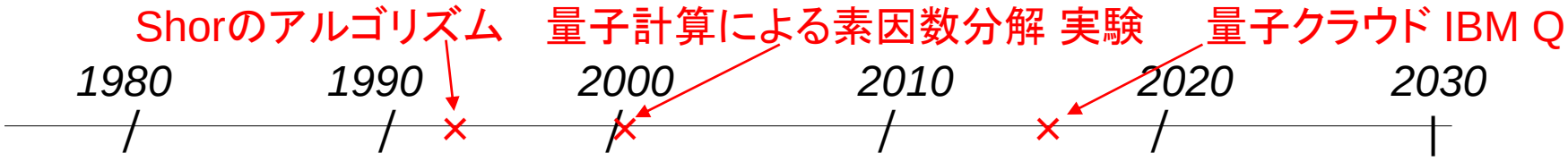
情報・システム工学概論

公開鍵暗号の数理（2回目）

高木　剛

東京大学工学部計数工学科

公開鍵暗号の歴史



RSA暗号 (素因数分解問題)

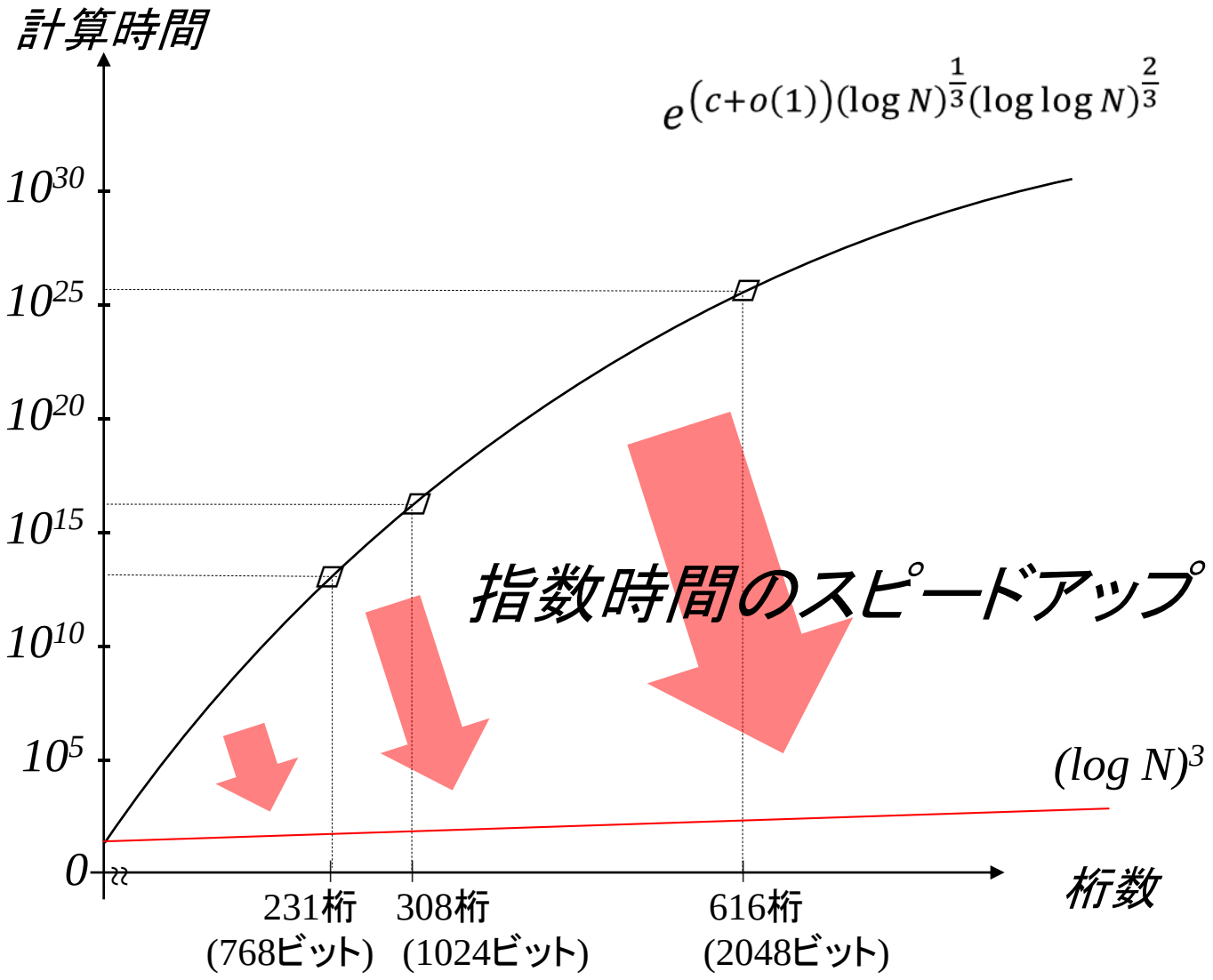
広く普及　楕円曲線暗号 (離散対数問題)

量子計算機で危殆化!!

耐量子計算機暗号
Post-Quantum Cryptography (PQC)
符号理論、格子理論, 多変数多項式,etc

研究段階

Shorの素因数分解アルゴリズム



量子クラウド IBM Q

https://www.research.ibm.com/ibm-q/ より転載

2017年11月、20量子ビットの量子コンピュータ
50量子ビットまで拡張予定

2018年3月、Googleも72量子ビットの「Bristlecone」を発表した

耐量子計算機暗号の研究動向

- **2015年8月：アメリカ国家安全保障局(NSA)は、耐量子計算機暗号への将来的な移行プランを発表した。**
  https://www.nsa.gov/ia/programs/suiteb_cryptography/

- **最近の耐量子計算機暗号関係のワークショップ**

2015年1月, DIMACS Workshop on The Mathematics of Post-Quantum Cryptography
http://dimacs.rutgers.edu/Workshops/Post-Quantum/

2015年4月, NIST Workshop on Cybersecurity in a Post-Quantum World
http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm

2015年9月, Dagstuhl Seminar - Quantum Cryptanalysis
https://www.dagstuhl.de/en/program/calendar/semhp/?semnr=15371

2015年10月, ESTI Workshop on Quantum-safe Cryptography

2016年2月, PQCrypto 2016: https://pqcrypto2016.jp/

- **耐量子計算機暗号関係の大型研究プロジェクト**

Post-quantum cryptography for long-term security: http://pqcrypto.eu.org/

CROSSING: https://www.crossing.tu-darmstadt.de/

JST CREST 暗号数理: https://cryptomath-crest.jp/

- 参加者240名(北米80名、欧州60名、アジア60名、日本40名)
- NISTが耐量子計算機暗号の標準化計画を発表した

NIST PQC 標準化計画

http://csrc.nist.gov/groups/ST/post-quantum-crypto/

公開鍵暗号プリミティブを公募(2017年11月30日〆切)

- 鍵交換方式 (key exchange)
- 暗号化 (public-key encryption)
- ディジタル署名 (digital signature)

公募〆切後、3～5年かけて安全性と効率性を評価する。

利用される数学問題

- 格子暗号 (Lattice-based cryptography)
- 符号暗号 (Code-based cryptography)
- 多変数多項式暗号 (Multivariate polynomial cryptography)
- ハッシュ関数署名 (Hash-based signature)
- 同種写像暗号 (Isogeny-based cryptography)

応募状況 (69件)

- **格子暗号 (24件)**

Compact LWE, CRYSTALS-DILITHIUM, CRYSTALS-KYBER, Ding Key Exchange, DRS, EMBLEM and R.EMBLEM, FALCON, Frodo, HILA5, KINDI, LAC, LIMA, Lizard, LOTUS, NewHope, NTRU-HRSS-KEM, NTRU Prime, NTRUEncrypt, Odd Manhattan, pqNTRUSign, qTESLA, Round2, SABER, Titanium

- **符号暗号 (16件)**

BIG QUAKE, BIKE, Classic McEliece, DAGS, Edon-K, HQC, LEDAkem, LEDApkc, McNie, NTS-KEM, pqsigRM, QC-MDPC KEM, RaCoSS, Ramstake, RLCE-KEM, RQC

- **多変数多項式暗号 (10件)**

CFPKM, DME, DualModeMS, GeMSS, Gui, HiMQ-3, LUOV, MQDSS, Rainbow, SRTPI

- **ハッシュ関数署名 (2件)**

Gravity-SPHINCS, SPHINCS+

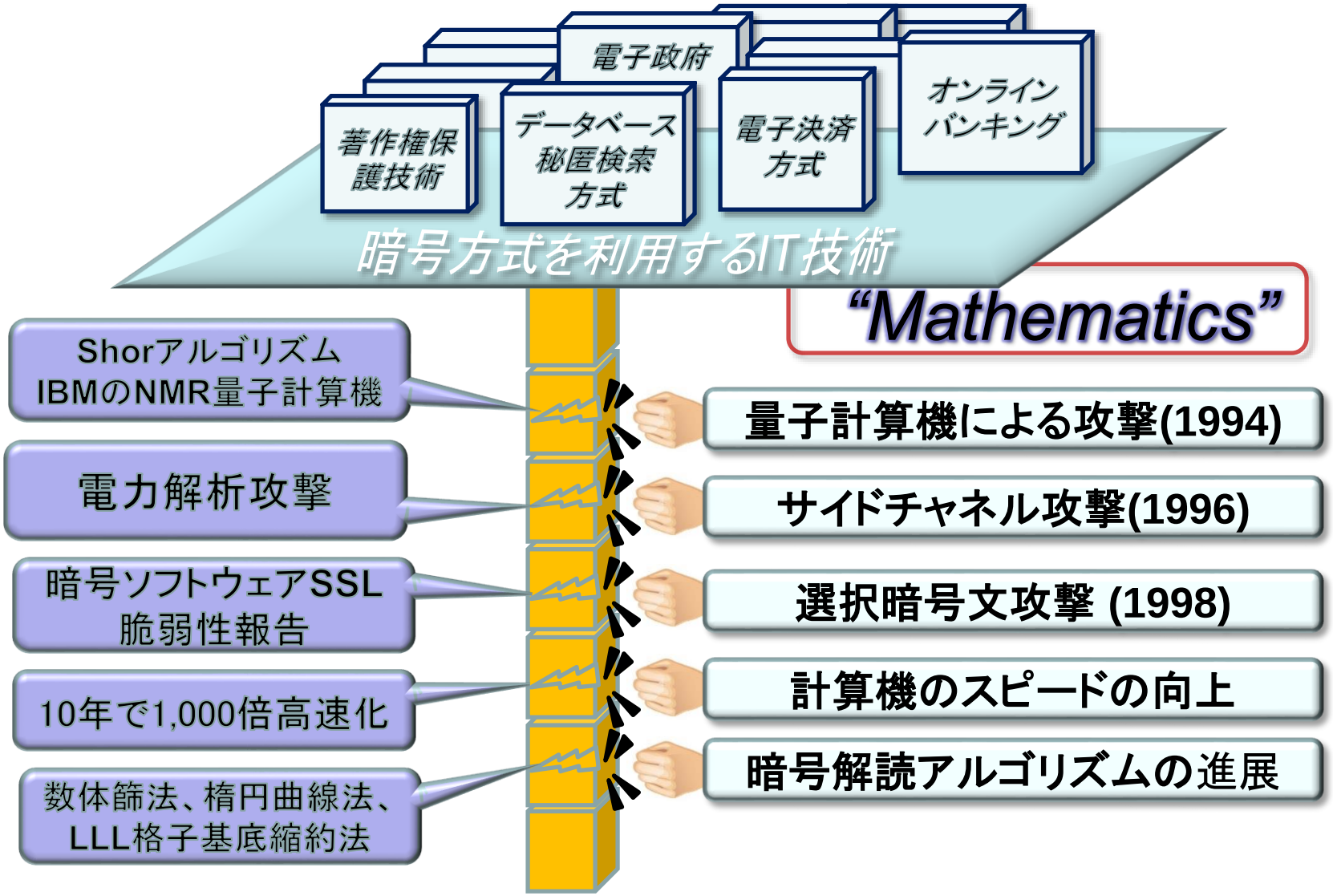
- **同種写像暗号 (1件)**

SIKE

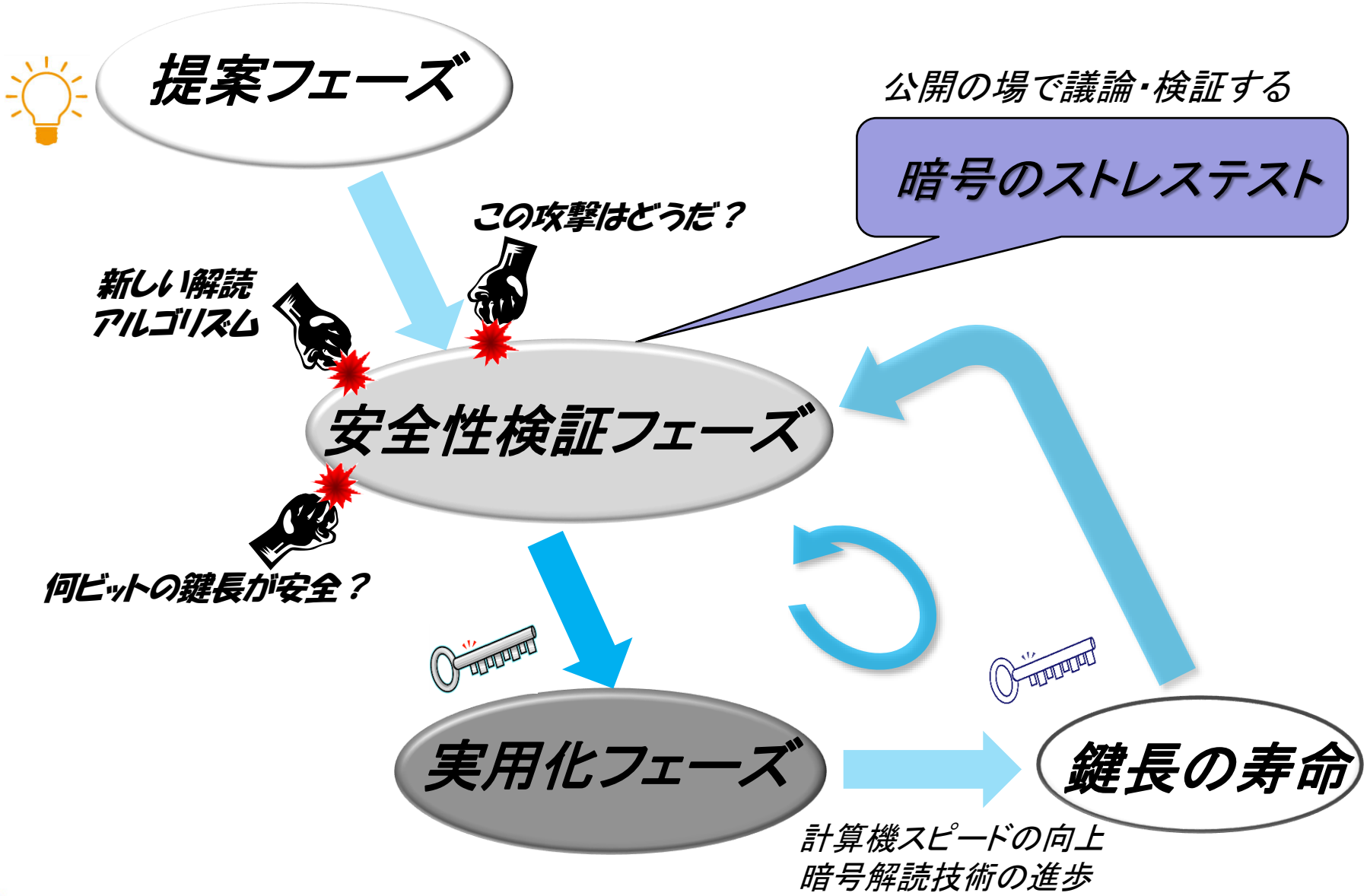
- **その他 (16件)**

Giophantus, Guess Again, HK17, LAKE, Lepton, LOCKER, Mersenne-756839, OKCN/AKCN/CNKE, Ouroboros-R, Picnic, Post-quantum RSAEncryption, Post-quantum RSASignature, RankSign, RVB, Three Bears, WalnutDSA

暗号の様々な危殆化リスク



暗号の安全性検証サイクル



多変数多項式暗号

多変数多項式求解問題 (MQ問題)

簡単な例：Z_7={0,1,2,…,6}を係数とする3個の2変数多項式

$$\begin{cases} f_1(x_1,x_2) = 2x_1^2 + 5x_1x_2 + x_2^2 + 3x_1 + 5x_2 + 1 \\ f_2(x_1,x_2) = 6x_1^2 + 4x_1x_2 + 2x_1 + 6x_2 + 2 \\ f_3(x_1,x_2) = 3x_1^2 + 6x_1x_2 + 6x_1 + 2x_2 + 3 \end{cases}$$

$f_1(x_1,x_2) = f_2(x_1,x_2) = f_3(x_1,x_2) = 0$ を満たす解を一つ求める.

MQ問題

有限体F_q上を係数とするm個のn変数の
2次多項式の共通解をひとつ求めよ:

$$\begin{cases} f_1(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)} = d_1 \\ f_2(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(2)} x_i x_j + \sum_{1\le i\le n} b_i^{(2)} x_i + c^{(2)} = d_2 \\ \vdots \\ f_m(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)} = d_m \end{cases}$$

$a_{ij}^{(k)}, b_i^{(k)}, c^{(k)}, d_k$ は有限体GF(q)の元とする。

グレブナー基底

MQ問題を解く計算量 *[3]*

$$O((m\binom{n+d_{reg}-1}{d_{reg}})^{\omega})$$

ここで、$2<\omega<3$ として、d_{reg} は多変数多項式システムから決まる定数.

Reference:

[1] Faugère, J.C., A New Efficient Algorithm for Computing Gröbner Bases (F4)", Journal of Pure and Applied Algebra, vol. 139, 1999.

[2] Faugère, J.C., A New Efficient Algorithm for Computing Gröbner Bases (F5)", ISSAC, ACM, 2002.

[3] Bettale, L., Faugère, J.C. and Perret L., Hybrid approach for solving multivariate systems over finite fields", J. Math. Crypt. vol. 2, 2008.

表 3　MQ Challenge における 6 種類の型

型	Schemes	m, n	有限体
I	暗号方式	$m = 2n$	$\mathbb{F}_2$
II	暗号方式	$m = 2n$	$\mathbb{F}_{2^8}$
III	暗号方式	$m = 2n$	$\mathbb{F}_{31}$
IV	ディジタル署名	$n \approx 1.5m$	$\mathbb{F}_2$
V	ディジタル署名	$n \approx 1.5m$	$\mathbb{F}_{2^8}$
VI	ディジタル署名	$n \approx 1.5m$	$\mathbb{F}_{31}$

2015年4月スタート

https://www.mqchallenge.org/

Fukuoka MQ Challenge

Type I | Type II | Type III | Type IV | Type V | Type VI

	Number of Variables (n)	Seed (0,1,2,3,4)	Date	Contestants	Computational Resource	Data
1	74	0	2016/12/17	Antoine Joux	New hybridized XL related algorithm, Heterogeneous cluster of Intel Xeon @ 2.7-3.5 Ghz	Details
2	74	4	2017/11/15	Kai-Chun Ning, Ruben Niederhagen	Parallel Crossbred, 54 GPUs in the Saber cluster	Details

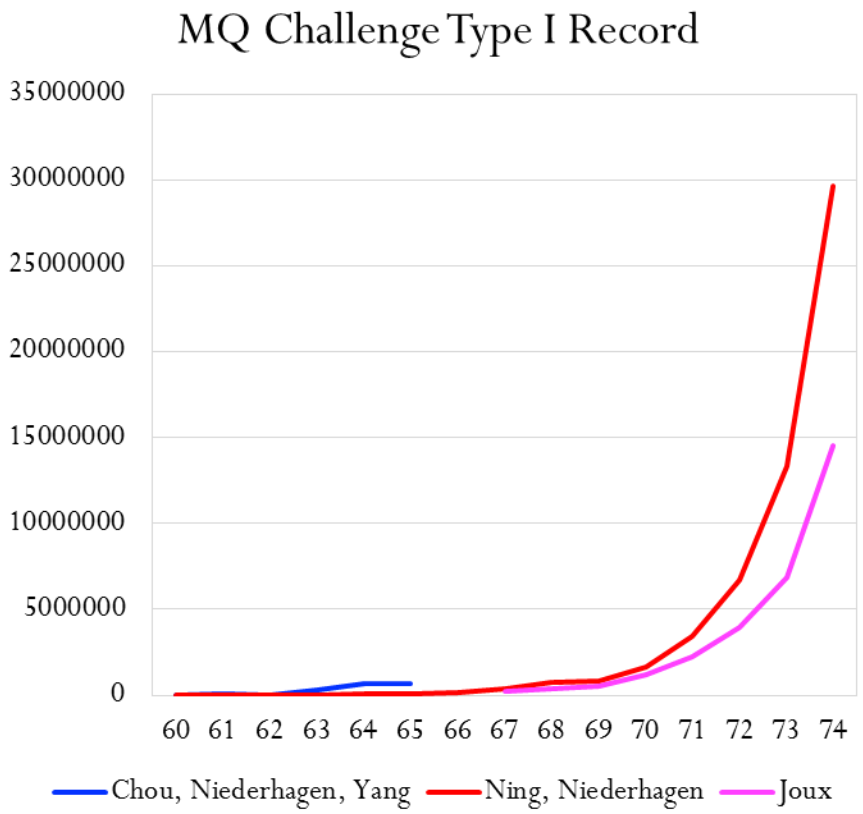
18 hours
448 cores

32.86 hours
54 GPUs

現在の世界記録 – Type I (GF(2), $m = 2n$)

n	m	*time* Chou, Niederhagen, Yang	*time* Ning, Niederhagen	*time*0.01* Joux
60	120	23537	5976	-
61	122	80245	11268	-
62	124	30553	21888	-
63	126	266460	35316	-
64	128	654780	49824	-
65	130	1001580	92484	-
66	132	676200	184284	-
67	134	-	354204	221184
68	136	-	772020	405504
69	138	-	824760	552960
70	140	-	1629540	1179648
71	142	-	3409920	2211840
72	144	-	6722784	3922329
73	146	-	13323132	6871449
74	148	-	29649780	14515200 (?)

unit: second



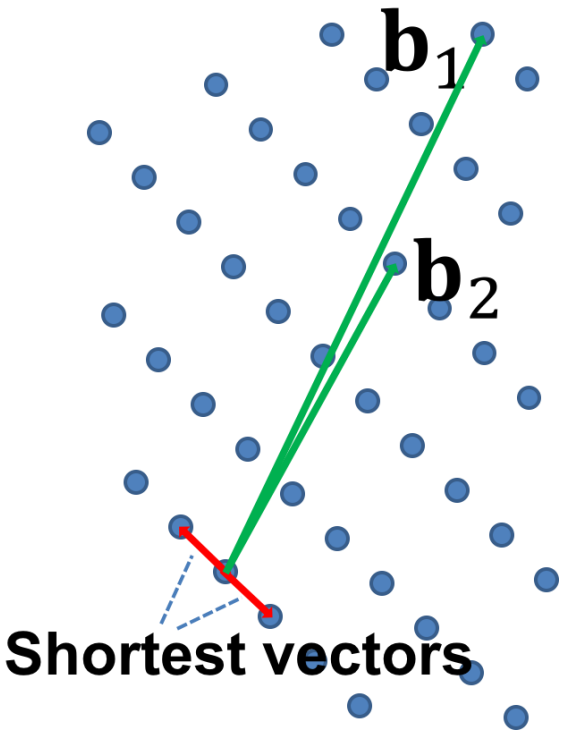
格子暗号

格子暗号の安全性

1次独立なベクトル $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ の整数係数の線形和全体

格子 $L(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \{\sum_{t=1}^{n} x_t \mathbf{b}_t, x_t \in \mathbb{Z}\}$.

Shortest Vector Problem (SVP)
Input: 格子Lの基底 $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$
Output: 非零の最短ベクトル

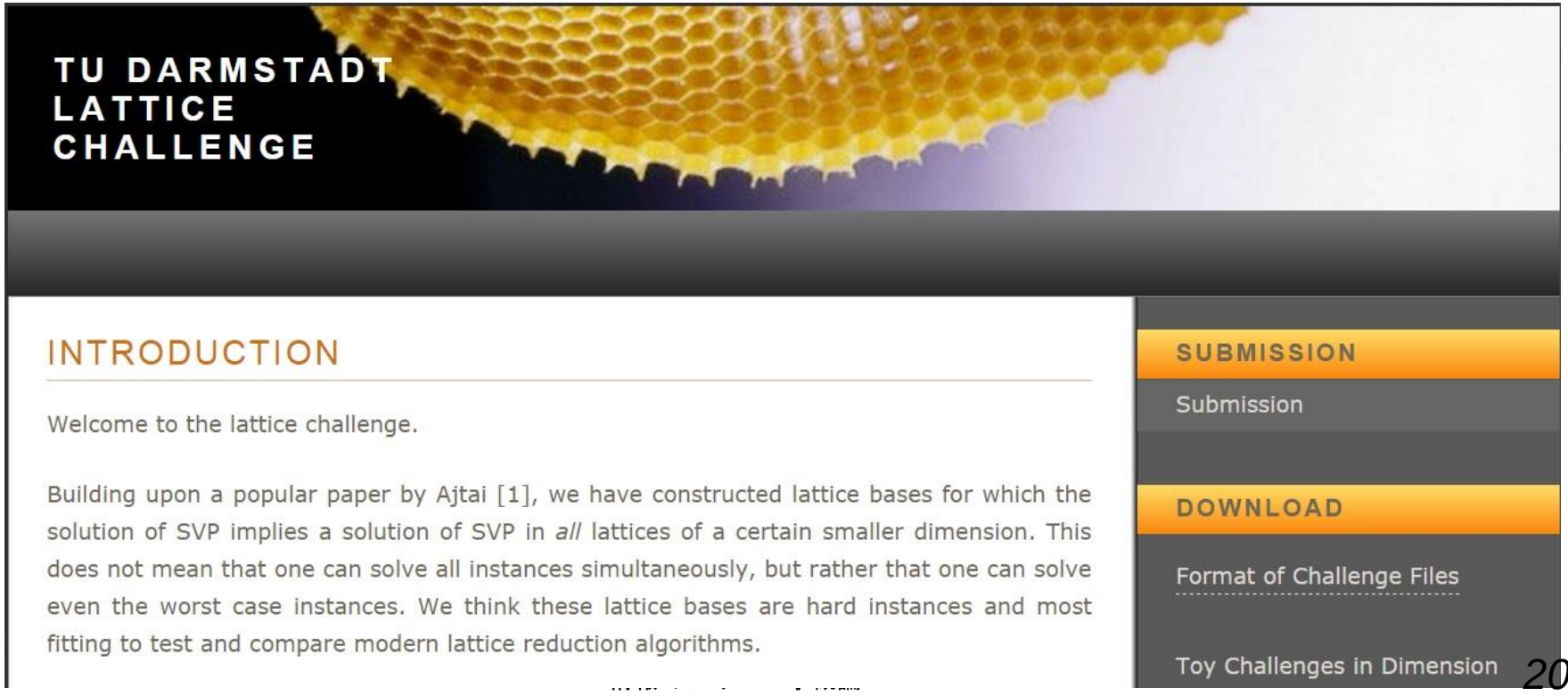


NP-hard な問題として暗号で利用
Ajtai 1996, Regev 2005など

Darmstadt 格子チャレンジ

https://www.latticechallenge.org/

- SVP チャレンジ / 格子チャレンジ (2008年から)
- イデアル格子チャレンジ (2013年から)
- LWE チャレンジ (2016年から)



SVP・近似版SVP

Gaussian Heuristics (GH):
最短ベクトルの長さは以下で見積もられる。

$$\frac{\Gamma(n/2+1)^{1/n}}{\sqrt{\pi}} \cdot (\det \mathcal{L})^{1/n}$$

- SVPチャレンジ

$$1.05 \cdot \frac{\Gamma(n/2+1)^{1/n}}{\sqrt{\pi}} \cdot (\det \mathcal{L})^{1/n}$$

- 近似版イデアル格子チャレンジ

$$n \cdot (\det \mathcal{L})^{1/n}$$

SVPを解く高速なアルゴリズム

(1) 格子基底縮約法

LLL (Lenstra–Lenstra–Lovász)アルゴリズム

BKZ (Block Korkine-Zolotarev)アルゴリズム

- 多項式時間 + 指数時間の総当り探索

(2) 列挙法 (Extreme pruning [Gama-Nguyen-Regev 2010])

- 時間: $2^{O(n^2)}$, メモリ: 多項式サイズ

(3) 篩法 (Gauss sieve algorithm [Micciancio-Voulgaris 2010])

- 時間: $2^{O(n)}$, メモリ: $2^{O(n)}$

(4) その他

イデアル格子

- 暗号の構成で、円分多項式 $g(x) = x^{2^h} + 1$など
  で生成されるイデアル格子が利用される。

- [Micciancio-Voulgaris 2010] ベクトルの巡回構造
  を利用した イデアル格子に対する篩法の高速化

- [Schneider 2011] $g(x) = x^{32} + 1$ で生成される
  イデアル格子に対して篩法の10倍の高速化

128次元イデアル格子チャレンジ

- イデアル格子 $g(x) = x^{128} + 1$
- 2,688 スレッド Amazon EC2
- 合計約30,000 CPU 時間
- ランダム格子から約60倍高速

HALL OF FAME

Position	Dimension	Index	Seed	Euclidean norm	Contestant	Solution	Using Ideal Structure	Subm. Date
1	128	256	0	2959	Tsukasa Ishiguro, Shinsaku Kiyomoto, Yutaka Miyake, Tsuyoshi Takagi	vec	yes	2013-04-11
2	108	324	0	2669	Tsukasa Ishiguro, Shinsaku Kiyomoto, Yutaka Miyake, Tsuyoshi Takagi	vec	yes	2013-03-8
3	100	202	0	2660	Po-Chun Kuo, Po-Hsiang Hao	vec	no	2013-02-21

近似版イデアル格子チャレンジ

Progressive BKZの計算量理論値

Dimension	$n \cdot \det^{1/n}$	
	blocksize	$\log_2(\text{Time[sec]})$
550	77	17.5
600	102	20.1
650	114	24.3
700	124	28.5
800	145	40.2
900	163	52.5
1000	182	67.2

SVP HALL OF FAME

Position	Dimension	Index	Seed	Euclidean norm	Contestant	Solution
1	130	131	0	2912	Shang-Yi Yang	vec
2	130	262	0	3000	Jean-Christophe Deneuville	vec
3	130	262	0	3004	Kenji KASHIWABARA and Tadanori TERUYA	vec
4	128	255	0	2924	Kenji KASHIWABARA and Tadanori TERUYA	vec
5	128	256	0	2959	Tsukasa Ishiguro, Shinsaku Kiyomoto, Yutaka Miyake, Tsuyoshi Takagi	vec

APPROX-SVP HALL OF FAME

Position	Dimension	Index	Seed	Euclidean norm	Contestant	Solution
1	652	653	0	626850	Yuntao Wang; Yoshinori Aono; Takuya Hayashi; Tsuyoshi Ta	ec
2	652	653	0	626936	Yuntao Wang; Yosh... Takuya Hayashi; Tsuyoshi Takagi	vec
3	652	653	0	661210	Jean-Christophe Deneuville	vec
4	652	653	0	661349	Yuntao Wang, Yoshinori Aono, Takuya Hayashi, Tsuyoshi Takagi	vec
5	600	601	0	542883	Jean-Christophe Deneuville	vec

$2^{24.0}$ sec

652次元を194日(1コア)で解読

処理性能の例 – メモリ量と演算速度

格子暗号 Ding Key Exchange (鍵交換) AES 128 レベルの安全性	**多変数多項式暗号** Rainbow (ディジタル署名) AES 128 レベルの安全性	**符号暗号** Classic McEliece (暗号化) AES 256 レベルの安全性
アリス: 848 バイト ボブ: 896 バイト	公開鍵: 148.5 キロバイト 秘密鍵: 97.9 キロバイト 署名: 64バイト	公開鍵: 1357.8キロバイト 秘密鍵: 14.1 キロバイト 暗号文: 240 バイト
鍵生成: 1.31 ミリ秒 暗号化: 1.71 ミリ秒 復号化: 1.19 ミリ秒	鍵生成: 394 ミリ秒 署名生成: 0.182 ミリ秒 署名検証: 0.106 ミリ秒	鍵生成: 1938.1 ミリ秒 暗号化: 0.095 ミリ秒 復号化: 0.148 ミリ秒

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions

まとめ

- 耐量子計算機暗号の最新動向
  米国標準技術研究所NISTによる標準化計画
- 多変数多項式の求解問題(MQ 問題)
  Fukuoka MQチャレンジ
- 格子理論での最短ベクトル問題(SVP)
  Darmstadt 格子チャレンジ
- 想定される攻撃者の計算限界を評価
  暗号解読コンテストの継続的な実施