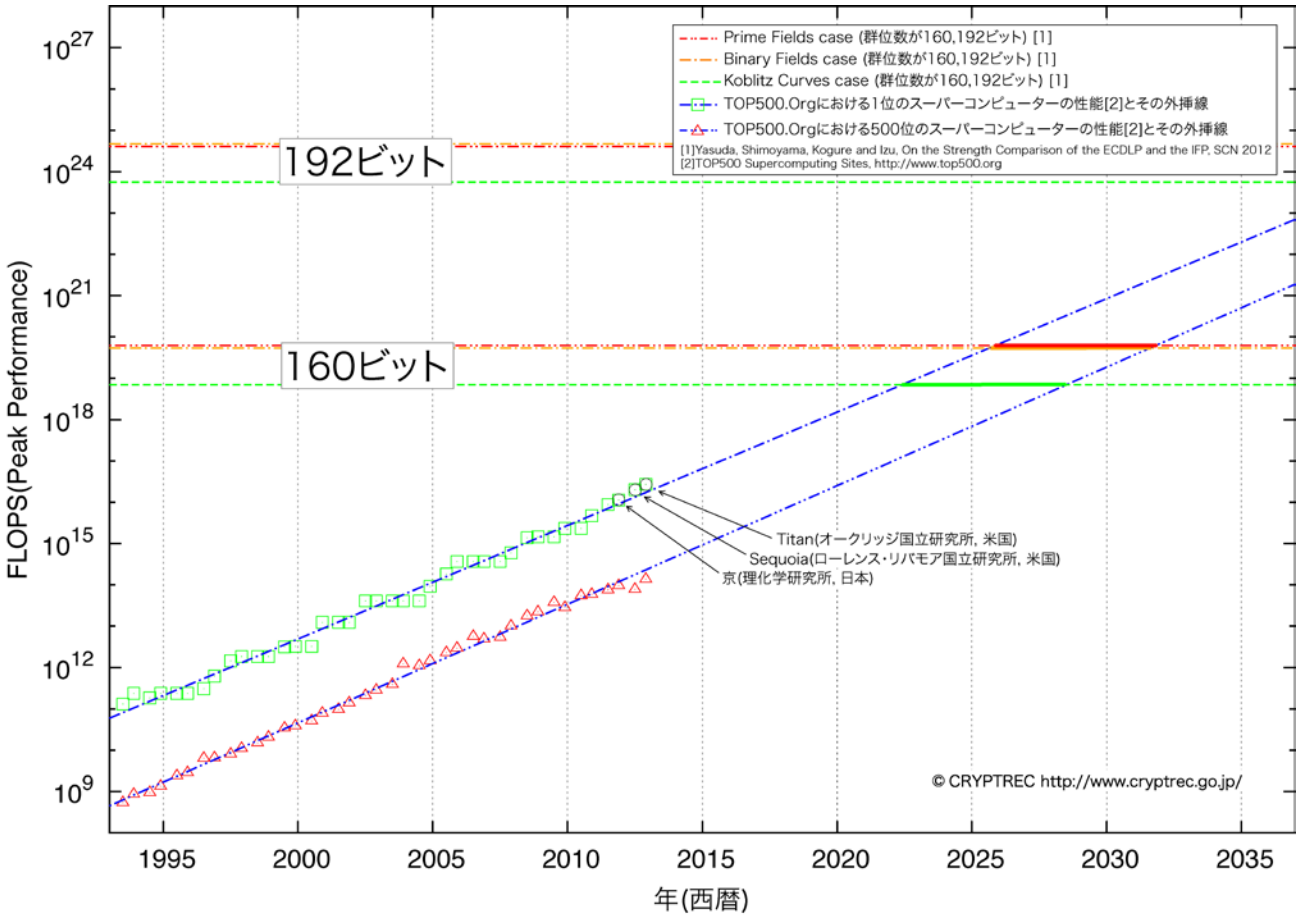
解読計算量の見積もり(1/2)

- 見積もり解読計算量T(単位: FLOPS)
  - N: ECDLPビットサイズ、Y = 365*24*60^2 seconds

$$T=\begin{cases} 3\cdot\sqrt{\pi 2^N}\,/\,2\times 270.05\,/\,4\times\left(\lceil N/64\rceil\right)^2\,/\,Y \text{ (prime fields case)},\\ 3\cdot\sqrt{\pi 2^N}\,/\,2\times 388.48\times(N/131)^{1.585}\,/\,Y \text{ (binary fields case)},\\ 3\cdot\sqrt{\pi 2^N/N}\,/\,2\times 1.62\times 388.48\times(N/131)^{1.585}\,/\,Y \text{ (Koblitz curves case)} \end{cases}$$

M. Yasuda, T. Shimoyama, J. Kogure, and T. Izu,
"On the Strength Comparison of the ECDLP and the IFP,"
SCN 2012, LNCS 7485, pp.302-325, Springer 2012.

解読計算量の見積もり(2/2)



ρ 法でECDLPを1年で解くのに要求される処理能力の予測(2013年2月)
(CRYPTREC Report 2012に掲載予定)

【参考】IFP vs ECDLP強度比較
（Yasuda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

ECDLPに依存している方式に対する鍵長の選択指針

- ECに関する選択指針
  - 現時点においてはρ法が有効
    - 推奨については検討が必要
- Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST SP 800-131A(January 2011)では、
  - 160ビット以上224ビット未満の場合は
    - 「Acceptable through 2010, Deprecated from 2011 through 2013, Disallowed after 2013」
  - 224ビット以上の場合は
    - 「Acceptable」

  とされている。

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

有限体GF(p)

- 素数 p=11,
- 有限体 GF(p)* = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

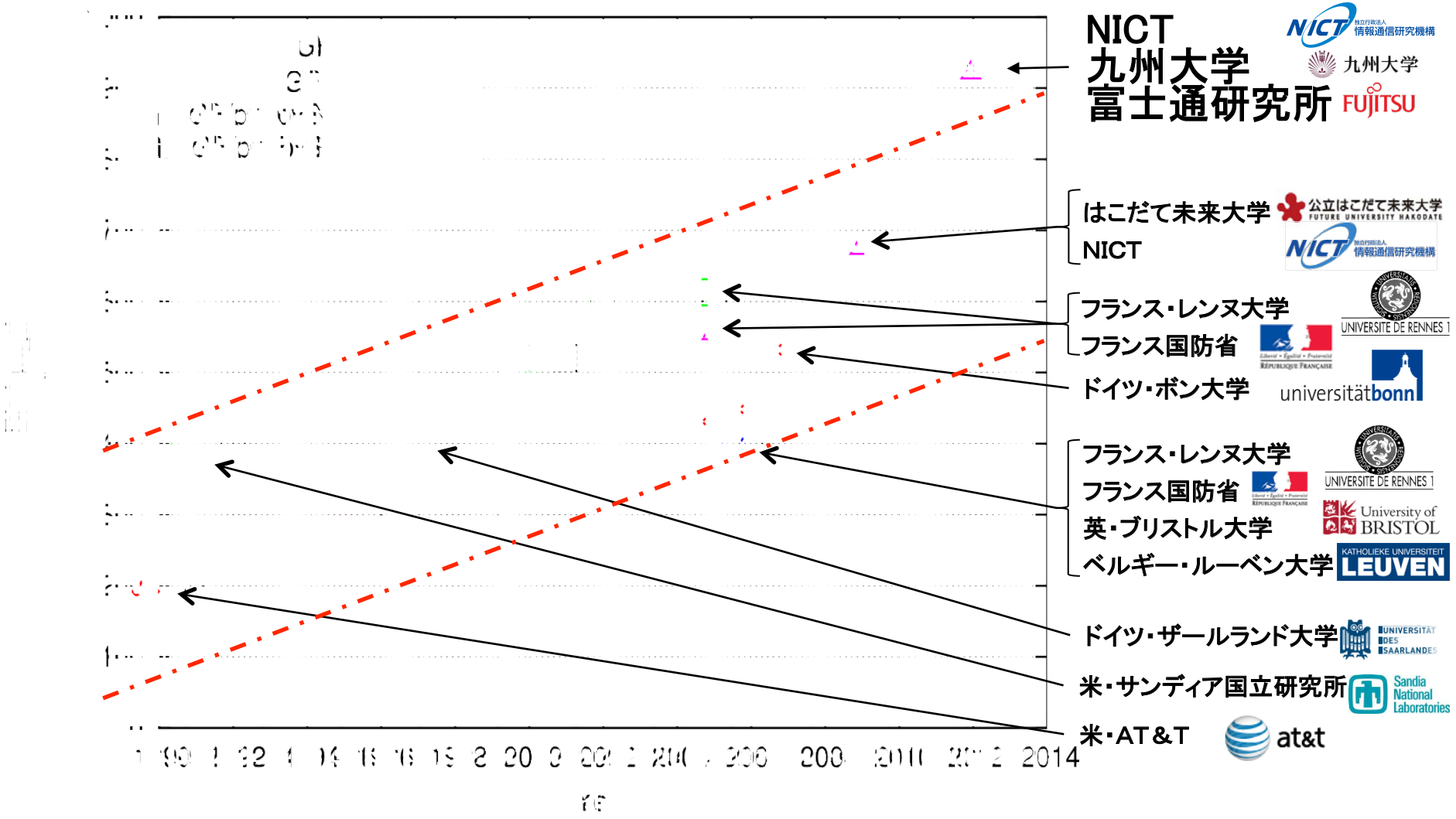
- $2^1 = 2$
- $2^2 = 4$
- $2^3 = 8$
- $2^4 = 16 = 1 \times 11 + 5 = 5$
- $2^5 = 2^4 \times 2 = 5 \times 2 = 10$
- $2^6 = 10 \times 2 = 1 \times 11 + 9 = 9$
- $2^7 = 18 = 7$
- $2^8 = 14 = 3$
- $2^9 = 6$
- $2^{10} = 12 = 1$

- 有限体上の離散対数問題

「$2^s = a$ を満たす秘密鍵 s を求めよ。」

離散対数問題の解読世界記録の推移

923ビット解読（2012年4月）



DLPに依存している方式に対する鍵長の選択指針(1/2)

- DLPに関する選択指針
  - 大きな標数の素体の場合は一般数体篩法が有効。
    - 現時点においてはIFPにおける指針と同様
      - 2048ビット以上が推奨
  - 小さな標数の拡大体の場合は関数体篩法が有効。
    - 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。

DLPに依存している方式に対する鍵長の選択指針(2/2)

- ドメインパラメーターにおける素数 p のサイズ
  - DSA、NIST FIPS 186-3(June 2009)
    - Nのサイズ 1024, 2048, 3072ビットの3種類を推奨していた。
  - DH、NIST SP 800-56A(March 2007)
    - pのサイズ 1024, 2048ビットの2種類を推奨していた。
- Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST SP 800-131A(January 2011)では、
  - 1024ビットの場合は
    - 「Acceptable through 2010, Deprecated from 2011 through 2013, Disallowed after 2013」
  - 2048ビット以上の場合は
    - 「Acceptable」

  とされている。

IFP, ECLPD, DLP以外

ポスト量子暗号
（Post-Quantum Cryptography）

- 1994年、Shorアルゴリズム：素因数分解問題と離散対数問題に対して量子計算モデルでの多項式時間解法

- 2001年、IBMが7-qbitの核磁気共鳴NMR量子コンピュータにより素因数分解実験(n=15)に成功

- 公開鍵暗号を構成する別の数学問題は？

  NP困難：符号理論、格子理論、多変数多項式など

完全準同型暗号
(Fully Homomorphic Encryption)

- 2009年、IBMのGentryは格子理論により、加法と乗法の両方を満たす準同型暗号を構成
- 暗号化した状態でデータ処理が可能であるため、クラウドコンピューティングでの秘匿計算に適している
- 整数、代数体イデアル、Ring-LWE などによる構成法も提案されている

多重線形性写像（Multi-linear Map）

- 2012年、Garg-Gentry-Halevi は格子理論により、ペアリングを3個以上のペアに拡張した。

$$
\begin{aligned}
& e(aP_1, P_2, \cdots, P_k) \\
&= e(P_1, aP_2, \cdots, P_k) \\
&\cdots \\
&= e(P_1, P_2, \cdots, aP_k) \\
&= e(P_1, P_2, \cdots, P_k)^a
\end{aligned}
$$

多重線形性を用いて新たな暗号プロトコルが構成可能

Thank you!