LATTICE BASED POST QUANTUM CRYPTOGRAPHY

Abderrahmane Nitaj

University of Caen Normandy, France

Taza, Morocco

December 20, 2024

Contents

Contents

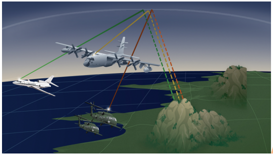
Modern cryptography

Used in:

1. Cyber Security
2. Online shopping and tickets
3. Online banking
4. Aircraft Communications
5. Satellite communications
6. Government communications
7. Crypto-currencies, Bitcoins

Partially used in:

1. Cell phone conversations
2. Emails
3. Medical records
4. Cloud storage, skype, facebook, ...



Modern Cryptography: Important dates

1. 1976: Diffie-Hellman Key Exchange,
2. 1978: Invention of RSA and McElliece,
3. 1984: Invention of El Gamal, ECC and BB84,
4. 1994: Publication of Shor's quantum algorithm.
5. 2001: Standardisation of AES (NIST),
6. 2016-2025: NIST Competition for the Post Quantum Cryptography,

Reduction to Order Finding

- **INPUT :** A positive integer n.
  1. Choose an integer x at random with $2 \leq x \leq n-1$.
  2. Compute the order r of x modulo n, that is

     the smallest $r \geq 1$ such that $x^r \equiv 1 \pmod{n}$.
  3. Compute $\gcd\left(n, x^{r/2}-1\right)$.
- **OUTPUT :** A factor of n.
- The quantum part is Step 2.
- The (quantum) polynomial time: $O\left((\log n)^3\right)$.

Example

- $n = 33010331766700717267150650747773$; $x = 2457121578 7981$.
- Then $r = 550172196111676677823842611058$ with $r \approx n^{0.97}$.
- $\gcd\left(n, x^{r/2}+1\right) = 113694290951743 99$ and
  $\gcd\left(n, x^{r/2}-1\right) = 290342914234027$.

Reduction to Order Finding

- **INPUT :** A positive integer n.
  1. Choose an integer x at random with $2 \le x \le n-1$.
  2. Compute the order r of x modulo n, that is
     the smallest $r \ge 1$ such that $x^r \equiv 1 \pmod{n}$.
  3. Compute $\gcd\left(n, x^{r/2}-1\right)$.
- **OUTPUT :** A factor of n.
- The quantum part is Step 2.
- The (quantum) polynomial time: $O\left((\log n)^3\right)$.

Example

- $n = 330103317667007172671506507477 3$; $x = 24571215787981$.
- Then $r = 5501721961116766778238426110 58$ with $r \approx n^{0.97}$.
- $\gcd\left(n, x^{r/2}+1\right) = 113694290951743 99$ and
  $\gcd\left(n, x^{r/2}-1\right) = 290342914234027$.

The Chinese case, 2024

Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage

WANG Chao WANG Qi-Di HONG Chun-Lei HU Qiao-Yun PEI Zhi
(*Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai* 200444)

Analysis of the attack

- D Wave Advantage: 5000 qubits, 2 million variables, unknown price.
- Based on quantum annealing: combinatorial optimization problems, not on Shor's algorithm.
- Factor an integer up to 2^{50}.
- Far from $2^{2048} \approx \left(2^{50}\right)^{41}$.

Consequences of Shor's algorithm

Cryptosystems vulnerable to quantum computers

1. RSA,
2. El Gamal,
3. Diffie-Hellman,
4. ECC,
5. Digital Signature Algorithm (DSA),
6. Elliptic Curve Digital Signature Algorithm (ECDSA)...

Contents

Definition of Post Quantum Cryptography

A system that is resistant to quantum attacks is a post quantum system.

Post-Quantum Cryptography Families

1. Code Based Cryptography: Encryption, Key Exchange, Signatures,
2. Lattices Based Cryptography: Encryption, Key Exchange, Signatures,
3. Hash Based Signatures: Digital Signatures,
4. Multivariate Cryptography: Digital Signatures,
5. Isogeny Based Cryptography:
   -~~SIKE~~ Signatures
   -NEW: Short Quaternion and Isogeny Signature , SQSign, 2020

NIST competition for Post Quantum Cryptography

- Rounds of the competition

Dates	2016-2019	2019-2020	2020-2022	2022-2024
Hard Problems	**Round 1**	**Round 2**	**Round 3**	**Round 4**
Lattices	25	11	5	0
Codes	16	7	1	3
Isogenies	1	0	0	0
Hash	2	1	0	0
Multivariate	10	4	1	0

- Standardized candidates after round 3:
  1. CRYSTALS-Kyber (Encryption, Lattices)
  2. CRYSTALS-Dilithium (Signature, Lattices)
  3. FALCON (Signature, Lattices)
  4. SPHINCS+ (Signature, Hash)

Contents

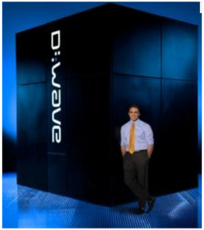
Lattice based Cryptosystems

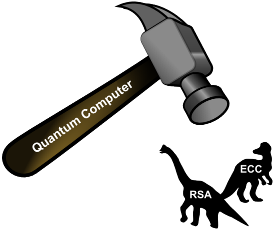
Most known schemes

- 1997: Ajtai-Dwork.
- 1998: NTRU by Hoffstein, Pipher, and Silverman.
- 1999: GGH by Goldreich, Goldwasser, and Halevi
- 2005: LWE, Learning with errors, by Regev.
- 2009: FHE, fully homomorphic encryption by Gentry.
- 2016: KYBER family by Bos, Ducas, Kiltz, Lepoint, Lyubashevsky, Schanck, Schwabe, Seiler, Stehlé.
- 2016: FrodoKEM by Alkim Bos, Ducas, Longa, Mironov Naehrig, Nikolaenko Peikert, Raghunathan, Stebila.
- 2017: New Hope by Alkim, Avanzi, Bos, Ducas, de la Piedra, Pppelmann, Schwabe, and Stebila.
- 2017: Falcon by Prest, Fouque, Hoffstein, Kirchner, Lyubashevsky, Pornin, Ricosset, Seiler, Whyte, and Zhang.

Why lattices?

- Many hard problems (SVP, CVP, SIS, ...).
- Fast implementation.
- Reasonable key sizes.
- Used in Key exchange, Encryption, signatures, zero knowledge.
- Recommended by international agencies (NIST, NSA, ENISA, ANSSI, BSI, ...)
- Resistance to all kind of attacks.





Introduction to lattices

Definition

Let n and d be two positive integers. Let $b_1 \cdots, b_d \in \mathbb{R}^n$ be d linearly independent vectors. The lattice $\mathcal{L}$ generated by $(b_1 \cdots, b_d)$ is the set

$$\mathcal{L} = \sum_{i=1}^{d} \mathbb{Z} b_i = \left\{ \sum_{i=1}^{d} x_i b_i \mid x_i \in \mathbb{Z} \right\}.$$

The vectors $b_1 \cdots, b_d$ are called a vector basis of $\mathcal{L}$.

Introduction to lattices

Lattice with dimension 2

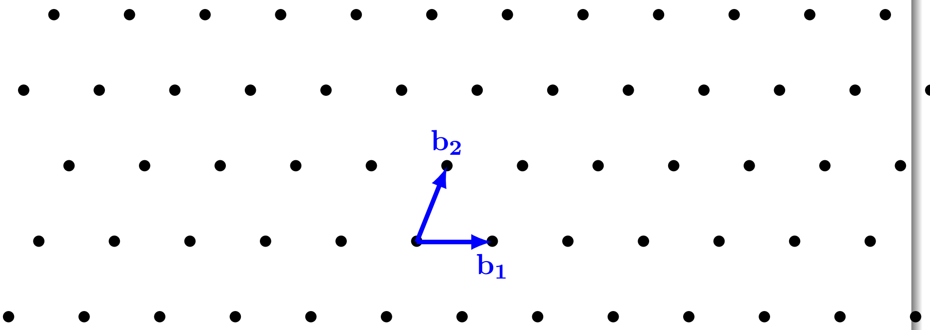


Figure: A lattice with the basis (b_1, b_2)

Introduction to lattices

Lattice with dimension 2

Introduction to lattices

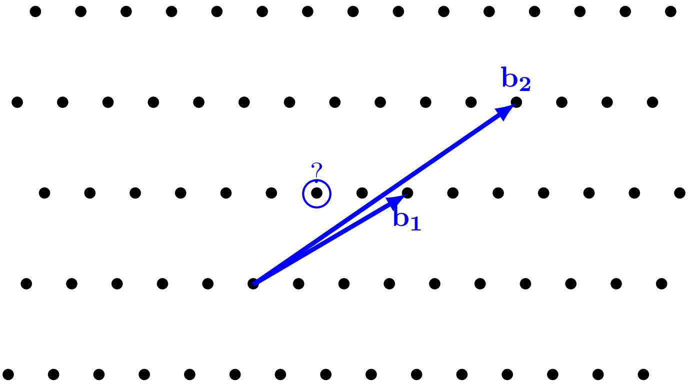


Figure: A lattice with *a bad* basis (b_1, b_2)

Introduction to lattices

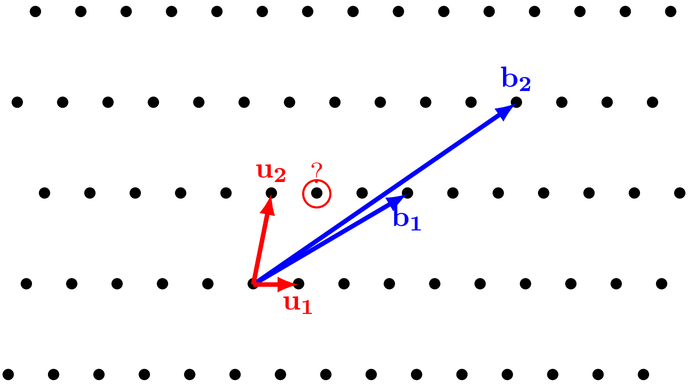


Figure: A lattice with *a good* basis (u_1, u_2)

Introduction to lattices

Comparison of bases

- In a lattice some bases are better than others.
- A good basis is a basis with
  - Short vectors.
  - Almost orthogonal vectors.

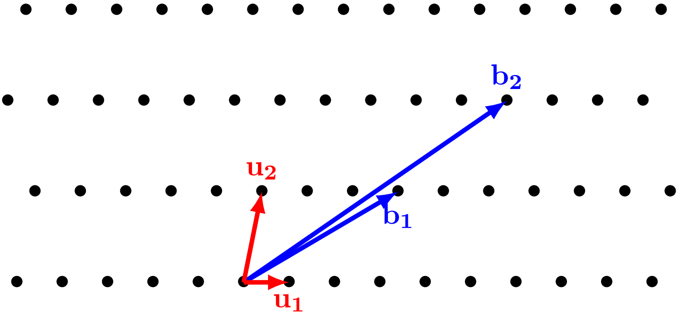


Figure: Comparison of the two bases

Lattice basis reduction

The LLL algorithm, Lenstra, Lenstra, and Lovász, 1982

Caen, France
June, 29th - July, 2nd 2007

Join the LLL+25 conference to celebrate the 25th birthday of the LLL algorithm.

Steering Committee

Arjen Lenstra, *EPFL, Lausanne, Switzerland*
Hendrik Lenstra, Jr., *Universiteit Leiden, Netherlands*
László Lovász *Eötvös Lorànd University, Hungary*

General Committee

Ali Akhavi, *Université de Caen, Université Paris 7*
Fabien Laguillaumie, *Université de Caen*
Damien Stehlé, *CNRS and E.N.S. Lyon*
Brigitte Vallée, *CNRS and Université de Caen*

Program Committee

Lattice basis reduction

The LLL algorithm

1. Invented in 1982 by Lenstra, Lenstra, and Lovász.
2. Cited more than 6256 times (December 2024).
3. Implemented on all computer algebra systems.
4. Efficient: polynomial complexity.
5. Used in cryptanalysis (Knapsack, GGH, NTRU, RSA, ...)
6. Used in number theory to solve Diophantine problems.
7. Finds a short nonzero vector b_1 in a lattice $\mathcal{L}$ of dimension n:

$$\|b_1\| \leq 2^{\frac{n-1}{4}} \det(\mathcal{L})^{\frac{1}{n}}.$$

8. For comparison, Minkowsk's Theorem asserts: In $\mathcal{L}$, there exists a nonzero vector b_1 such that

$$\|b_1\| \leq \sqrt{n} \det(\mathcal{L})^{\frac{1}{n}}.$$

Lattices

The Shortest Vector Problem (SVP):

Given a basis matrix B for $\mathcal{L}$, compute a non-zero vector $v \in \mathcal{L}$ such that $\|v\|$ is minimal, that is $\|v\| = \lambda_1(\mathcal{L})$.

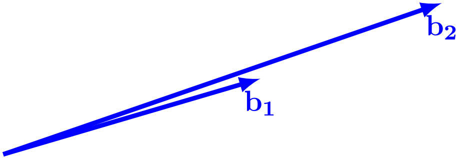


Figure: Where is the shortest vector?

Example $b_1 = (2, 15), \quad b_2 = (6, 49)$,
Compute the SVP $v = xb_1 + yb_2$ with $x, y \in \mathbb{Z}$, that is minimize $(2x + 6y)^2 + (15x + 49y)^2$.

Lattices

The Shortest Vector Problem (SVP):

Given a basis matrix B for $\mathcal{L}$, compute a non-zero vector $v \in \mathcal{L}$ such that $\|v\|$ is minimal, that is $\|v\| = \lambda_1(\mathcal{L})$.

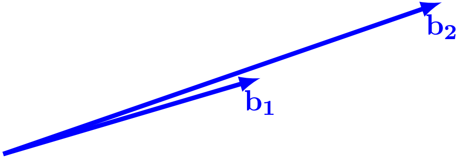


Figure: Where is the shortest vector?

Example: $b_1 = (2, 15)$, $\quad b_2 = (6, 49)$, $\quad$ Compute the SVP

Solution: $v = (2, -1) = 13b_1 - 4b_2$.

Lattices: The Shortest Vector Problem (SVP):

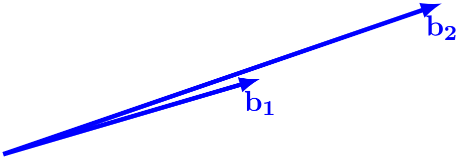
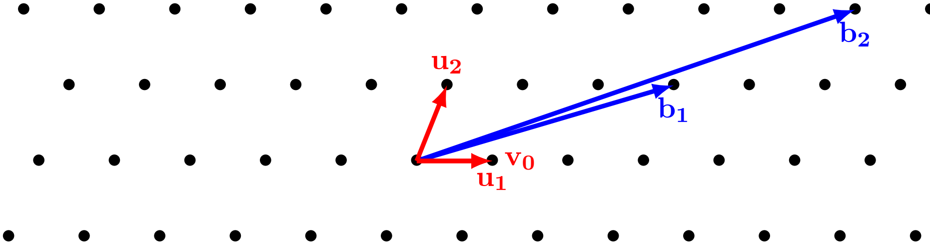


Figure: Where is the shortest vector?



Lattices

The Closest Vector Problem (CVP):

Given a basis matrix B for $\mathcal{L}$ and a vector $v \notin \mathcal{L}$, find a vector $u \in \mathcal{L}$ such that $\|v-u\|$ is minimal, that is $\|v-u\| \leq \lambda_1(\mathcal{L})$.

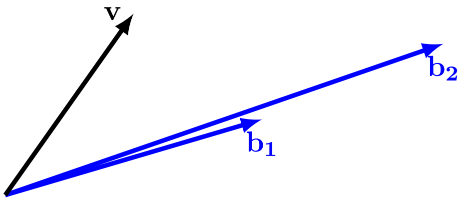


Figure: Where is the closest vector to v?

Lattices: The Closest Vector Problem (CVP)

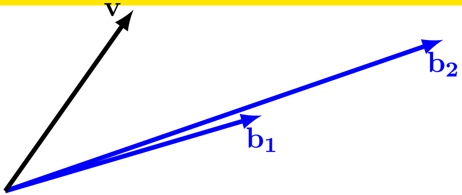


Figure: Where is the closest vector to v?

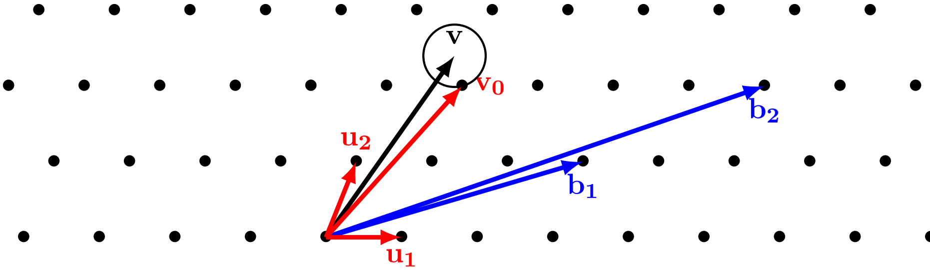


Figure: The closest vector to v is v_0

Lattices

The Approximate Shortest Vector Problem (SVP$_\gamma$

Given $\gamma > 0$, a basis matrix B for $\mathcal{L}$, find a non zero vector $u \in \mathcal{L}$ such that $\|u\| \leq \gamma\lambda_1(\mathcal{L})$.

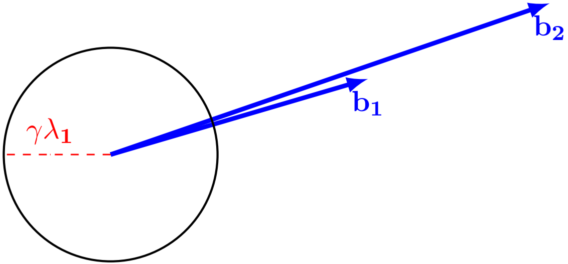


Figure: Find one or several nonzero short vectors

The Approximate Shortest Vector Problem (SVP$_\gamma$

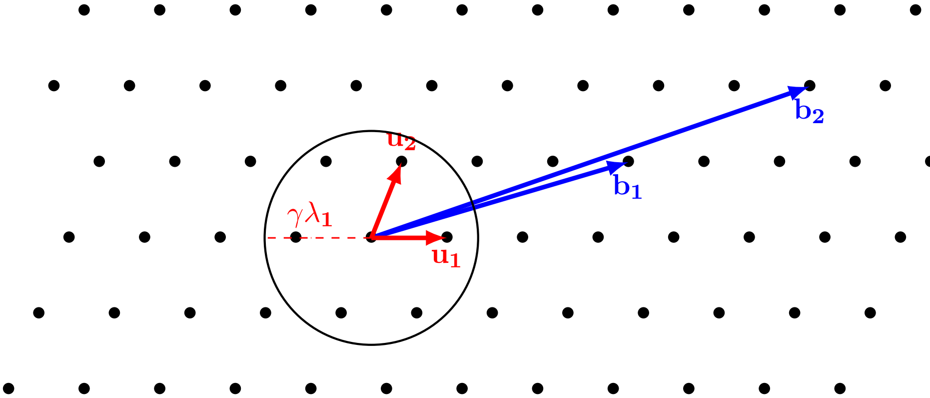


Figure: Several vectors close to v

Lattices

The Bounded Distance Decoding problem (BDD):

Given $\gamma > 0$, a basis matrix B for $\mathcal{L}$ and a vector $v \notin \mathcal{L}$, find a vector $u \in \mathcal{L}$ such that $\|v - u\| \leq \gamma\lambda_1(\mathcal{L})$.

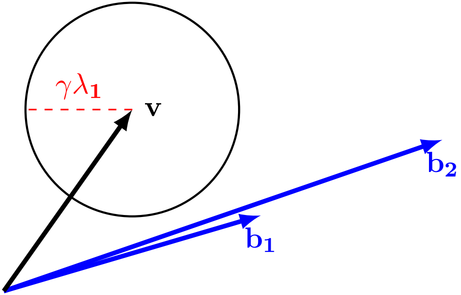


Figure: Find one or several vectors close to v

The Bounded Distance Decoding problem (BDD)

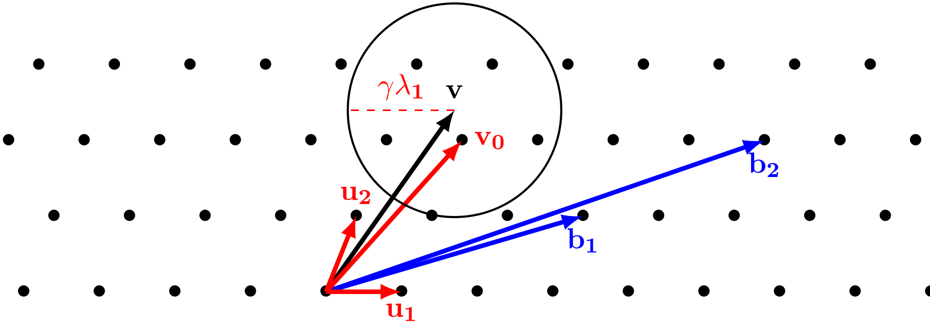


Figure: Several vectors close to v

Contents

NTRU

- NTRU: Presented by Hoffstein, Pipher, and Silverman in 1998.
- The parameters: n is prime, q is small, p is prime.
- The arithmetic on $(R_q, +, \times)$ with $R_q = \mathbb{Z}_q[X]/(X^n - 1)$.
- For $h \in R_q$, the lattice is

$$L = \{(u, v) \in R_q^2 \mid u * h = v \pmod{q}\}.$$

- Problem: Given $h \in \mathcal{R}_q$, find two short polynomials f and g such that $f * h = g$.
- The lattice hard problem: The shortest vector problem (SVP).
  Given a lattice $\mathcal{L}$ with a basis B, find a nonzero vector $v \in \mathcal{L}$
  such that $\|v\| \leq \lambda_1(\mathcal{L}(B))$.

Learning With Errors (LWE) Problem

LWE: Presented by Regev in 2005.

Examples

- Easy: solve the system for large integers

$$\begin{bmatrix} 17 & 42 & 127 \\ 24 & 3 & 71 \\ 7 & 23 & 45 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 116 & \pmod{503} \\ 158 & \pmod{503} \\ 271 & \pmod{503} \end{bmatrix}$$

- Hard: solve the system

$$\underbrace{\begin{bmatrix} 117 & 422 & 127 \\ 214 & 23 & 71 \\ 17 & 223 & 45 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}}_{S} \underbrace{+}_{+} \underbrace{\begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix}}_{E} \underbrace{=}_{=} \underbrace{\begin{bmatrix} 144 & \pmod{503} \\ 229 & \pmod{503} \\ 503 & \pmod{503} \end{bmatrix}}_{P}$$

- Hard Problem: Given A and $P = AS + E$, find S with short E.

Learning With Errors (LWE) Problem

The LWE problem:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix} = \begin{bmatrix} a_{1,1} & \cdots & a_{1,m-1} & a_{1,m} \\ a_{2,1} & \cdots & a_{2,m-1} & a_{2,m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,m-1} & a_{n-1,m} \\ a_{n,1} & \cdots & a_{n,m-1} & a_{n,m} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{m-1} \\ s_m \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_{n-1} \\ e_n \end{bmatrix}$$

- a_i are randomly uniform.
- s_i are randomly uniform.
- e_i drawn with a discrete Gaussian distribution χ with

$$\chi(x) = \frac{\exp\left(-\frac{\pi\|x\|^2}{r^2}\right)}{\sum_{y\in\mathcal{L}} \exp\left(-\frac{\pi\|y\|^2}{r^2}\right)}.$$

Learning With Errors (LWE) Scheme

The LWE scheme:

- The arithmetic : $(\mathbb{Z}_q, +, \times)$.
- The equation: $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \pmod{q}$.
- The lattice:

$$\mathcal{L} = \{\mathbf{x} \in \mathbb{Z}^n \mid \exists \mathbf{s} \in \mathbb{Z}^m, \mathbf{x} = \mathbf{A}\mathbf{s} \pmod{q}\}.$$

- The shortest norm: $\lambda_1(\mathcal{L}_A) \approx \sqrt{n} q^{1-\frac{m}{n}}$
- The minimal distance: $\|\mathbf{b} - \mathbf{A}\mathbf{s}\| = \|e\| \approx \sqrt{n}\alpha q$.
- Finding $\mathbf{s}$ implies solving the BDD_γ with $\gamma = \alpha q^{\frac{m}{n}}$.
- The lattice hard problem: γ-bounded distance decoding problem (BDD_γ): Given $0 < \gamma$, a vector $u \notin \mathcal{L}$,

  find a vector $v \in \mathcal{L}$ such that $\|u - v\| \leq \gamma \lambda_1(\mathcal{L}(B))$.

Ring-LWE

- RLWE: Presented by Lyubashevsky, Peikert, and Regev in 2010.
- $n = 2^k$, q is prime.
- The arithmetic on $(R_q, +, \times)$ with $R_q = \mathbb{Z}_q[X]/(X^n + 1)$.
- Problem: Given a series of samples $(a, as + e) \in R_q^2$ such that
  1. $a \in R_q$ uniformly,
  2. $e \in R_q$ according to a Gaussian distribution χ,

  find s.
- The lattice:

$$\mathcal{L} = \{\mathbf{x} \in \mathbb{Z}^n \mid \exists \mathbf{s} \in \mathbb{Z}^m, \mathbf{x} = \mathbf{A}\mathbf{s} \pmod{q}\}.$$

- The lattice hard problem: The Approximate SVP$_\gamma$.

Given $0 < \gamma$, a vector $u \notin \mathcal{L}$, find a vector $v \in \mathcal{L}$ such that

$\|u - v\| \leq \gamma \lambda_1(\mathcal{L}(B))$.

Module-LWE

- MLWE: Presented by Brakerski, C. Gentry, and V. Vaikuntanathan and then Langlois and Stehlé.
- $\mathbb{K}$ a number field of degree n, $\mathcal{O}_{\mathbb{K}}$ its ring of integers.
- The arithmetic on $(\mathcal{O}_{\mathbb{K},q}, +, \times)$ with $\mathcal{O}_{\mathbb{K},q} = \mathcal{O}_{\mathbb{K}}/q\mathcal{O}_{\mathbb{K}}$.
- Problem: Given a series of samples $(a, as/q + e \mod \mathcal{O}_{\mathbb{K}}) \in \mathcal{O}_{\mathbb{K},q}^2$ such that
  1. $a \in \mathcal{O}_{\mathbb{K},q}^d$ uniformly,
  2. $e \in \mathcal{O}_{\mathbb{K},q}$ according to a Gaussian distribution χ,

  find s.
- The lattice hard problem: The Approximate SVP$_\gamma$.

  Given a lattice $\mathcal{L}$ with a basis B, find a nonzero vector $v \in \mathcal{L}$

  such that $\|v\| \leq \gamma\lambda_1(\mathcal{L}(B))$.

Crystals-Kyber

- Crystals-Kyber: Presented by Avanzi, Bos, Ducas, Kiltz, Lepoint, Lyubashevsky, Schanck, Schwabe, Seiler, Stehlé in 2017.
- $n = 256$, $q = 7681$ is prime.
- The arithmetic on $(R_q^2, R_q^3, R_q^4, , +, \times)$ with $R_q = \mathbb{Z}_q[X]/(X^n + 1)$.
- Problem: Given a series of samples $(a, as + e) \in R_q^2$ such that
  1. $a \in R_q$ uniformly,
  2. $e \in R_q$ according to a binomial distribution B_η,

  distinguish between $(a, as + e)$ and a uniform $(a, b) \in R_q^2$.
- The hard problem: Module-LWE
- The lattice hard problem: The Approximate SVP$_\gamma$.

  Given a lattice $\mathcal{L}$ with a basis B, find a nonzero vector $v \in \mathcal{L}$

  such that $\|v\| \leq \gamma\lambda_1(\mathcal{L}(B))$.

Crystals-Dilithium

- Crystals-Dilithium: Presented by Bai, Ducas, Kiltz, Lepoint, Lyubashevsky, Schwabe, Seiler, Stehlé in 2017.
- $n = 256$, $q = 8380417$ is prime.
- The arithmetic on $(R_q, +, \times)$ with $R_q = \mathbb{Z}_q[X]/(X^n + 1)$.
- Problem: Given a series of samples $(a, as + e) \in R_q^2$ such that
  1. $a \in R_q$ uniformly,
  2. $e \in R_q$ according to a binomial distribution B_η,

  find s.
- The hard problem: Module SIS and RLWE
- The lattice hard problem: The shortest integer solution.

  Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a nonzero vector $\mathbf{v} \in \mathbb{Z}_q^m$

  such that $\mathbf{Av} = 0 \pmod q$ and $\|v\| \leq \beta$.

FALCON

- Falcon: Presented by Fouque, Hoffstein, Kirchner, Lyubashevsky, Pornin, Prest, Ricosset, Seiler, Whyte,Zhang in 2017.
- $n = 512, 1024$, $q = 12 \cdot 1024 + 1$ is prime.
- The arithmetic on $(R_q, +, \times)$ with $R_q = \mathbb{Z}_q[X]/(X^n + 1)$.
- For $h \in R_q$, the lattice is

$$L = \{(u, v) \in R_q^2 \mid u * h = v \pmod{q}\}.$$

- The hard problem: Ring-SIS on NTRU matrices.
- The lattice hard problem: The shortest integer solution.

Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a nonzero vector $\mathbf{v} \in \mathbb{Z}_q^m$

such that $\mathbf{A}\mathbf{v} = 0 \pmod{q}$ and $\|v\| \leq \beta$.

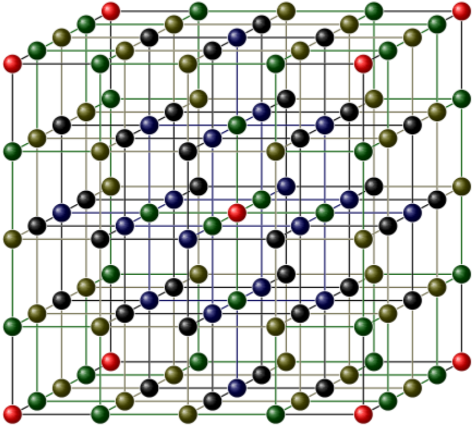
Contents

Conclusion

- Many companies like IBM, Google, Intel and many countries are investing to develop quantum computers.
- Quantum computers will break all the currently deployed public key cryptosystems (DH,RSA,ECC).
- SOLUTION: Post quantum systems can be deployed on classical computers.

Best Solution to Quantum Threats

LATTICE BASED CRYPTOGRAPHY



Thank you – Merci

شكرًا