Institute of Mathematics for Industry
Kyushu University

次世代公開鍵暗号に関する研究の最前線

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/

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

公開鍵の例

RSA暗号 (1024 bits)

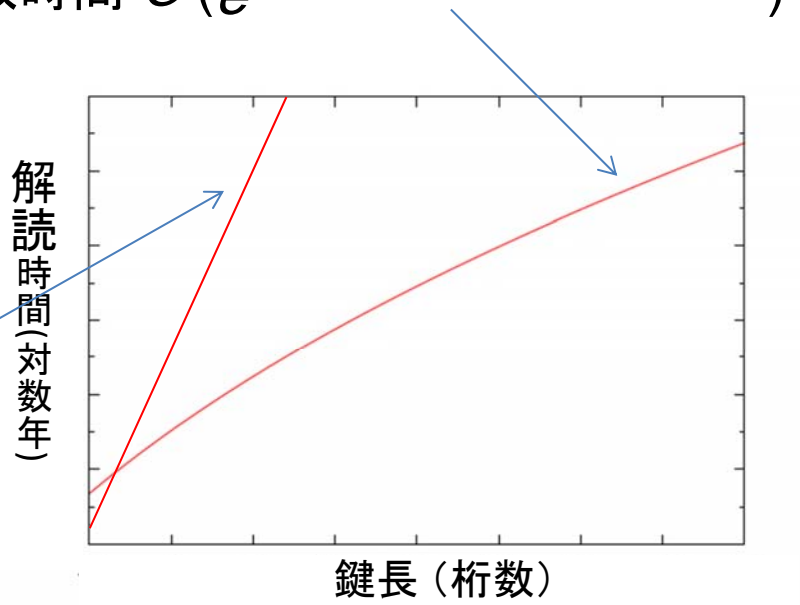
N = 826ed558a0f0cba7ae09485abf80c544837efeb7116153f5d6479d5945fdb6c61f50c984445d601d85eceb6b
ad9f700b90ae28984dd590f5ca3e6ed968a3ca32a5cf584992d92590ae9ed4f81b70d008a9e4a16905925dbb
79d82b67dc6b70869a83f037c147d298c0e2eea5f858f3881ad1071c5c221ecb795d78b68bae7863

素因数分解 → 一般数体篩法: 準指数時間 $O(e^{(c+o(1))(\log N)^{1/3}(\log\log N)^{2/3}})$

楕円曲線暗号 (160 bits)

x = 4a96b568 8ef57328 46646989 68c38bb9 13cbfc82
y = 23a62855 3168947d 59dcc912 04235137 7ac5fb32

楕円曲線上の離散対数問題
→ρ法: 指数時間 $O(2^{n/2})$
n: 鍵長(ビット)



素因数分解問題

問題: 次の整数を素因数分解せよ。

- 15
- 187
- 1961
- 16637
- ...

素因数分解問題

問題: 次の整数を素因数分解せよ。

- $15 = 3 \times 5$
- $187 = 11 \times 17$
- $1961 = 37 \times 53$
- $16637 = 127 \times 131$
- ・・・

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

CRYPTREC Report 2011 (http://www.cryptrec.jp/)

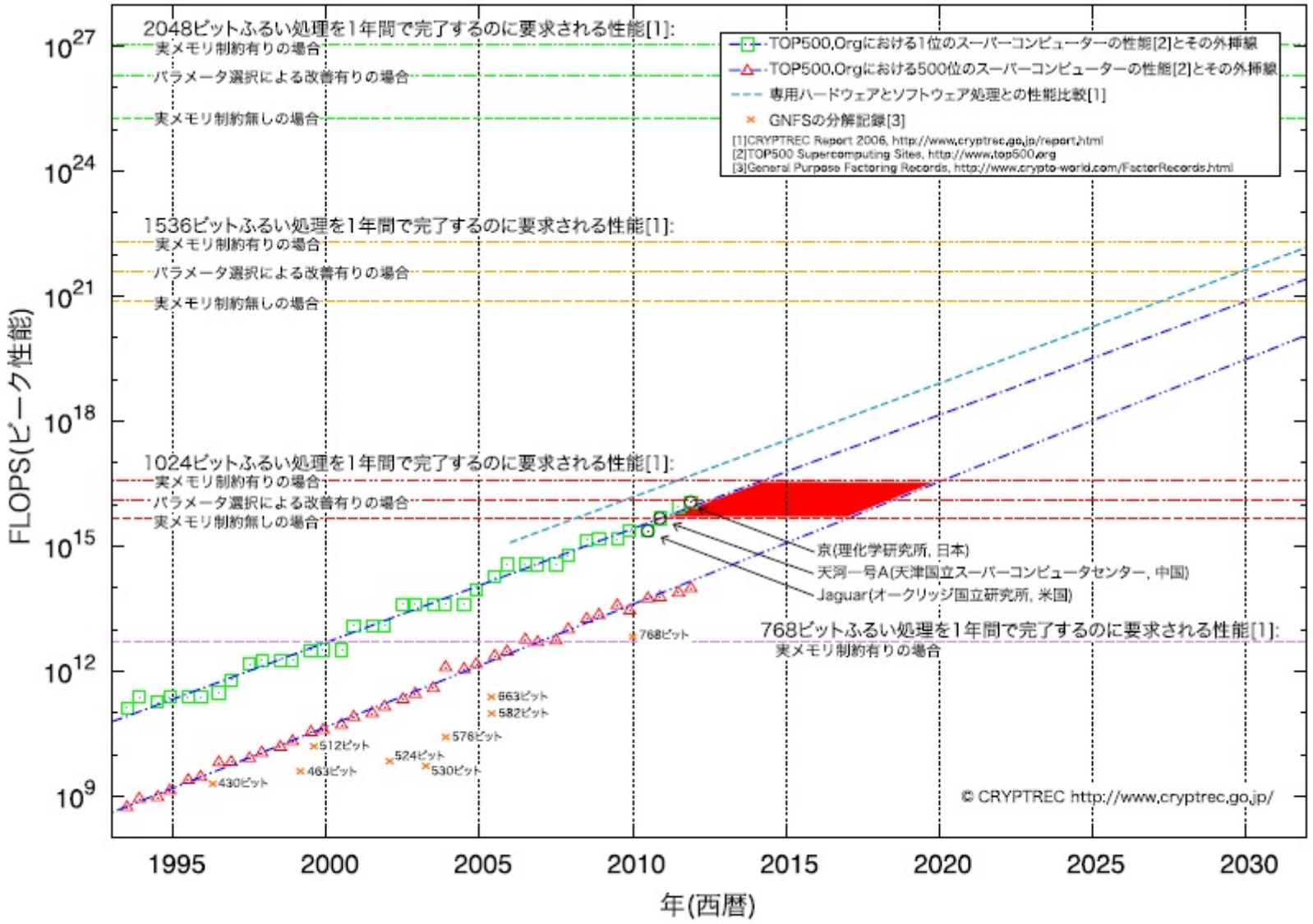
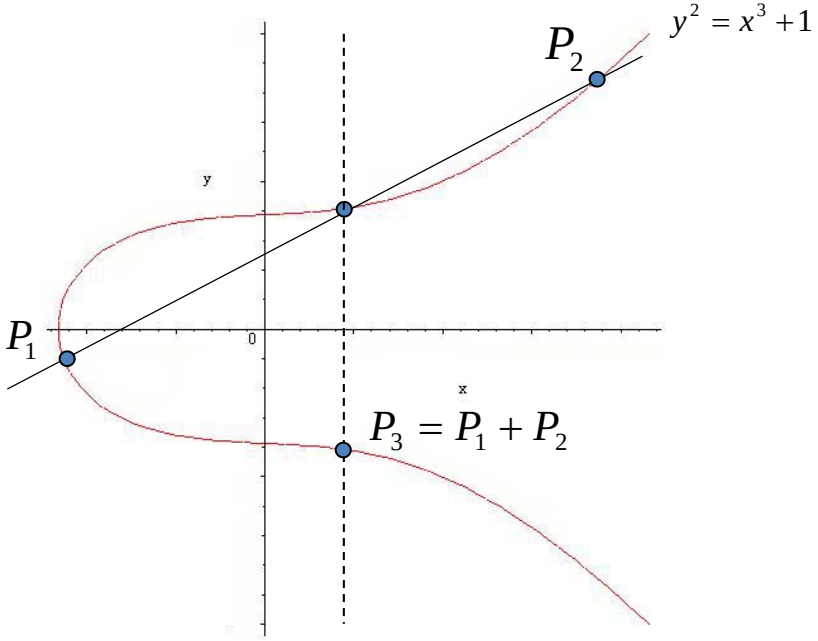


図 4.2：1 年間でふるい処理を完了するのに要求される処理能力の予測(2011 年 12 月更新)

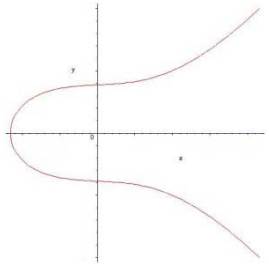
楕円曲線暗号

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

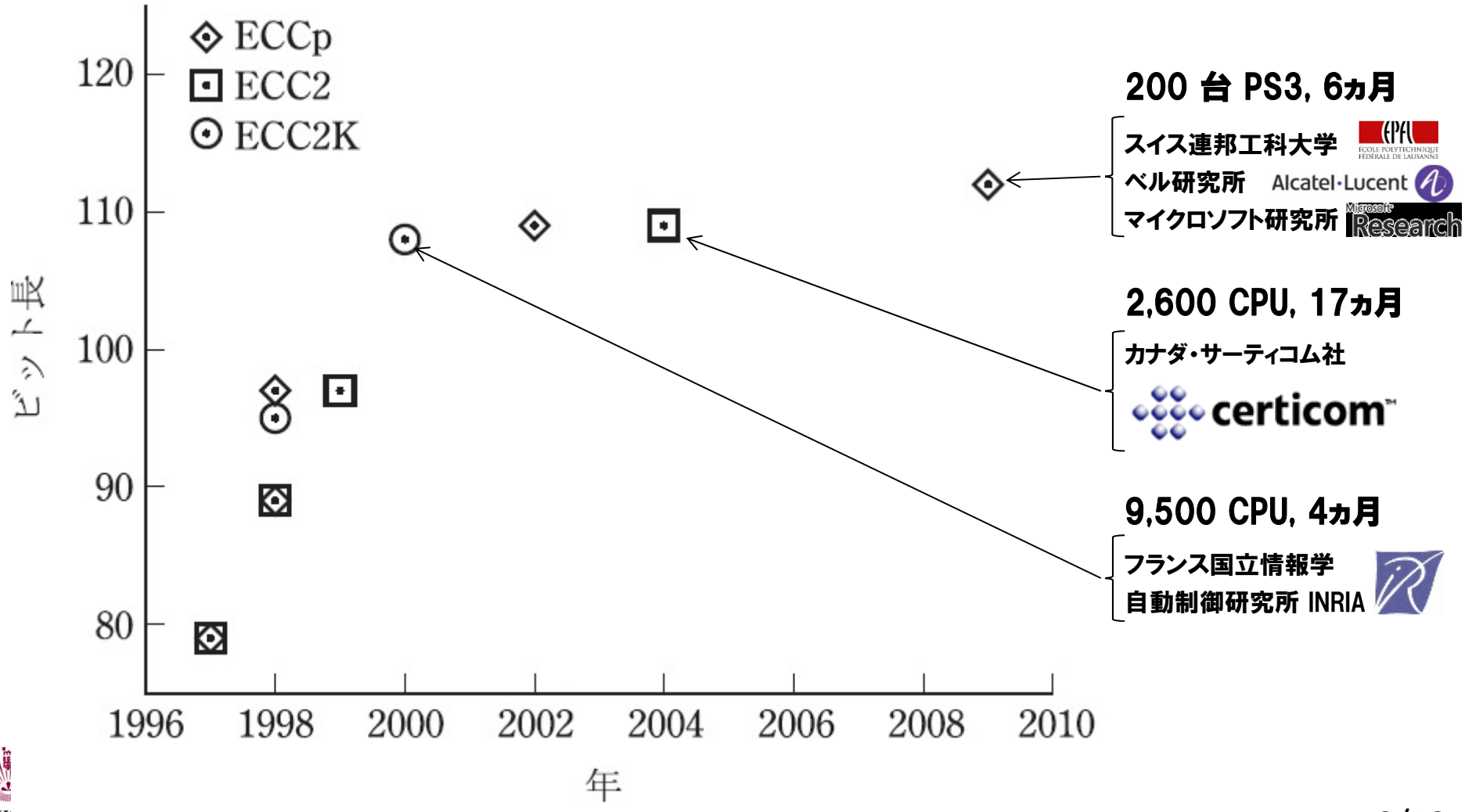


- 楕円曲線暗号の安全性　≒ 楕円曲線上の離散対数問題

「aP = Q を満たす秘密鍵 a を求めよ。」



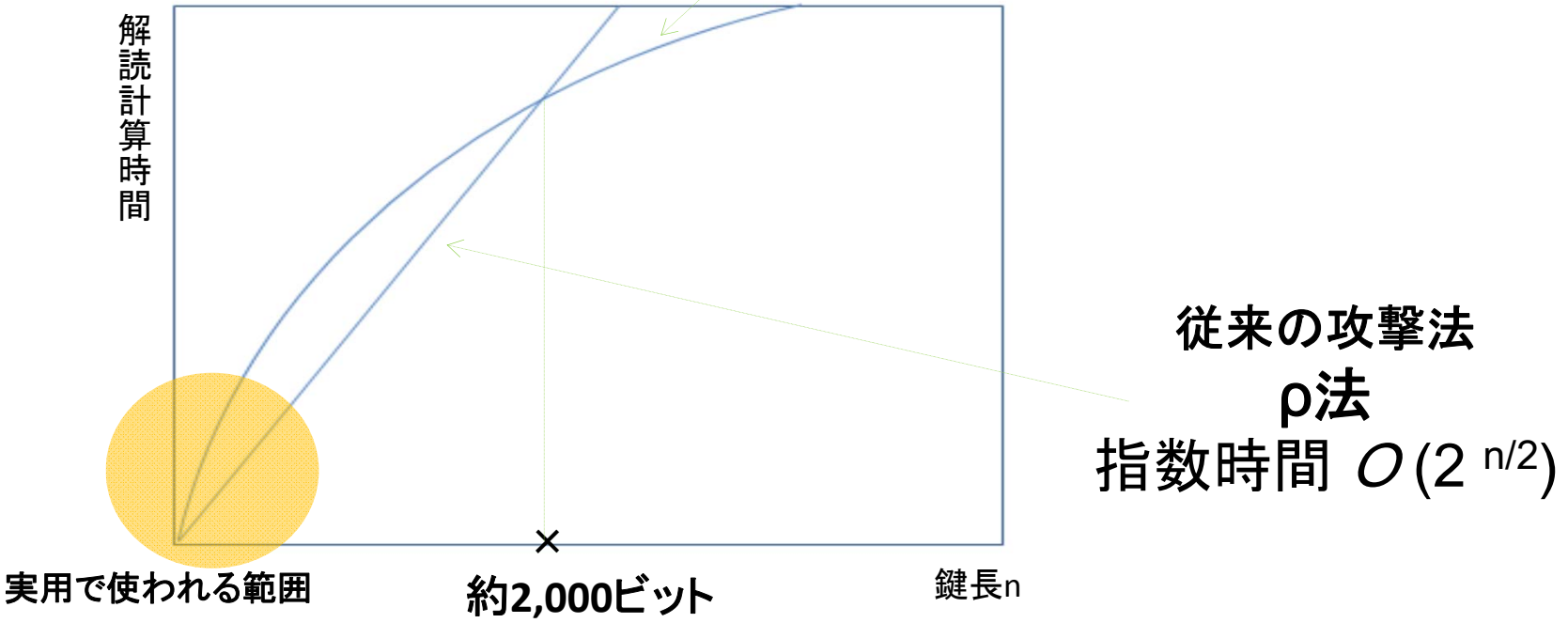
楕円曲線上の離散対数問題
解読世界記録の推移



KYUSHU UNIVERSITY

Faugère *et al.*のアルゴリズム

- 指数計算法をグレブナ基底を利用した高速化
- Petit-Quisquaterは、Asiacrypt 2012において、この計算時間を準指数時間$O(2^{c\, n^{2/3} \log n})$と見積もる。



IDベース暗号

- 公開鍵の例

RSA暗号 → 2個の素数の積

n = 826ed558a0f0cba7ae09485abf80c544837efeb7116153f5d6479d5945fdb6c61f50c984445d601d85eceb6b
ad9f700b90ae28984dd590f5ca3e6ed968a3ca32a5cf584992d92590ae9ed4f81b70d008a9e4a16905925dbb
79d82b67dc6b70869a83f037c147d298c0e2eea5f858f3881ad1071c5c221ecb795d78b68bae7863

楕円曲線暗号 → 楕円曲線上のランダムな点

x = 4a96b568 8ef57328 46646989 68c38bb9 13cbfc82
y = 23a62855 3168947d 59dcc912 04235137 7ac5fb32

IDベース暗号 → 鍵長以下の自由なビット列
(氏名、email アドレス，携帯電話の番号，基礎年金番号など)

ペアリング暗号

- 鍵隔離暗号 (Key-Insulated Encryption)
- 代理再暗号化 (Proxy Re-encryption)
- キーワード検索暗号 (Keyword Searchable Encryption)
- 放送暗号 (Broadcast Encryption)
- グループ署名 (Group Signature)
- 属性暗号 (Attribute-based Encryption)
- 関数型暗号 (Functional Encryption)
- ・・・

ペアリング暗号の安全性

- $e: E(GF(p)) \times E(GF(p)) \rightarrow GF(p^k)$

  $E(GF(p))$: 楕円曲線
  $GF(p^k)$: 有限体

- 双線形性

$$e(aP, Q) = e(P, aQ) = e(P, Q)^a$$

$P \in E(GF(p))$, $Q \in GF(p^k)$, $a \in Z$

ペアリング暗号の安全性 ≒ 有限体上の離散対数問題解読

有限体GF(p)

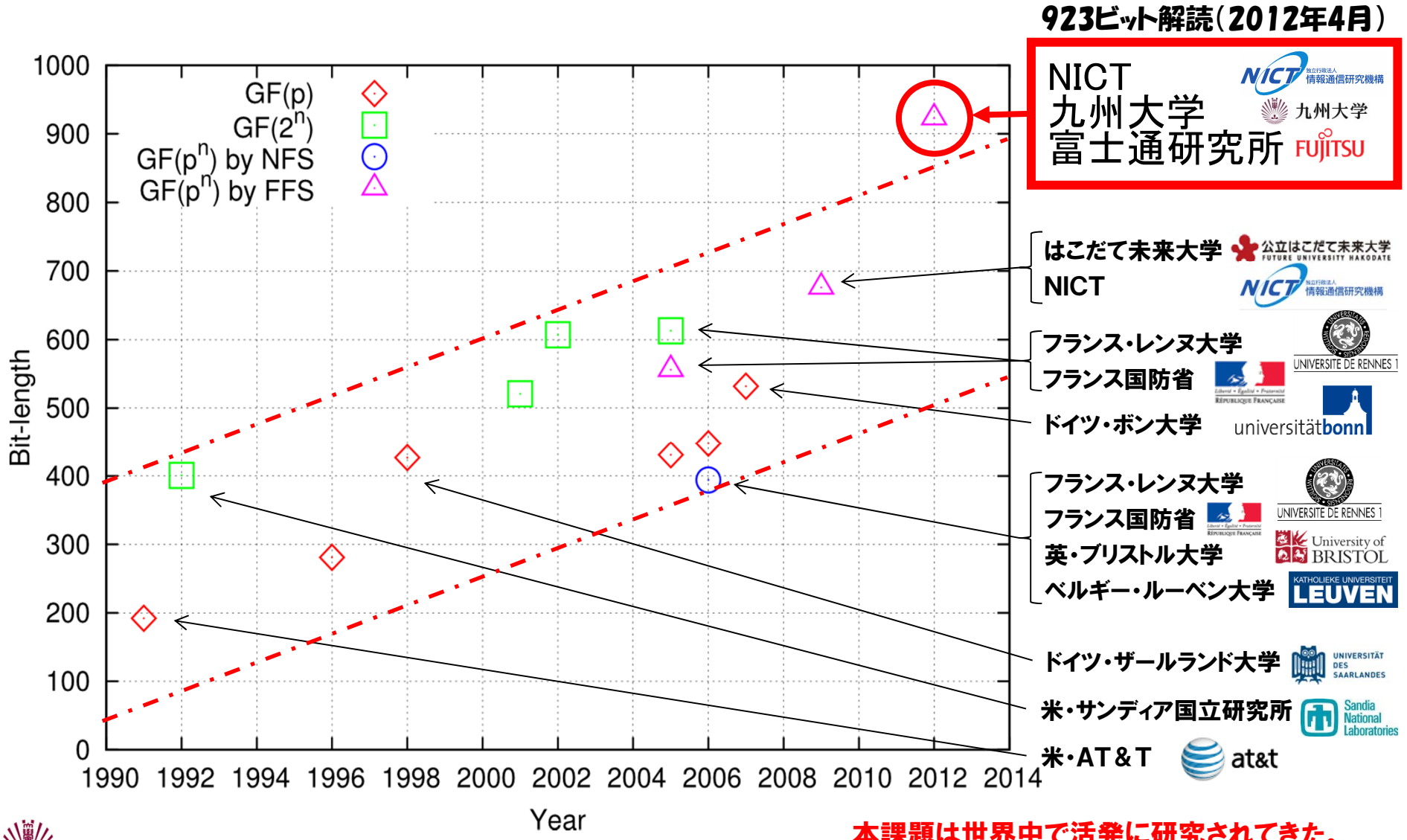
- 素数 p=11,
- 有限体 GF(p)* = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

- $2^1 = 2$
- $2^2 = 4$
- $2^3 = 8$
- $2^4 = 16 = 1x11 + 5 = 5$
- $2^5 = 2^4x2 = 5x2 = 10$
- $2^6 = 10x2 = 1x11 + 9 = 9$
- $2^7 = 18 = 7$
- $2^8 = 14 = 3$
- $2^9 = 6$
- $2^{10} = 12 = 1$

- 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



本課題は世界中で活発に研究されてきた。

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!
Q&A