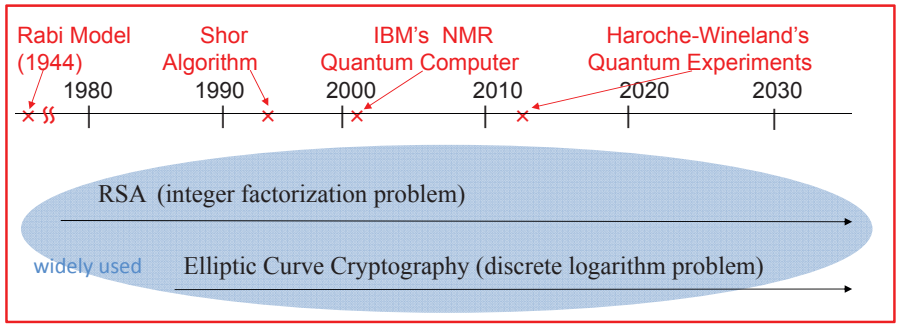
Recent Developments in Post-Quantum Cryptography

Tsuyoshi Takagi

Department of Mathematical Engineering
University of Tokyo, Japan

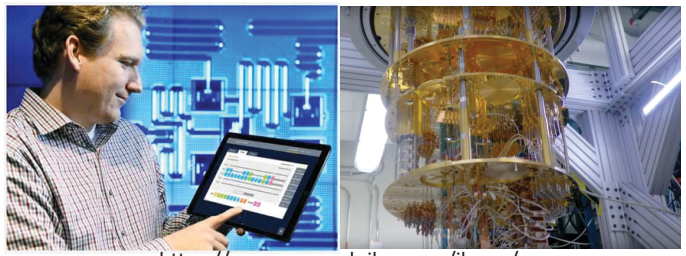
History of Public-Key Cryptography



These cryptosystems are no longer secure in the era of quantum computer.

Post-quantum cryptography (PQC)
(coding, multivariate polynomial, lattice, isogeny, etc)
research phase

Quantum Cloud - IBM Q



https://www.research.ibm.com/ibm-q/

Currently IBM Q has 20 qubits in November 2017, and they plan to extend it to 50 qubits in a few years.

Google also tries to build a 72-qubit Processor.

Trend in Post-Quantum Cryptography

- **National Security Agency (NSA)** announced preliminary plans for transitioning to quantum resistant algorithms in August 2015
  https://www.nsa.gov/ia/programs/suiteb_cryptography/

- **Some Workshops in 2015-2016**

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

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

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

November 2015, ESTI Workshop on Quantum-safe Cryptography

February 2016, PQCrypto 2016: https://pqcrypto2016.jp/

- **Big Research Projects**

Post-quantum cryptography for long-term security: http://pqcrypto.eu.org/
CROSSING: https://www.crossing.tu-darmstadt.de/
JST CREST CryptoMath: https://cryptomath-crest.jp/

PQCrypto 2016

https://pqcrypto2016.jp/
Nishijin Plaza, Kyushu University

The Seventh International Conference on Post-Quantum Cryptography

Fukuoka, Japan, February 24-26, 2016

- More than 240 participants (USA/Canada 70, Europe 60, Asia 60, Japan 40, others 10)

- NIST announced preliminary plans for transitioning to quantum resistant algorithms.

NIST PQC Standardizations

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

Deadline: November, 2017

Public-Key Cryptography Primitives
- digital signatures
- encryption
- Key-establishment (KEMs)

Some Candidates of PQC (NISTIR 8105)
- Hash-based signature
- Code-based cryptography
- Multivariate polynomial cryptography
- Lattice-based cryptography
- Isogeny-based cryptography

69 proper submissions

- **Lattice-based (24 submissions)**

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

- **Code-based (16 submissions)**

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

- **Multivariate Polynomial (10 submissions)**

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

- **Hash-based (2 submissions)**

Gravity-SPHINCS, SPHINCS+

- **Isogeny-based (1 submission)**

SIKE

- **Others (16 submissions)**

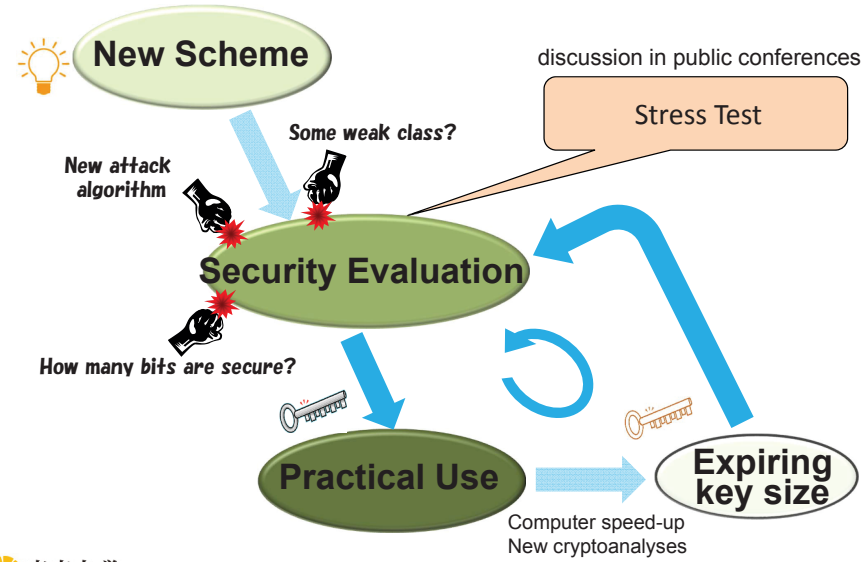
Giophantus, Guess Again, HK17, LAKE, Lepton, LOCKER, Mersenne-756839, OKCN/AKCN/CNKE, Ouroboros-R, Picnic, Post-quantum RSAEncryption, Post-quantum RSASignature, RankSign, RVB, Three Bears, WalnutDSA

Time line of NIST PQC Project

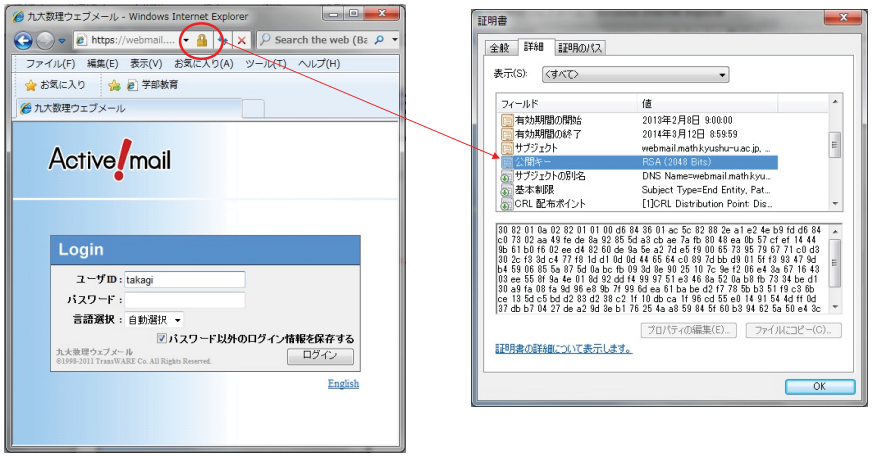
https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

- April 2018: 1st NIST PQC Workshop (submitters' presentations)
- August 2019: 2nd NIST PQC Workshop (smaller number of submissions)
- 2020/2021: Select algorithms or start a 3rd Round
- 2022/2024: Draft standards available

Security Evaluation Cycle



Example of RSA public key



Current record for factoring integers

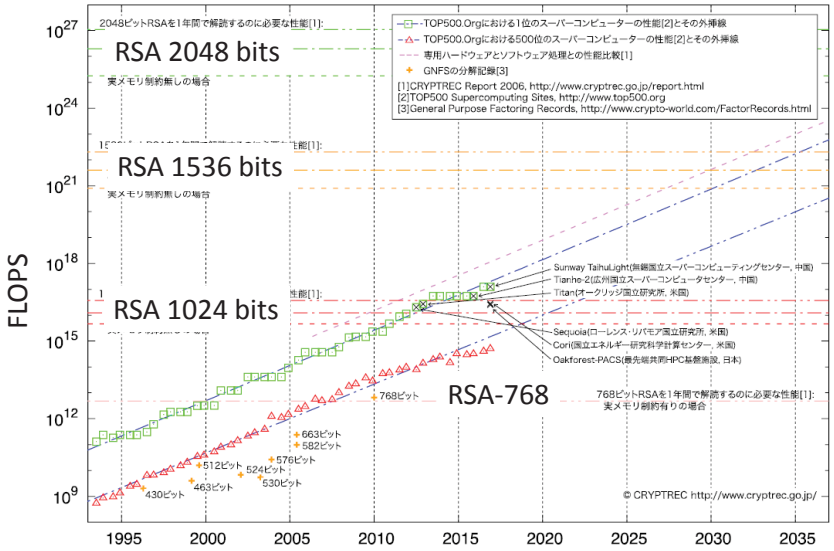
- January 2010, 768 bits, 1500 CPU years, Aoki et al.
- 12301866845301177551304949583849627207728535695953347921973
  22452151726400507263657518745202199786469389956474942774063
  84592519255732630345373154826850791702612214291346167042921
  43116022212404792747377940806653514195974598569021434 13
  =
  33478071698956898786044169848212690817704794983713768568912
  43138898288379387800228761471165253174308773781446799948 9
  ×
  36746043666799590428244633799627952632279158164343087642676
  03228381573966651127923337341714339681027009279873630891 7

Number field sieve $O\left(e^{(c+o(1))(\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}}}\right)$

Cryptography Research and Evaluation Committees in Japan

CRYPTREC Cryptography Research and Evaluation Committees http://www.cryptrec.go.jp/

Estimation for Key Length of RSA



http://www.cryptrec.jp/

Multivariate Public-Key Cryptography (MPKC)

Multivariate Quadratic polynomial problem (MQ Problem)

An example: 2 variables and 3 equations over finite field GF(7)

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

We try to find a common solution of $f_i(x_1,x_2) = 0$ for i=1,2,3.

MQ problem

MPKC are public key cryptosystems whose security depends on the difficulty in solving a system of multivariate quadratic polynomials with coefficients in a finite field K.

MQ problem: find a solution of the system of multivariate equations:

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

It is believed that it is difficult to solve (general) MQ problem.

Fukuoka MQ Challenge

Starting from April 2015
https://www.mqchallenge.org/

Gröbner basis attack

A fundamental tool for solving MQ problem is Gröbner basis. Faugère proposed efficient algorithms as F_4 and F_5 to improve original algorithm[1][2].

Complexity for solving MQ problem[3]

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

where $2 < \omega < 3$, and d_{reg} is an invariant determined by the multivariate polynomial system.

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 press, 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.

Simulated encryption scheme

- Simple matrix scheme, Extension Field Cancellation, …
- We choose *p*arameters *m=2n*.
  - To ensure the success of decryption, parameters n ≤ m are used
  - *m=2n* is suggested by Simple matrix scheme.

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

$d_1,\ldots,d_n$ is chosen to have a solution

Simulated signature scheme

- UOV, Rainbow (multilayered UOV), …
- We choose *p*arameters *n*~1.5*m*.
  - suggested by Rainbow scheme
- Due to the free variables, the complexity is equal to *n=m*.

$$\begin{cases} f_1(x_1,\ldots,x_m,x_{m+1},\ldots,x_{\lceil 1.5m\rceil}) = \sum_{1\le i,j\le \lceil 1.5m\rceil} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le \lceil 1.5m\rceil} b_i^{(1)} x_i + c^{(1)} = d_1 \\ \vdots \\ f_m(x_1,\ldots,x_m,x_{m+1},\ldots,x_{\lceil 1.5m\rceil}) = \sum_{1\le i,j\le \lceil 1.5m\rceil} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le \lceil 1.5m\rceil} b_i^{(m)} x_i + c^{(m)} = d_m \end{cases}$$

We can assign random value to free variables $x_{m+1},\ldots,x_{\lceil 1.5m\rceil}$

Base fields

- In MPKC scheme, finite field with small size are used.
  - In order to get efficient arithmetic operation.

- How to choose base field for the MQ problem
  - Binary field : GF(2)
    - The most typical field.
    - More solvers can solve systems over binary field, ex, SAT solver.
  - Binary extension field : GF(2^8)
    - Binary extension field are used in many applications.
    - GF(2^8) is the reasonable size for the cryptanalysis.
  - Prime field : GF(31)
    - Another typical field used in cryptography is prime field.
    - GF(31) also had the reasonable size for the cryptanalysis.

6 Types of Challenges

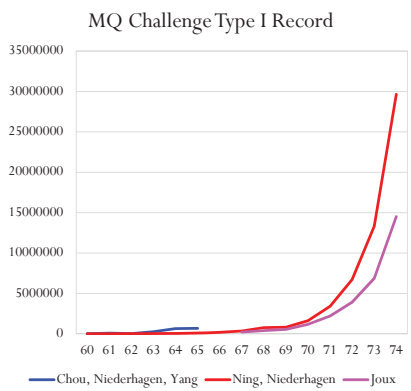
- m: # equations, n: # variables, q: base field GF(q)

Type			
I	$m = 2n$	$GF(2)$	Encryption
II	$m = 2n$	$GF(2^8)$	Encryption
III	$m = 2n$	$GF(31)$	Encryption
IV	$n \approx 1{,}5m$	$GF(2)$	Signature
V	$n \approx 1{,}5m$	$GF(2^8)$	Signature
VI	$n \approx 1{,}5m$	$GF(31)$	Signature

Current Record – 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



Lattice-based Cryptography

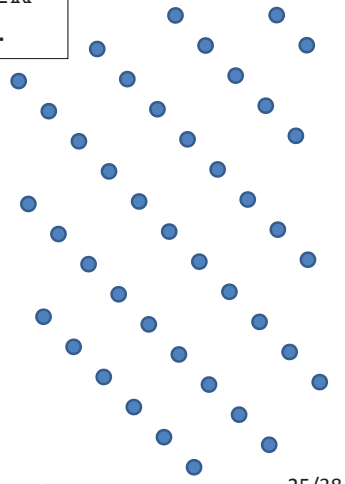
Lattice-based Cryptography

A **lattice** $\boldsymbol{L}$ is the set of all integer combinations of n linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$

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

Shortest Vector Problem (SVP)
Input: basis $\mathbf{b}_1, \dots, \mathbf{b}_n$ of lattice $\boldsymbol{L}$
Output: non-zero shortest vector in $\boldsymbol{L}$

NP-hard problem
SVP is used in cryptography
Ajtai 1996, Regev 2005



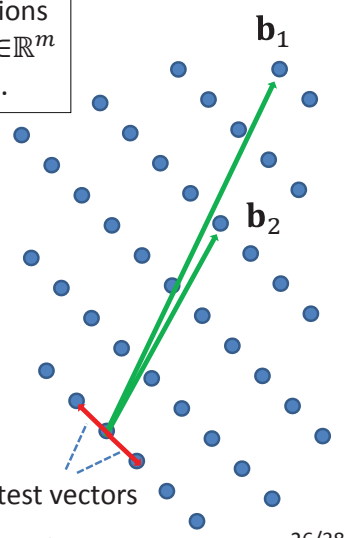
Lattice-based Cryptography

A **lattice** $\boldsymbol{L}$ is the set of all integer combinations of n linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$

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

Shortest Vector Problem (SVP)
Input: basis $\mathbf{b}_1, \dots, \mathbf{b}_n$ of lattice $\boldsymbol{L}$
Output: non-zero shortest vector in $\boldsymbol{L}$

NP-hard problem
SVP is used in cryptography
Ajtai 1996, Regev 2005



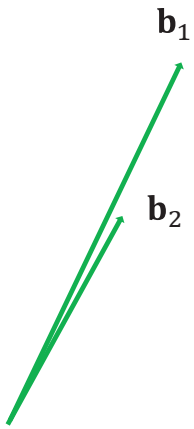
Lattice-based Cryptography

A **lattice** $\boldsymbol{L}$ is the set of all integer combinations of n linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$

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

Shortest Vector Problem (SVP)
Input: basis $\mathbf{b}_1, \dots, \mathbf{b}_n$ of lattice $\boldsymbol{L}$
Output: non-zero shortest vector in $\boldsymbol{L}$

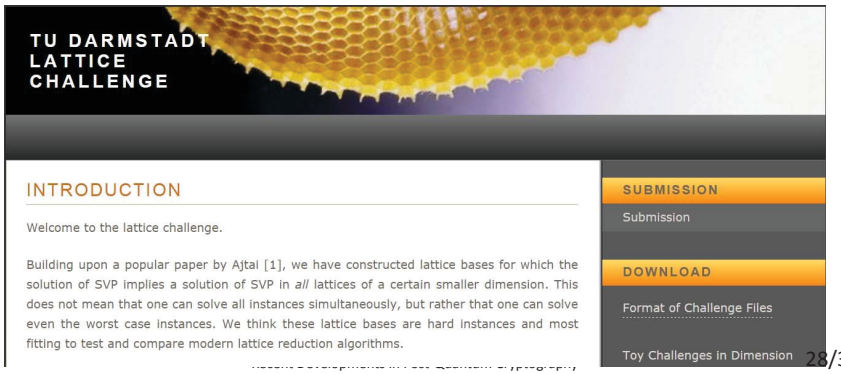
NP-hard problem
SVP is used in cryptography
Ajtai 1996, Regev 2005



Darmstadt Lattice Challenge

https://www.latticechallenge.org/

- SVP Challenge / Lattice Challenge (since 2008)
- Ideal Lattice Challenge (since 2013)
- LWE Challenge (since 2016)



Algorithms for solving the SVP

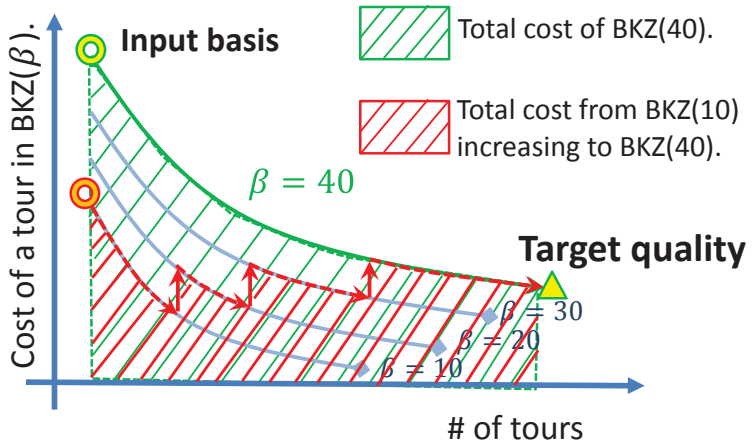
(1) Lattice basis reduction (LLL/BKZ algorithm)
- polynomial-time (+ exponential-time exhaustive search)

(2) Enumeration (Extreme pruning [Gama-Nguyen-Regev 2010])
- time: $2^{O(n^2)}$, space: polynomial size

(3) Sieving (Gauss sieve algorithm [Micciancio-Voulgaris 2010])
- time: heuristically $2^{O(n)}$, space: $2^{O(n)}$

(4) Others

Idea of progressive BKZ



Darmstadt Lattice Challenge

Cost Estimation of Progressive BKZ

Dimension	$n \cdot \det^{1/n}$	
	blocksize	$\log_2$(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

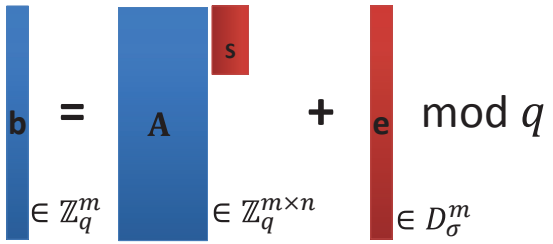
APPROX-SVP HALL OF FAME

Position	Dimension	Index	Seed	Euclidean norm	Contestant	Solution
1	652	653	0	626850	Yuntao Wang; Yoshinori Takuya Hayashi; Jintai Tsuyoshi Takagi	$2^{24.0}$ sec
2	652	653	0	626936	Yuntao Wang; Yoshinori Aono; 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

We have solved SVP of 652 dimensions.
EUROCRYPT2016

Learning with Errors (LWE) Problem

Dimension n;
Standard deviation σ of discrete Gaussian distribution D_σ;
Number of samples m;
Modulus q;
Relative error size: $\alpha = \sigma/q$;



Embedding Technique on LWE

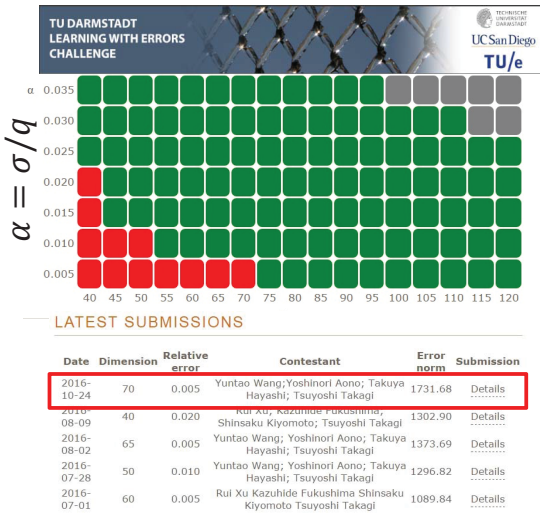
Embedding technique [Kannan@1987]:
Reduce LWE problem to unique-SVP problem.

Input: an instance $(\mathbf{A}, \mathbf{b} \equiv \mathbf{As} + \mathbf{e} \pmod q) \in (\mathbb{Z}_q^{m\times n}, \mathbb{Z}_q^m)$.
Output: secret vector $\mathbf{s} \in \mathbb{Z}_q^n$.
Step 1. construct basis $\mathbf{B}_{\text{HNF}}$ of $L_1 = \{\mathbf{v} \in \mathbb{Z}_m \,|\mathbf{v} \equiv \mathbf{As} \pmod q, \mathbf{s} \in \mathbb{Z}_n\}$.
Step 2. Rescale $\mathbf{B}_{HNF}$ to $\mathbf{B}' = \begin{pmatrix} \mathbf{B}_{HNF}^T & \mathbf{b} \\ 0 & M \end{pmatrix}$ as a basis of L_2 to reduce BDD to unique-SVP.
Step 3. Process $\mathbf{B}'$ using reduction algorithm to derive a short vector

$$\mathbf{w} = \begin{pmatrix} \mathbf{e} \\ M \end{pmatrix} = \mathbf{B}' \begin{pmatrix} \mathbf{u} \\ 1 \end{pmatrix}$$

which satisfies $\|\mathbf{w}\| \le \sqrt{\|\mathbf{e}\|^2 + M^2}$, here $\|\mathbf{e}\| \approx m\sqrt{\sigma}$.
Step 4. Compute the error vector $\mathbf{e} = \mathbf{b} - \mathbf{Bu}$;
and compute the secret vector $\mathbf{s}$ in $(\mathbf{b} - \mathbf{e}) = \mathbf{As}$.

Experimental Results: TU Darmstadt LWE Challenge

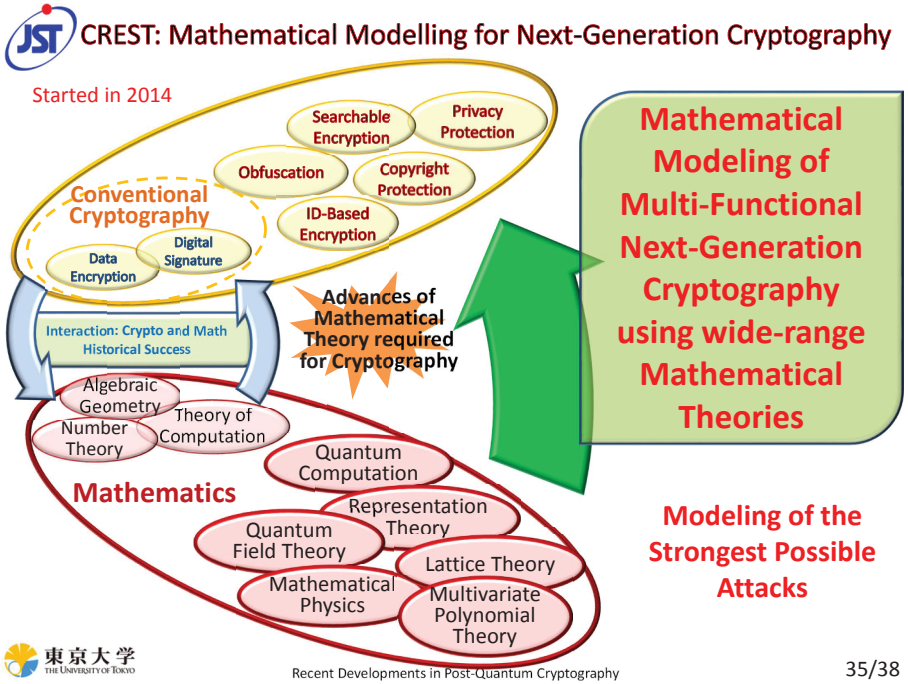


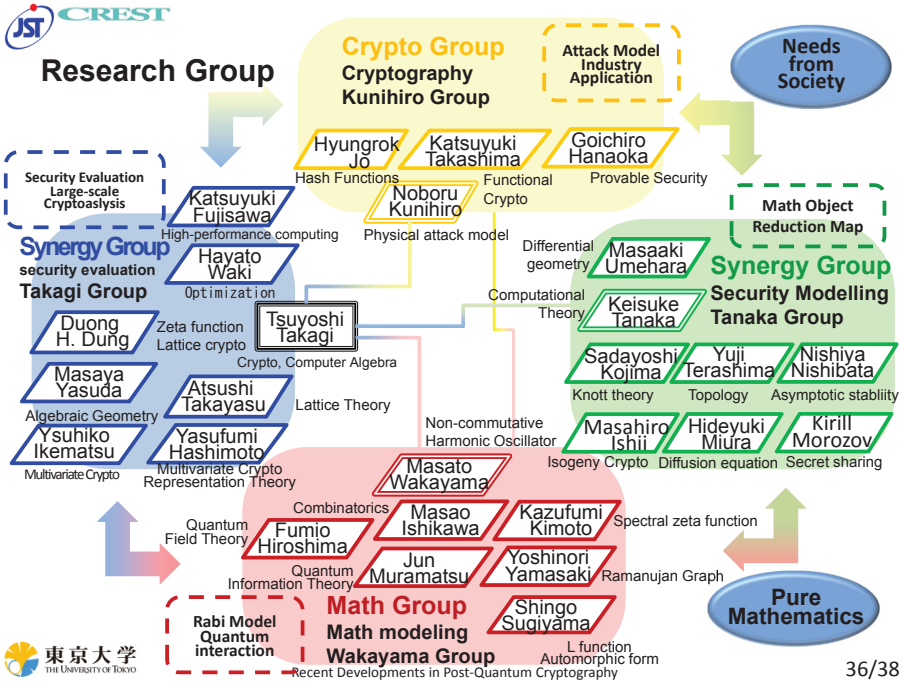
(α, n) = (0.005, 70)

Embedding technique
+ Progressive BKZ

E5-2697 v2 @ 2.70GHz

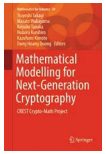
32.73 single core hours





Book “CREST Crypto-Math”

- Published on July 2017 from Springer
  Mathematical Modelling for Next-Generation Cryptography
  Mathematics for Industry Vol.29, Springer, 2017. (359ページ)
  http://www.springer.com/in/book/9789811050640



19 papers about research results, technical survey, open problems in this project.

Part I Mathematical Cryptography
- Hash-based Signature, Code-based Crypto, Multivariate Polynomial Crypto, Isogeny-based Crypto,

Part II Mathematics Towards Cryptography
- Quantum Rabi Model, Group-Subgroup Pair Graphs, Ramanujan Cayley Graphs

Part III Lattices and Cryptography
- Learning with Errors Problem, Integer Quadratic Programming, Log Units and L-function

Part IV Cryptographic Protocols
- Security in Leakage Model, Fully Homomorphic Encryptions, Identity-based Encryptions

Conclusion

- Recent developments in Post-Quantum Cryptography
  - NIST PQC Standardization
- Multivariate Polynomial Cryptography
  - Fukuoka MQ Challenge
- Lattice-based Cryptography
  - Darmstadt Lattice Challenge
- JST CREST Crypto-Math Project
  - Mathematical Modelling for Next-Generation Cryptography