Research
A SCIENCE PARTNER JOURNAL

REVIEW ARTICLE

The Mathematical Foundation of Post-Quantum Cryptography

Chuanming Zong

Center for Applied Mathematics, Tianjin University, Tianjin 300072, China.

Address correspondence to: cmzong@math.pku.edu.cn

Citation: Zong C. The Mathematical Foundation of Post-Quantum Cryptography. *Research* 2025;8:Article 0801. https://doi.org/10.34133/research.0801

Submitted 11 June 2025
Revised 26 June 2025
Accepted 4 July 2025
Published 26 August 2025

In 1994, P. Shor discovered quantum algorithms that can break both the RSA cryptosystem and the ElGamal cryptosystem. In 2007, a Canadian company D-Wave demonstrated the first quantum computer. These events and quick further developments have brought a crisis to secret communication. In 2022, the National Institute of Standards and Technology (NIST) announced 4 candidates—CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, and Sphincs+—for post-quantum cryptography standards. The first 3 are based on lattice theory and the last on Hash functions. In 2024, NIST announced 3 standards: FIPS 203 based on CRYSTALS-Kyber, FIPS 204 based on CRYSTALS-Dilithium, and FIPS 205 based on Sphincs+. The fourth standard based on Falcon is on the way. It is well known that the security of the lattice-based cryptosystems relies on the hardness of the shortest vector problem (SVP), the closest vector problem (CVP), and their generalizations. In fact, the SVP is a ball packing problem and the CVP is a ball covering problem. Furthermore, both SVP and CVP are equivalent to arithmetic problems for positive definite quadratic forms. There are several books and survey papers dealing with the computational complexity of the lattice-based cryptography for classical computers. However, there is no review article to demonstrate the mathematical foundation of the complexity theory. This paper will briefly introduce post-quantum cryptography and demonstrate its mathematical roots in ball packing, ball covering, and positive definite quadratic forms.

Mathematical Cryptography

In 1976, W. Diffie and M. E. Hellman [1] proposed the principle of public key cryptography. One year later, the first public key cryptosystem RSA was invented by R. L. Rivest, A. Shamir, and L. Adleman [2]. These events not only inaugurated a new era in secret communication but also marked the birth of mathematical cryptography (see [3,4]), the public key cryptography based on mathematical theories. Since then, several other mathematical cryptosystems have been discovered, including the discrete logarithm cryptosystem invented by T. ElGamal [5] in 1985, the elliptic curve cryptosystem ECC designed by V. S. Miller [6] in 1985 and by N. Koblitz [7] in 1987, respectively, and the lattice-based cryptosystems AD discovered by M. Ajtai and C. Dwork [8] in 1997, GGH invented by O. Goldreich, S. Goldwasser and S. Halevi [9] in 1997, NTRU designed by J. Hoffstein, J. Pipher, and J. H. Silverman [10] in 1998, LWE discovered by O. Regev [11] in 2005, and FHE invented by C. Gentry [12] in 2009. In the past half century, mathematical cryptography has played a crucial role in the modern technology of computers and the internet. At the same time, it has been developed into an active interdisciplinary research field between mathematics and cryptography.

Before Diffie-Hellman, both the enciphering process and the deciphering process of any secret communication used the same secret key. Ciphers of this sort are known as symmetric ciphers. If Bob wants to send a secret message $\mathbf{m}$ to Alice, they have to share a secret key $\mathbf{k}$. Bob first scrambles his message $\mathbf{m}$ by the key $\mathbf{k}$ to a ciphertext $\mathbf{c}$ and then sends it through some channel to Alice. When Alice receives the ciphertext $\mathbf{c}$, she uses the secret key $\mathbf{k}$ to unscramble it and reconstitute $\mathbf{m}$. During this process, if the communication channel is not secure, their adversary Eve can intercept not only the ciphertext $\mathbf{c}$ but also the secret key $\mathbf{k}$ and then reconstitute their secret message $\mathbf{m}$.

In the 1970s, when computers and networks were becoming part of daily life, symmetric ciphers were no longer efficient enough for key distribution, key management, and digital signatures. In Diffie and Hellman's ideal public key cryptosystem, enciphering and deciphering are governed by distinct keys, $\mathbf{k}_e$ and $\mathbf{k}_d$, such that computing the decryption key (the private key) $\mathbf{k}_d$ from the encryption key (the public key) $\mathbf{k}_e$ is computationally infeasible. All users of a network place their encryption keys in a public directory. Then, the users can encrypt their messages using the receivers' public keys and decrypt the received messages using their own private keys. We now introduce RSA, NTRU, and LWE as examples, since RSA is the first functioning public key cryptosystem and both NTRU and LWE are crucial for post-quantum cryptography.

The RSA cryptosystem

First, Alice chooses 2 large primes p and q, keeps them secret, defines $N = pq$ implying

$$\varphi(N) = (p-1)(q-1), \tag{1}$$

where $\varphi(N)$ is Euler's totient function, and chooses an enciphering exponent e satisfying

$$\gcd(e, \varphi(N)) = 1. \tag{2}$$

In other words, e and $\varphi(N)$ have no common divisor. Then, she chooses (N, e) as the public key and publishes it. Of course, both Bob and Eve can get it. Second, Bob enciphers his plaintext $\mathbf{m}$ by Alice's public key to the following ciphertext

$$\mathbf{c} \equiv \mathbf{m}^e \pmod{N} \tag{3}$$

and sends it to Alice. Third, since Alice knows $\varphi(N) = (p-1)(q-1)$, she can compute d satisfying

$$ed \equiv 1 \pmod{\varphi(N)} \tag{4}$$

and decipher Bob's message as

$$\mathbf{c}^d \equiv \mathbf{m}^{ed} \equiv \mathbf{m} \pmod{N}, \tag{5}$$

based on Euler's formula

$$\mathbf{m}^{\varphi(N)} \equiv 1 \pmod{N}. \tag{6}$$

In the RSA cryptosystem, besides Euler's formula, 2 other mathematical results are also crucial. First, when p and q are known, it is relatively easy to compute the deciphering key d. For example, the Euclidean algorithm takes at most $2\log_2(\varphi(N)) + 2$ iterations to compute $\gcd(e, \varphi(N))$ and it takes only a small multiple of $\log_2(\varphi(N))$ steps to compute d. On the other hand, without knowledge of p and q, to factorize the large integer N is hard. There are many electronic computer algorithms to factorize large integers. However, none of them are efficient enough to break the RSA cryptosystem. The computational hardness of integer factorization is the security guarantee of the RSA cryptosystem.

The NTRU cryptosystem

Let N, p, q, d_1, and d_2 be suitable integers. Let $\mathbb{Z}_q$ be the ring of integers modulo q, let $\mathcal{R}$, $\mathcal{R}_p$, and $\mathcal{R}_q$ be 3 polynomial rings defined by

$$\begin{aligned} \mathcal{R} &= \mathbb{Z}[x]/(x^N - 1), \\ \mathcal{R}_p &= \mathbb{Z}_p[x]/(x^N - 1), \\ \mathcal{R}_q &= \mathbb{Z}_q[x]/(x^N - 1), \end{aligned} \tag{7}$$

and let $T(d_1, d_2)$ denote the set of all polynomials in $\mathcal{R}$ that has d_1 coefficients equal to 1, d_2 coefficients equal to -1, and all other coefficients equal to 0.

First, Alice and Bob choose a group of public parameters (N, p, q, d) such that both N and p prime,

$$\gcd(p, q) = \gcd(N, q) = 1, \tag{8}$$

and $q > (6d+1,)p$. Second, Alice chooses $\mathbf{k}_1 \in T(d+1, d)$ and $\mathbf{k}_2 \in T(d, d)$ as private keys, where $\mathbf{k}_1$ is invertible in both $\mathcal{R}_p$ and $\mathcal{R}_q$, computes the inverse $\mathbf{g}_p$ of $\mathbf{k}_1$ in $\mathcal{R}_p$ and the inverse $\mathbf{g}_q$ of $\mathbf{k}_1$ in $\mathcal{R}_q$, computes

$$\mathbf{h} = \mathbf{g}_q \mathbf{k}_2, \tag{9}$$

and publishes $\mathbf{h}$ as the public key. Third, Bob chooses a random $\mathbf{r} \in T(d, d)$, encrypts his plaintext $\mathbf{m} \in \mathcal{R}_p$ to

$$\mathbf{c} \equiv p\mathbf{r}\mathbf{h} + \mathbf{m} \pmod{q}, \tag{10}$$

and sends the ciphertext $\mathbf{c}$ to Alice. Finally, when Alice receives $\mathbf{c}$, she computes

$$\mathbf{m}^\circ \equiv \mathbf{k}_1 \mathbf{c} \pmod{q}, \tag{11}$$

lifts it to $\mathbf{m}^\bullet \in \mathcal{R}$, and decrypts as

$$\mathbf{m} \equiv \mathbf{g}_p \mathbf{m}^\bullet \pmod{p}. \tag{12}$$

More precisely, we have

$$\mathbf{m}^\circ = \mathbf{k}_1 \mathbf{c} \equiv p\mathbf{k}_1 \mathbf{g}_q \mathbf{k}_2 \mathbf{r} + \mathbf{k}_1 \mathbf{m} \equiv p\mathbf{k}_2 \mathbf{r} + \mathbf{k}_1 \mathbf{m} \pmod{q}. \tag{13}$$

Since $\mathbf{k}_1$, $\mathbf{k}_2$, $\mathbf{r}$, and $\mathbf{m}$ are polynomials of small coefficients, $p\mathbf{k}_2\mathbf{r} + \mathbf{k}_1\mathbf{m}$ has coefficients within $(-q/2, q/2)$ for proper parameters. This means that

$$\mathbf{m}^\bullet = p\mathbf{k}_2\mathbf{r} + \mathbf{k}_1\mathbf{m}. \tag{14}$$

The LWE cryptosystem

Let n, m, ℓ, t, r, and q be suitable integers and let α be a positive real number. Let $\mathbb{Z}_q^n$ denote the set of vectors $(a_1, a_2, \ldots, a_n)$ with $a_i \in \mathbb{Z}_q$, and let $\mathbb{Z}_q^{n\times\ell}$ denote the set of $n \times \ell$ matrices with entries $a_{ij} \in \mathbb{Z}_q$. Furthermore, let Ψ_α denote the distribution on $\mathbb{Z}_q$ obtained by sampling a normal variable with mean 0 and standard deviation $\alpha q/\sqrt{2\pi}$, rounding the result to the nearest integer, and reducing it modulo q, let f be the function that maps the message space $\mathbb{Z}_t^\ell$ to $\mathbb{Z}_q^\ell$ by multiplying each coordinate by q/t and rounding to the nearest integer, and let f^{-1} denote the inverse of f.

First, Alice and Bob choose a group of public parameters $(n, m, \ell, t, r, q, \alpha)$. Second, Alice chooses $S \in \mathbb{Z}_q^{n\times\ell}$ uniformly at random as the private key, takes $A \in \mathbb{Z}_q^{m\times n}$ uniformly at random, takes $E \in \mathbb{Z}_q^{m\times\ell}$ by choosing each entry according to Ψ_α, and chooses (A, P) as the public key, where

$$P = AS + E. \tag{15}$$

Third, Bob chooses $\mathbf{a} \in \mathbb{Z}_t^m$ uniformly at random and encrypts a message $\mathbf{v} \in \mathbb{Z}_t^\ell$ to $(\mathbf{u}, \mathbf{c})$, where $\mathbf{u} = A'\mathbf{a}$ and

$$\mathbf{c} = P'\mathbf{a} + f(\mathbf{v}). \tag{16}$$

Finally, when Alice receives $(\mathbf{u}, \mathbf{c})$, she decrypts it by her secret key S as

$$\mathbf{v} = f^{-1}(\mathbf{c} - S'\mathbf{u}). \tag{17}$$

Lattice is a mathematical concept introduced by Gauss at the beginning of the 19th century and further developed by Minkowski and many others (see [13,14]). Let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ be n linearly independent vectors in the n-dimensional Euclidean space $\mathbb{E}^n$. We call

$$\Lambda = \{z_1\mathbf{a}_1 + z_2\mathbf{a}_2 + \ldots + z_n\mathbf{a}_n : \ z_i \in \mathbb{Z}\} \tag{18}$$

an n-dimensional lattice and call $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ a basis of the lattice Λ.

At the first glance, both NTRU and LWE have nothing to do with lattice. In fact, both of them can be reformulated in

lattice and their security depends on the computational complexity of some lattice problems (see [15]).

Post-Quantum Cryptography

The classical computer is based on the laws of electronics. Its fundamental unit of information is the binary digit (bit) 0 or 1. Sequences of bits are manipulated by Boolean logic gates, and a succession of gates yields a computation.

Quantum Turing machine

At the beginning of the 1980s, Y. I. Manin, P. Benioff, R. Feynman, and D. Deutsch started investigating the possibility of creating a computer based on the laws of quantum mechanics (see [16]). In particular, Deutsch introduced the quantum Turing machine and quantum circuits in 1985.

A quantum computer operates on quantum bits (or qubits). The state of a qubit can be represented as

$$\alpha_1|0\rangle + \alpha_2|1\rangle, \tag{19}$$

where $|0\rangle$ is its ground state, $|1\rangle$ is its excited state, and α_i are complex numbers satisfying $|\alpha_1|^2 + |\alpha_2|^2 = 1$. In a system of n qubits, let $|\mathbf{s}_i\rangle = |s_1^i s_2^i \dots s_n^i\rangle$ denote the 2^n basis states with $s_j^i \in \{0, 1\}$, the superposition of states can be represented as

$$\sum_{i=1}^{2^n} \alpha_i |\mathbf{s}_i\rangle, \tag{20}$$

where α_i are complex numbers satisfying $\sum |\alpha_i|^2 = 1$, and $|\alpha_i|^2$ represents the possibility of the system yield state $|\mathbf{s}_i\rangle$. The quantum computer manipulates qubits via quantum logic gates to process computations. A quantum logic gate will change one superposition of states to one other superposition of states by a unitary transformation, where unitary means that the conjugate transpose of the transformation matrix is equal to its inverse. For example, suppose a quantum computer of 3 qubits is in the superposition of states

$$\frac{1}{2}|000\rangle - \frac{1}{2}|010\rangle + \frac{1}{2}|101\rangle - \frac{1}{2}|111\rangle \tag{21}$$

and the logic gate changes the last 2 qubits of the state by

$$\begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} \rightarrow \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{i}{2} & -\frac{1}{2} & -\frac{i}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{i}{2} & -\frac{1}{2} & \frac{i}{2} \end{pmatrix} \begin{matrix} 00 \\ 01 \\ 10 \\ 11. \end{matrix} \tag{22}$$

Then, the computer will go to the superposition of states

$$\frac{1}{2}|001\rangle + \frac{1}{2}|011\rangle + \frac{i}{2}|101\rangle - \frac{i}{2}|111\rangle. \tag{23}$$

Since the state of the output of a quantum computer can be a coherent superposition of states corresponding to different solutions of a problem, it may allow many computations to be done simultaneously and quickly (see [17]).

Quantum computing

In the early 1990s, when the quantum computer was not yet born, Deutsch, R. Jozsa, Shor, and L. Grover started to explore quantum computing (see [16]). First, Deutsch and Jozsa [18] presented a problem that can be solved by a quantum computer with certainty in polynomial time, which is exponentially less time than any classical deterministic computer, and less than the expected time of any classical stochastic computer.

Almost at the same time, Shor [19] discovered polynomial time quantum algorithms to deal with the discrete logarithm problem and the factorization problem. Assume that $0 \le a < q$ and

$$a = \sum_{i=0}^{k-1} \alpha_i 2^i \tag{24}$$

is the binary representation of a. Then, he defines the state $|\mathbf{a}\rangle = |\alpha_{k-1}\alpha_{k-2}\cdots\alpha_0\rangle$ and introduces the following unitary transformation:

$$|\mathbf{a}\rangle \rightarrow \frac{1}{q^{1/2}} \sum_{b=0}^{q-1} \exp(2\pi i ab/q)|\mathbf{b}\rangle. \tag{25}$$

This transformation, as a quantum logic gate, plays a key role in his algorithms. A decade later, J. Proos and C. Zalka [20] succeeded in modifying Shor's discrete logarithm quantum algorithm for elliptic curves. It follows that once there is a functioning quantum computer, Shor's algorithms could break the RSA cryptosystem, the ElGamal cryptosystem, and the ECC cryptosystem. Over the years, several improvements to Shor's algorithms have been discovered. For example, the one was announced by Regev [21] in 2023.

Quantum computer

In 1998, the first quantum computer models appeared at Oxford University, IBM's Almaden Research Center, and Los Alamos. In 2007, a Canadian company D-Wave demonstrated the Orion system, a 16-qubit quantum annealing processor, running 3 different applications at the Computer History Museum in Mountain View, California. This marked the first public demonstration of a quantum computer. In 2011, D-Wave announced D-Wave One, operating on a 128-qubit chipset using quantum annealing to solve optimization problems. In the following years, several companies developed gate model quantum machines, including Google, IBM, Intel, and Rigetti. Gate model quantum computers use gates similar in concept to classical computers but with vastly different logic and architecture. By 2020, there were about a hundred working quantum computers worldwide.

In 2001, a group of researchers at IBM successfully applied Shor's algorithm to factorize 15, using nuclear magnetic resonance. In 2019, the numbers 15, 21, and 35 were factorized by applying Shor's algorithm on a 6-qubit IBM quantum processor (see [22]).

Post-quantum cryptography

As larger and larger quantum computers are built, cryptosystems such as RSA, ElGamal, and ECC will no longer be secure, so post-quantum cryptography will be critical for the future of secret communication.

In 2006, the first international workshop on post-quantum cryptography took place at the Katholieke Universiteit Leuven.

Since then, post-quantum cryptography has gradually become an important research branch of cryptography. In particular, it has become a focus topic of CRYPTO, EUROCRYPT, and ASIACRYPT.

In 2016, the National Institute of Standards and Technology (NIST) launched a global project to solicit and select a handful of encryption algorithms with the ability to resist quantum computer attacks. On 2022 July 5, after 3 rounds of competition and selection, NIST announced 4 algorithms that will underpin its future cryptography standards. They include one algorithm (CRYSTALS-Kyber) for general encryption and key establishment purposes and 3 (CRYSTALS-Dilithium, Falcon, and Sphincs+) for digital signatures (see [23–25]). On 2024 August 13, the agency announced 3 post-quantum cryptography standards: FIPS 203 based on CRYSTALS-Kyber, FIPS 204 based on CRYSTALS-Dilithium, and FIPS 205 based on Sphincs+. The fourth standard based on Falcon is on the way. On 2024 November 12, NIST published the guideline "Transition to post-quantum cryptography standards", which lists detailed route and time table. In fact, many high-tech companies and institutions have already completed the transition.

It is well known that both CRYSTALS-Kyber and CRYSTALS-Dilithium are based on LWE, Falcon is based on NTRU, and Sphincs+ is based on Hash functions. Both NTRU and LWE are lattice-based cryptosystems. Lattice-based cryptography was born more or less at the same time of Shor's quantum algorithms for the discrete logarithm problem and the factorization problem (see [26–28]). It has been explored as a key candidate for post-quantum cryptography ever since.

The Shortest Vector Problem and the Closest Vector Problem

No one can predict the future of the post-quantum cryptography. Currently, a decisive role is played by lattice-based cryptosystems. No matter how different in form, the security of all known lattice-based cryptosystems and algorithms relies on the computational complexity of the following 2 problems and their variations:

The shortest vector problem (SVP): Find a shortest nonzero vector in an n-dimensional lattice Λ, i.e., find a nonzero vector $\mathbf{v} \in \Lambda$ that minimizes the Euclidean norm $\|\mathbf{v}\|$.

The closest vector problem (CVP): Given a vector $\mathbf{x} \in \mathbb{E}^n$ that is not in Λ, find a vector $\mathbf{v} \in \Lambda$ that is closest to $\mathbf{x}$, i.e., find a vector $\mathbf{v} \in \Lambda$ that minimizes the Euclidean norm $\|\mathbf{v}-\mathbf{x}\|$.

In fact, the security of all AD , NTRU, and LWE depends on the complexity of SVP and its variations, and the security of GGH and NTRU is based on the complexity of CVP and its approximation (see [15,27]).

Complexity theory of classical computer

A Turing machine $\mathcal{M}$ runs in time $t(n)$ if, for every input string $\mathbf{s}$ of length n over some fixed input alphabet, $\mathcal{M}(\mathbf{s})$ halts after at most $t(n)$ steps. Efficient computation with a Turing machine means that it halts in polynomial time in the size of the input, i.e., the Turing machine runs in time $t(n) = a + n^b$ for some constants a and b independent of n.

A decision problem consists of deciding whether the input string satisfies some specified property or not. The class of decision problems that can be solved by a deterministic Turing machine in polynomial time is called $\mathcal{P}$. The class of decision problem that can be solved by a nondeterministic Turing machine in polynomial time is called $\mathcal{NP}$. Clearly, we have $\mathcal{P} \subseteq \mathcal{NP}$. It is widely believed that $\mathcal{P} \neq \mathcal{NP}$, i.e., there are $\mathcal{NP}$ problems that cannot be solved in deterministic polynomial time. In fact, to prove or disprove $\mathcal{P} = \mathcal{NP}$ is a fundamental problem in both mathematics and computer science.

Let P_1 and P_2 be 2 decision problems consisting of strings of alphabet. A reduction from P_1 to P_2 is a polynomial time computable function f such that $\mathbf{s} \in P_1$ if and only if $f(\mathbf{s}) \in P_2$. Clearly, if P_1 reduces to P_2 and P_2 can be solved in polynomial time, then P_1 can also be solved in polynomial time. A decision problem P is $\mathcal{NP}$-hard if any other $\mathcal{NP}$ problem Q reduces to P. If P is also in $\mathcal{NP}$, then P is $\mathcal{NP}$-complete. Evidently, if a problem P is $\mathcal{NP}$-hard, then P cannot be solved in polynomial time unless $\mathcal{P} = \mathcal{NP}$.

The complexity of SVP for the classical computer

First, a lattice may have many shortest vectors. It is easy to see that the integer lattice $\mathbb{Z}^n$ has $2n$ shortest vectors. It is known that the 8-dimensional E_8 lattice has 240 shortest vectors and the 24-dimensional Leech lattice has 196,560 shortest lattice vectors. In general, an n-dimensional lattice Λ has at most

$$2^{0.401n(1+o(1))} \tag{26}$$

shortest vectors (see [14]). However, lattice-based cryptography uses random lattices rather than a particular one, so the following result is pertinent.

Theorem 3.1 (Södergren [29]**).** In $\mathbb{E}^n$, $n \geq 2$, a random lattice has exactly one pair $(\pm\mathbf{v})$ of shortest nonzero vectors, i.e., if we randomly pick a lattice, the probability of it having only one pair of shortest lattice vectors is one.

It is interesting to notice that Theorem 3.1 was proved only in 2010, much later than it was applied in lattice-based cryptography. Obviously, it has been taken for granted by cryptographers. Nevertheless, if Theorem 3.1 were not true, the SVP-based cryptosystems would be impossible.

Usually, lattices are given by their bases. One may intuitively believe that the bases should contain some short lattice vector. In fact, this is far from the truth. For example, let Λ be the integer lattice $\mathbb{Z}^2$, let m be a large integer, and define $\mathbf{a}_1 = (1, m+1)$ and $\mathbf{a}_2 = -(1, m)$. It can be verified that $\{\mathbf{a}_1, \mathbf{a}_2\}$ is a basis of Λ and

$$\|\mathbf{a}_1\| \geq \|\mathbf{a}_2\| = \sqrt{1+m^2}. \tag{27}$$

In other words, both vectors of a basis of Λ can be arbitrarily long. Nevertheless, the length of the shortest vectors of a lattice Λ can be bounded in terms of its determinant $\det(\Lambda)$. In 1891, Minkowski obtained the following fundamental result about the length of the shortest lattice vector.

Theorem 3.2. Every lattice Λ of dimension n contains a nonzero vector $\mathbf{v}$ satisfying

$$\|\mathbf{v}\| \leq \left(\sqrt{2/\pi e} + o(1)\right) \sqrt[n]{\det(\Lambda)}\sqrt{n}. \tag{28}$$

This result tells us the approximate range of the shortest lattice vectors. It can be regarded as the first cornerstone of the lattice-based cryptography.

At the beginning of the 1980s, about 2 decades before lattice-based cryptography was born, people started to study the

computational complexity of lattices. In 1981, P. van Emde Boas [30] made the following conjecture.

Conjecture 3.1. The SVP is $\mathcal{NP}$-hard.

In the same paper, he proved that the SVP in the L_∞ norm is indeed $\mathcal{NP}$-hard. However, 40 years later, the Euclidean case is still open today. Meanwhile, research has turned toward randomized reduction and approximation. Unlike deterministic reduction, randomized reduction allows the mapping function to be computable in polynomial time by a probabilistic algorithm. (A probabilistic Turing machine is a nondeterministic Turing machine that chooses between the available transitions at each point according to some probability. A quantum computer is another model of computation that is inherently probabilistic.) Therefore, the output of the reduction is only required to be correct with sufficiently high probability. In 1997, Ajtai [31] proved the following theorem.

Theorem 3.3. The SVP is $\mathcal{NP}$-hard under randomized reduction.

In fact, even approximating the shortest vector is not easy. In 1998, D. Micciancio improved Ajtai's theorem, showing that approximating the shortest vector within a factor $\sqrt{2}$ under randomized reduction is $\mathcal{NP}$-hard. In 2005, S. Khot [32] proved the following theorem.

Theorem 3.4. To approximate the shortest vector of an n-dimensional lattice within any constant factor c under randomized reduction is $\mathcal{NP}$-hard.

All Ajtai, Micciancio, and Khot's works deal with general L_p norms. For simplicity, we only concentrate on the Euclidean case. Theorem 3.4 has been further extended by I. Haviv, Regev, and others.

In 2004, Ajtai [33] introduced a new problem, called the short integer solution (SIS) problem, over random q-ary lattices. He proved that, under certain hypotheses, solving SIS over a lattice chosen randomly from an easily samplable distribution is at least as hard as approximating the SVP for any lattice.

The complexity of CVP for the classical computer

In 1981, when he proposed Conjecture 3.1, van Emde Boas proved that CVP is $\mathcal{NP}$-hard. On the other hand, it can be shown that CVP is in $\mathcal{NP}$. Thus, we have the following theorem.

Theorem 3.5. The CVP is $\mathcal{NP}$-complete.

As with the SVP, there are many complexity results about approximating the CVP. We cite one of them here as an example.

Theorem 3.6 (Dinur, Kindler, Raz and Safra [34]**).** To approximate the closest vector of an n-dimensional lattice to a given point of $\mathbb{E}^n$ within a factor $n^{c/\log\log n}$, where c is some absolute constant, is $\mathcal{NP}$-hard.

It was conjectured by L. Babai in 1986 that the SVP is not harder than the CVP. In 1999, this conjecture was proved by Goldreich et al. [35]. On the other hand, in practice, a CVP in dimension n can usually be transformed into solving an SVP in dimension $n + 1$; so, for cryptographic purposes, they tend to be of roughly equal difficulty.

Theorem 3.7. There is an approximation-preserving polynomial time reduction from the SVP to the CVP.

The Lenstra–Lenstra–Lovász algorithm

Since every pair of bases of a lattice is connected by a unimodular matrix, when the initial basis of the lattice is not very good (for example, from the perspective of orthogonality), one may hope to reduce it to a good one. It is easy to show that, if $\mathbf{v}_1$ is one of the shortest vectors of the lattice, it has a basis with $\mathbf{v}_1$ as one of the n generators. Many great mathematicians have made contributions in reduction theory, including Lagrange, Gauss, Hermite, Minkowski, Voronoi, Korkin, and Zolotarov (see [14,36]). Nevertheless, in higher dimensions, finding or even approximating the shortest vector turns out to be extremely hard. In 1982, A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász [37] proposed an algorithm (known as the LLL algorithm), which can not only efficiently approximate the shortest vector of a lattice but also approximate the closest vector.

Theorem 3.8. Let Λ be an n-dimensional integer lattice, i.e., $\Lambda \subseteq \mathbb{Z}^n$, and let $\ell(\Lambda)$ denote the length of the shortest nonzero vector of Λ. The LLL algorithm can find a nonzero lattice vector $\mathbf{v} \in \Lambda$ in polynomial time satisfying

$$\|\mathbf{v}\| \le \left(2/\sqrt{3}\right)^n \ell(\Lambda). \tag{29}$$

Theorem 3.9 (Babai [38]**).** There are polynomial time algorithms that solve the CVP within a factor $2\left(2/\sqrt{3}\right)^n$. In other words, for any $\mathbf{x} \in \mathbb{E}^n$ one can find a lattice vector $\mathbf{v} \in \Lambda$ satisfying

$$\|\mathbf{x}-\mathbf{v}\| \le 2\left(2/\sqrt{3}\right)^n d(\mathbf{x},\Lambda). \tag{30}$$

In both Theorem 3.8 and Theorem 3.9, the approximation factors are exponential in the dimensions. Over the years, many efforts have been made to improve the approximation factors, such as the BKZ algorithm proposed in 1987 by C.-P. Schnorr and R. Kannan (see [39]). Nevertheless, no real progress has been achieved. Essentially, all these algorithms are based on various types of basis reductions, which will be introduced in the last section.

SVP and CVP have several variants and generalizations that are useful in lattice-based cryptosystems as well, such as SVP_γ, CVP_γ, GapSVP, GapCVP, the shortest basis problem (SBP), the quasi-orthogonal basis problem (QOBP), the successive minima problem (SMP), the shortest independent vector problem (SIVP), the shortest diagonal problem (SDP), and the densest sublattice problem (DSP) (see [13,15,27,28,40]). For example, let Λ be an n-dimensional lattice and let k be a given positive number, the GapSVP with approximation factor $\gamma(n)$ asks to decide whether $\ell(\Lambda) \le k$ or $\ell(\Lambda) > \gamma(n)k$.

The complexity of SVP and CVP for the quantum computer

Since the birth of Shor's quantum algorithms for discrete logarithms and factoring in 1994, in particular since the NIST initiated the post-quantum cryptography competition in 2016, people have tried hard to search for efficient quantum computing algorithms for the SVP and the CVP, or tried to prove that there is no such algorithm. Up to now, none of this effort has succeeded. This failure led to the following conjectures.

Conjecture 3.2. There is no polynomial time quantum algorithm that can approximate the SVP within a polynomial factor.

Conjecture 3.3. There is no polynomial time quantum algorithm that can approximate the CVP within a polynomial factor.

If Conjectures 3.2 and 3.3 are correct, they will provide evidence for the security of lattice-based cryptosystems in the quantum computing era. For the updated computational results, we refer the readers to [41].

Ball Packing and Ball Covering

Let B^n denote the n-dimensional unit ball $\{\mathbf{x}: \sum x_i^2 \le 1\}$ in $\mathbb{E}^n$ and let X denote a discrete set of points in $\mathbb{E}^n$. We call $B^n + X = \{B^n + \mathbf{x}_i : \mathbf{x}_i \in X\}$ a ball packing (in discrete geometry, it is called sphere packing rather than ball packing) if the interiors of the balls are disjoint. In particular, we call it a lattice ball packing if X is a lattice. Let $\delta(B^n)$ denote the density of the densest ball packings in $\mathbb{E}^n$ and let $\delta^*(B^n)$ denote the density of the densest lattice ball packings. Clearly, we have

$$\delta^*(B^n) \le \delta(B^n). \tag{31}$$

Assume that Λ is an n-dimensional lattice in $\mathbb{E}^n$. Let $\ell(\Lambda)$ denote the length of the shortest nonzero vectors of Λ and take $r = \ell(\Lambda)/2$. It is easy to see that $rB^n + \Lambda$ is a lattice ball packing in $\mathbb{E}^n$ (see Fig. 1). Then, the SVP can be reformulated in terms of ball packing.

SVP in ball packing. For a given n-dimensional lattice Λ, find the largest number r such that $rB^n + \Lambda$ is a ball packing and the corresponding balls that touch rB^n at its boundary.

In fact, based on the previous discussion, one can deduce the following connection between the length $\ell(\Lambda)$ of the shortest nonzero vector of a lattice Λ and the ball packing densities $\delta^*(B^n)$ and $\delta(B^n)$.

Theorem 4.1. Let Λ be an n-dimensional lattice and let ω_n denote the volume of B^n. We have

$$\ell(\Lambda) \le 2\sqrt[n]{\det(\Lambda)\cdot\delta^*(B^n)/\omega_n} \le 2\sqrt[n]{\det(\Lambda)\cdot\delta(B^n)/\omega_n}. \tag{32}$$

Ball packing, including the study of $\delta(B^n)$ and $\delta^*(B^n)$, is a classic subject in mathematics. It has been studied by many prominent mathematicians including Kepler, Newton, Gauss, and Minkowski (see [14]). However, our knowledge in this field is still very limited.

In 1594, T. Harriot discovered the face-centered cubic lattice ball packing in $\mathbb{E}^3$ and determined that its density is $\pi/\sqrt{18} = 0.74\cdots$. However, he was not able to prove that the density is the maximum. Then, he told his discovery to Kepler. In 1611, Kepler made the following conjecture: *The density of the densest ball packing in* $\mathbb{E}^3$ *is* $\pi/\sqrt{18}$. *In other words*,

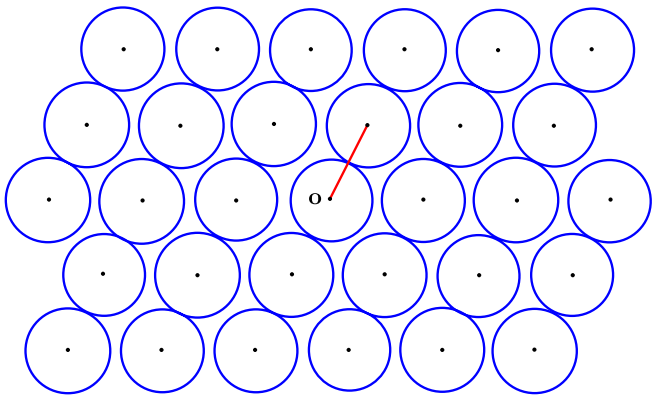

Fig. 1. SVP in ball packing. The balls of the radii of half the length of the shortest lattice vectors form a lattice packing.

$$\delta(B^3) = \frac{\pi}{\sqrt{18}}. \tag{33}$$

In 1694, Newton and D. Gregory discussed the following problem: *Can* 13 *unit balls in* $\mathbb{E}^3$ *be brought into contact with a fixed one*? These 2 natural and simple sounding problems initiated ball packing as a field of mathematical research. Some key results about $\delta^*(B^n)$ and $\delta(B^n)$ are summarized in Table 1 (see [14,42,43]).

Besides Theorem 4.1, reduction methods to determine the values of $\delta^*(B^n)$ are useful in algorithms for SVP and CVP. For example, the Korkin–Zolotarov reduction is employed in the block Korkin–Zolotarov algorithm developed by Schnorr [39] in 1987.

In general dimensions, we have

$$cn^2 2^{-n} \le \delta^*(B^n) \le \delta(B^n) \le 2^{-0.599n(1+o(1))} \tag{34}$$

for a suitable positive constant c, where a weaker lower bound was first proved by Minkowski in 1905, then improved and generalized by E. Hlawka, C. L. Siegel, H. Davenport, C. A. Rogers, W. M. Schmidt, B. Klartag, and others (see [44]), and the upper bound was proved by G. A. Kabatjanski and V. I. Levenštein in 1978 (see [14]). Clearly, the upper bound and Theorem 4.1 have the following corollary, which is an improvement of Theorem 3.2.

Corollary 4.1. Every lattice Λ of dimension n contains a nonzero vector $\mathbf{v}$ satisfying

$$\|\mathbf{v}\| \le \left(\pi^{-0.5}e^{-0.5}2^{-0.099} + o(1)\right)\sqrt[n]{\det(\Lambda)}\sqrt{n}. \tag{35}$$

There are hundreds of papers on ball packing, employing methods and tools from various fields of mathematics. As well, there are many fascinating open problems on ball packing. Here, we list 2 of them as examples.

Table 1. Known results about ball packing densities

n	$\delta^*(B^n)$	Author Date	$\delta(B^n)$	Author Date
2	$\frac{\pi}{\sqrt{12}}$	Lagrange 1173	$\frac{\pi}{\sqrt{12}}$	Thue 1892
3	$\frac{\pi}{\sqrt{18}}$	Gauss 1831	$\frac{\pi}{\sqrt{18}}$	Hales 2005
4	$\frac{\pi^2}{16}$	Korkin, Zolotarev 1872	??	??
5	$\frac{\pi^2}{15\sqrt{2}}$	Korkin, Zolotarev 1877	??	??
6	$\frac{\pi^3}{48\sqrt{3}}$	Blichfeldt 1925	??	??
7	$\frac{\pi^3}{105}$	Blichfeldt 1926	??	??
8	$\frac{\pi^4}{384}$	Blichfeldt 1934	$\frac{\pi^4}{384}$	Viazovska 2017
24	$\frac{\pi^{12}}{12!}$	Cohn, Kumar 2009	$\frac{\pi^{12}}{12!}$	Cohn, Kumar, Miller, Radchenko, Viazovska 2017

Problem 4.1. Determine the asymptotic orders of $\delta^*(B^n)$ and $\delta(B^n)$, if they exist.

Problem 4.2. Is there a dimension n satisfying

$$\delta^*\left(B^n\right) \neq \delta\left(B^n\right)? \tag{36}$$

Clearly, a solution to Problem 4.1 will provide further improvement of Theorem 4.1 and better understanding of SVP. Similar to the ball case, one can define and study lattice packing of any centrally symmetric convex body, which corresponds to the SVP in a metric linear space.

Assume that Λ is an n-dimensional lattice in $\mathbb{E}^n$. For every point $\mathbf{x} \in \mathbb{E}^n$, we define the distance between $\mathbf{x}$ and its closest lattice point $\mathbf{v} \in \Lambda$ as $d(\mathbf{x}, \Lambda)$. Then, we define

$$\rho(\Lambda) = \max_{\mathbf{x} \in \mathbb{E}^n} d(\mathbf{x}, \Lambda). \tag{37}$$

It is easy to see that $\rho(\Lambda)B^n + \Lambda$ is a covering of $\mathbb{E}^n$ (see Fig. 2). In fact, $\rho(\Lambda)$ is the smallest radius ρ such that $\rho B^n + \Lambda$ is a covering of $\mathbb{E}^n$.

CVP in ball covering. Given an n-dimensional lattice Λ, find the smallest number ρ such that $\rho B^n + \Lambda$ is a covering of $\mathbb{E}^n$. For any $\mathbf{x} \in \mathbb{E}^n$, find a lattice point $\mathbf{v} \in \rho B^n + \mathbf{x}$.

Clearly, finding a lattice point $\mathbf{v} \in \rho B^n + \mathbf{x}$ is slightly simpler than the CVP. However, this covering model can illustrate the fundamental difficulty of the CVP. First, unlike Theorem 3.2 and Theorem 4.1, there is no upper bound for $\rho(\Lambda)$ in terms of $\det(\Lambda)$ and n. Let m be a large integer, take $\mathbf{a}_1 = (m, 0)$ and $\mathbf{a}_2 = (0, 1/m)$, and define Λ to be the 2-dimensional lattice generated by $\mathbf{a}_1$ and $\mathbf{a}_2$. Then, we have $\det(\Lambda) = 1$. If $\mathbf{x} = (m/2, 1/2m)$, one can easily deduce that

$$\rho(\Lambda) = d(\mathbf{x}, \Lambda) = \frac{1}{2}\sqrt{m^2 + 1/m^2}. \tag{38}$$

Apparently, $\rho(\Lambda)$ can not be bounded from above just in terms of $\det(\Lambda)$.

Let $\theta(B^n)$ denote the density of the thinnest ball covering of $\mathbb{E}^n$ and let $\theta^*(B^n)$ denote the density of the thinnest lattice ball covering of $\mathbb{E}^n$. As a counterpart to Theorem 4.1, we have the following relation between $\rho(\Lambda)$ and $\theta^*(B^n)$.

Theorem 4.2. Let Λ be an n-dimensional lattice and let ω_n denote the volume of B^n. We have

$$\rho(\Lambda) \geq \sqrt[n]{\det(\Lambda) \cdot \theta^*(B^n)/\omega_n} \geq \sqrt[n]{\det(\Lambda) \cdot \theta(B^n)/\omega_n}. \tag{39}$$

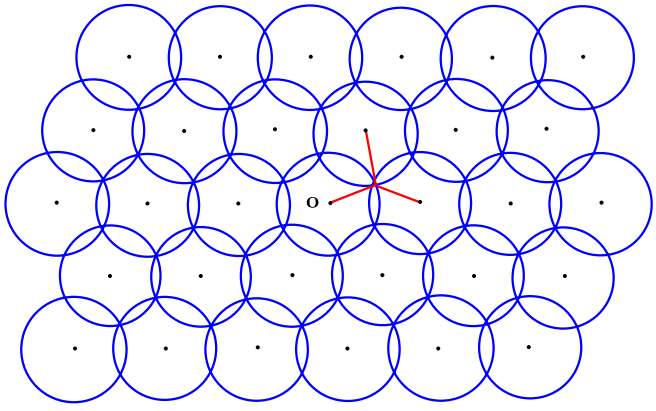

Fig. 2. CVP in the ball covering. The balls of radii of the maximum distance between a point to its closest lattice vectors form a lattice covering.

Ball covering, in certain sense, is regarded as a dual concept of ball packing. In fact, they are not much related. Up to now, the known exact results about $\theta(B^n)$ and $\theta^*(B^n)$ are summarized in Table 2.

In general dimensions, there is a constant c such that

$$(1+o(1))\frac{n}{\sqrt{e^3}} \leq \theta\left(B^n\right) \leq \theta^*\left(B^n\right) \leq cn\left(\log_e n\right)^{\log_2 \sqrt{2\pi e}}, \tag{40}$$

where the lower bound was achieved by H. S. M. Coxeter, L. Few, and Rogers in 1959, and the upper bound was discovered by Rogers in 1959 (see [21,45,46]). Clearly, the lower bound and Theorem 4.2 have the following corollary, which in certain sense shows the complexity of CVP.

Corollary 4.2. Let Λ be an n-dimensional lattice. We have

$$\rho(\Lambda) \geq \left((2\pi e)^{-0.5} + o(1)\right)\sqrt[n]{\det(\Lambda)}\sqrt{n}. \tag{41}$$

Corollary 4.1 and Corollary 4.2 together provide an explanation for Theorem 3.7, i.e., the CVP is harder than the SVP.

One may realize that there are very few concrete results on ball covering in the past half a century, particularly compared to ball packing. It is fascinating to notice that, unlike the packing case, the thinnest lattice ball covering in $\mathbb{E}^8$ is not achieved by the E_8 lattice. At least, the A_8^* lattice provides a ball covering with a density thinner than the E_8 lattice. Therefore, the following problem is important and perhaps very challenging.

Problem 4.3. Determine the values of $\theta^*\left(B^8\right)$, $\theta\left(B^8\right)$, $\theta^*\left(B^{24}\right)$, and $\theta\left(B^{24}\right)$.

Two bridges connecting SVP and CVP

Let $\mathcal{L}_n$ denote the family of all n-dimensional lattices. In 1950, Rogers defined and studied

$$\phi^*\left(B^n\right) = \min_{\Lambda \in \mathcal{L}_n} \frac{2\rho(\Lambda)}{\ell(\Lambda)}, \tag{42}$$

where $\ell(\Lambda)$ is the length of the shortest nonzero vectors of Λ and $\rho(\Lambda)$ is the maximum distance between a point $\mathbf{x} \in \mathbb{E}^n$ and its closest lattice point. They are known as Rogers' constants.

From the intuitive point of view, one may think that $\phi^*(B^n)$ can be arbitrarily large when $n \to \infty$. Surprisingly, Rogers proved by a reduction method that

$$\phi^*\left(B^n\right) \leq 3 \tag{43}$$

Table 2. Known results about ball covering densities

n	$\theta^*\left(B^n\right)$	Author Date	$\theta\left(B^n\right)$	Author Date
2	$\frac{2\pi}{3\sqrt{3}}$	Kersshner 1939	$\frac{2\pi}{3\sqrt{3}}$	Kersshner 1939
3	$\frac{5\sqrt{5}\pi}{24}$	Bambah 1954	??	??
4	$\frac{2\pi^2}{5\sqrt{5}}$	Delone, Ryskov 1963	??	??
5	$\frac{245\sqrt{35}\pi^2}{3888\sqrt{3}}$	Ryskov, Baranovskii 1975	??	??

holds in every dimension. In 1972, via mean value techniques developed by Rogers and Siegel, G. L. Butler improved Rogers' upper bound to

$$\phi^*\left(B^n\right) \leq 2 + o(1). \tag{44}$$

It follows from Rogers' upper bound that, for many n-dimensional lattices, the longest distance in CVP is only a constant multiple of the length of the SVP. In recent years, this idea has been applied to cryptographic analysis by Micciancio [47] and others.

The constant $\phi^*(B^n)$ has a couple of different interpretations. For example, $\phi^*(B^n)$ is the largest number such that every lattice ball packing $B^n + \Lambda$ has a hole into which one can put a ball of radius $\phi^*(B^n) - 1$. In the 1980s, several mathematicians studied $\phi^*(B^n)$ from different respects. Up to now, the known exact results are listed in Table 3.

Just like the ball covering case, there are many important open problems about $\phi^*(B^n)$. We list 2 of them here as examples.

Problem 4.4. Determine the values of $\phi^*\left(B^8\right)$ and $\phi^*\left(B^{24}\right)$, and their corresponding lattices.

Problem 4.5. Is there a dimension n such that

$$\phi^*\left(B^n\right) \geq 2? \tag{45}$$

What is known about the Leech lattice supports the conjecture that $\phi^*\left(B^{24}\right) = \sqrt{2}$. If one can improve Butler's upper bound to $\phi^*(B^n) \leq 2 - c$, where c is a positive constant, the lower bound for $\delta^*(B^n)$ will be improved to

$$\delta^*\left(B^n\right) \geq (2-c)^{-n}. \tag{46}$$

If a dimension n can be found such that $\phi^*(B^n) \geq 2$, then

$$\delta^*\left(B^n\right) \neq \delta\left(B^n\right), \tag{47}$$

which would solve Problem 4.2. It is easy to see that $\phi^*(B^n)$ can be generalized from the ball to arbitrary centrally symmetric convex bodies. For more on $\phi^*(B^n)$ and its generalizations, we refer to [48–50].

There is another important notion that is closely related to both the SVP and the CVP, the Dirichlet–Voronoi cell of Λ:

$$D = \left\{\mathbf{x}: \langle \mathbf{x}, \mathbf{v}\rangle \leq \frac{1}{2}\langle \mathbf{v}, \mathbf{v}\rangle \text{ for all } \mathbf{v} \in \Lambda \setminus \{\mathbf{o}\}\right\}. \tag{48}$$

Roughly speaking, D is the set of points that are closer to the origin than any other lattice point. Clearly, D is a centrally symmetric polytope such that $D + \Lambda$ is a tiling of $\mathbb{E}^n$ (see Fig. 3).

Table 3. Known results about Rogers' constants

n	2	3	4	5
$\phi^*(B^n)$	$2/\sqrt{3}$	$\sqrt{5/3}$	$\sqrt{2\sqrt{3}\left(\sqrt{3}-1\right)}$	$\sqrt{\frac{3}{2}+\sqrt{\frac{13}{6}}}$
Author		Boroczky	Horvath	Hovarth
Date		1986	1982	1986

Furthermore, one can deduce that

$$\ell(\Lambda) = 2\min\{d(\mathbf{o}, F): F \text{ is a facet of } D\} \tag{49}$$

and

$$\rho(\Lambda) = \max\{\|\mathbf{v}\|: \mathbf{v} \text{ is a vertex of } D\}. \tag{50}$$

Therefore, the Dirichlet–Voronoi cell of a lattice encodes information about both SVP and CVP. In fact, the CVP can be reformulated as:

CVP in D–V cell. Let Λ be an n-dimensional lattice and $\mathbf{x}$ be an arbitrary point of $\mathbb{E}^n$. If D is the Dirichlet–Voronoi cell of Λ, find a lattice point $\mathbf{v}$ satisfying $\mathbf{x} \in D + \mathbf{v}$.

We end this section with 2 well-known problems about the Dirichlet–Voronoi cells of lattices.

Problem 4.6. When $n \geq 6$, classify all Dirichlet–Voronoi cells of the n-dimensional lattices, i.e., determine their geometric shapes.

Voronoi's conjecture. Every parallelotope is an affine image of a lattice Dirichlet–Voronoi cell.

When $n \leq 5$, both Problem 4.6 and Voronoi's conjecture have been solved. The Dirichlet–Voronoi cell has been applied to lattice-based cryptography by Micciancio and others since 2010.

Positive Definite Quadratic Forms

Let Λ be a lattice with a basis $\left\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\right\}$, where $\mathbf{a}_i = \left(a_{i1}, a_{i2}, \ldots, a_{in}\right)$, and let A denote the $n \times n$ matrix with entries a_{ij}. Then, the lattice can be expressed as

$$\Lambda = \left\{\mathbf{z}A: \ \mathbf{z} \in \mathbb{Z}^n\right\} \tag{51}$$

and the norms of the lattice vectors can be expressed as a positive definite quadratic form

$$Q(\mathbf{z}) = \langle \mathbf{z}A, \mathbf{z}A\rangle = \mathbf{z}AA'\mathbf{z}', \tag{52}$$

where A' and $\mathbf{z}'$ indicate the transposes of A and $\mathbf{z}$, respectively. Assume that

$$Q(\mathbf{x}) = \sum_{1 \leq i,j \leq n} c_{ij}x_ix_j = \mathbf{x}C\mathbf{x}' \tag{53}$$

is a positive definite quadratic form of n variables, where $c_{ij} = c_{ji}$ and C is the symmetric matrix with entries c_{ij}. It is known that there is an $n \times n$ matrix A satisfying $C = AA'$. Then, the quadratic form also produces a lattice

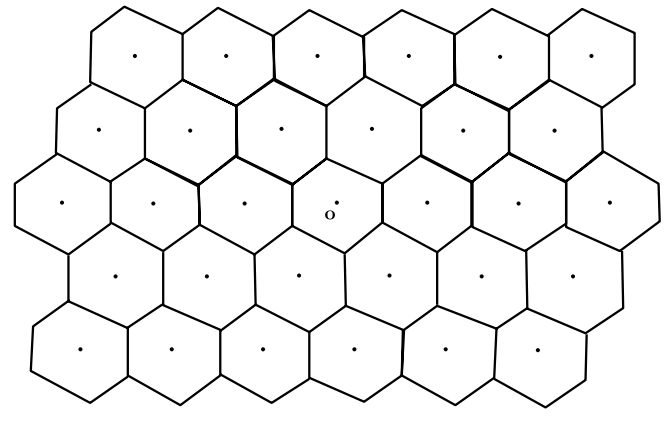

Fig. 3. CVP in D–V cell. The Dirichlet–Voronoi cells form a lattice tiling.

$$\Lambda = \{\mathbf{z}A:\ \mathbf{z}\in\mathbb{Z}^n\}. \tag{54}$$

Therefore, there is a nice correspondence between lattices and positive definite quadratic forms. Then, the SVP is equivalent to the following problem.

SVP in quadratic form. Find a nonzero vector $\mathbf{z}\in\mathbb{Z}^n$ that minimizes the positive definite quadratic form $Q(\mathbf{z})$.

Let $\mathrm{dis}(Q)$ be the discriminant of the quadratic form $Q(\mathbf{x})$ and let $\mathcal{Q}_n$ denote the family of all positive definite quadratic forms in n variables. Then, we define

$$m(Q) = \min_{\mathbf{z}\in\mathbb{Z}^n\setminus\{\mathbf{o}\}} Q(\mathbf{z}) \tag{55}$$

and

$$\gamma_n = \sup_{Q\in\mathcal{Q}_n} \frac{m(Q)}{\sqrt[n]{\mathrm{dis}(Q)}}. \tag{56}$$

Usually, γ_n is called Hermite's constant. These constants are closely related to the densities $\delta^*(B^n)$ of the densest lattice ball packings. Since $\ell(\Lambda)=\sqrt{m(Q)}$ and $\mathrm{dis}(Q)=\det(\Lambda)^2$, one can easily deduce that

$$\delta^*\left(B^n\right) = \frac{\omega_n \gamma_n^{n/2}}{2^n}, \tag{57}$$

where ω_n is the volume of the n-dimensional unit ball B^n. In fact, all the known exact results about $\delta^*(B^n)\left(\text{except }\delta^*\left(B^{24}\right)\right)$ were derived from the known results about γ_n (see Table 4).

In lattice-based cryptography, approximating SVP is practically important. In fact, both SIS and LWE can be reduced to this type of problems. Let γ be a suitable positive number or a suitable function of n. Then, the SVP_γ asking, for any given n-dimensional lattice Λ, to find a nonzero lattice point $\mathbf{v}\in\Lambda$ satisfying

$$||\mathbf{v}|| \le \gamma\,\ell(\Lambda). \tag{58}$$

In terms of positive definite quadratic forms, the SVP_γ can be reformulated as:

SVPγ in quadratic form. For a given positive definite quadratic form $Q(\mathbf{z})$ and a suitable approximation parameter γ, find a nonzero integral solution $\mathbf{z}$ to

$$Q(\mathbf{z}) \le \gamma^2 m(Q). \tag{59}$$

Table 4. Known results about Hermite's constants

n	γ_n	Author Date	n	γ_n	Author Date
2	$2/\sqrt{3}$	Lagrange 1773	6	$\sqrt[6]{\frac{64}{3}}$	Blichfeldt 1925
3	$\sqrt[3]{2}$	Gauss 1831	7	$\sqrt[7]{64}$	Blichfeldt 1926
4	$\sqrt{2}$	Zolotarev, Korkin 1872	8	2	Blichfeldt 1934
5	$\sqrt[5]{8}$	Zolotarev, Korkin 1877	24	4	Cohn, Kumar 2009

In 1953, R. A. Rankin [51] introduced a generalization of Hermite's constant. Let r be an integer, $1\le r\le n-1$, and let $m_r(Q)$ denote the lower bound of any principal minor of order r of any form equivalent to $Q(\mathbf{x})$. He defined

$$\gamma_{n,r} = \sup_{Q\in\mathcal{Q}_n} \frac{m_r(Q)}{\mathrm{dis}(Q)^{r/n}}. \tag{60}$$

Twenty years ago, Rankin's constant led P. Nguyen and others to introduce the DSP, a generalization of the SVP. This new problem has been studied by Micciancio, Nguyen, and others. It has important applications to blockwise lattice reduction generalizing LLL and Schnorr's algorithm.

Assume that $\Lambda=\{\mathbf{z}A:\ \mathbf{z}\in\mathbb{Z}^n\}$ is an n-dimensional lattice in $\mathbb{E}^n$, where A is a nonsingular $n\times n$ matrix. For any point $\mathbf{p}=\mathbf{y}A\in\mathbb{E}^n$ and $\mathbf{v}=\mathbf{z}A\in\Lambda$, we have

$$\|\mathbf{p}-\mathbf{v}\| = \|(\mathbf{y}-\mathbf{z})A\| = \sqrt{Q(\mathbf{y}-\mathbf{z})}. \tag{61}$$

Therefore, the CVP is equivalent to the following problem.

CVP in quadratic form. Given a positive definite quadratic form $Q(\mathbf{x})$ and a vector $\mathbf{y}$, find an integer vector $\mathbf{z}\in\mathbb{Z}^n$ that minimizes $Q(\mathbf{y}-\mathbf{z})$.

Let C denote the unit cube $\left\{\left(x_1,x_2,\ldots,x_n\right):\ 0\le x_i<1\right\}$, let Λ be the lattice corresponding to $Q(\mathbf{x})$, and define

$$\rho(Q) = \sqrt{\max_{\mathbf{y}\in C}\min_{\mathbf{z}\in\mathbb{Z}^n} Q(\mathbf{y}-\mathbf{z})}. \tag{62}$$

It can be verified that $\rho(Q)$ is the smallest number ρ such that $\rho B^n+\Lambda$ is a ball covering of $\mathbb{E}^n$. Consequently, we get

$$\theta^*\left(B^n\right) = \min_{Q\in\mathcal{Q}_n} \frac{\omega_n \rho(Q)^n}{\sqrt{\mathrm{dis}(Q)}}. \tag{63}$$

In fact, most of the known exact results about $\delta^*(B^n)$ and $\theta^*(B^n)$ were achieved by studying quadratic forms.

Besides the fact that both SVP and CVP can be reformulated in terms of quadratic forms, in recent years Nguyen, L. Ducas, and others have applied quadratic forms directly to lattice-based cryptography.

Reduction theory of quadratic forms (lattices)

If $\{\mathbf{a}_1,\mathbf{a}_2,\ldots,\mathbf{a}_n\}$ is an orthogonal basis of Λ, then the corresponding quadratic form $Q(\mathbf{x})=\mathbf{x}C\mathbf{x}'$ is standard. In this case, both SVP and CVP can be solved easily, since the shortest basis vector is the shortest nonzero lattice vector of Λ. If $\mathbf{w}=w_1\mathbf{a}_1+w_2\mathbf{a}_2+\cdots+w_n\mathbf{a}_n\in\mathbb{E}^n$, taking

$$\mathbf{v} = \lfloor w_1\rceil\mathbf{a}_1+\lfloor w_2\rceil\mathbf{a}_2+\cdots+\lfloor w_n\rceil\mathbf{a}_n, \tag{64}$$

where $\lfloor x\rceil$ denotes the closest integer to x, one can show that $\mathbf{v}\in\Lambda$ is a closest lattice vector of $\mathbf{w}$.

It is well known that most lattices have no orthogonal bases. Nevertheless, every lattice has some relatively good bases. Correspondingly, every positive definite quadratic form has a comparatively good equivalent form. This is the philosophy of reduction theory. In history, reduction theory was first developed for quadratic forms rather than for lattices.

Let U be a unimodular matrix and write

$$\tilde{Q}(\mathbf{x}) = \mathbf{x}UCU'\mathbf{x}'. \tag{65}$$

We say $\tilde{Q}(\mathbf{x})$ is equivalent to $Q(\mathbf{x})$. Since the map $\mathbf{z}\to\mathbf{z}U$ is an automophism in $\mathbb{Z}^n$, one has

$$m(\tilde{Q}) = m(Q) \tag{66}$$

and

$$\mathrm{dis}(\tilde{Q}) = \det(UCU') = \mathrm{dis}(Q). \tag{67}$$

In 1773, Lagrange proved that every positive definite binary quadratic form $Q(\mathbf{x}) = \mathbf{x}C\mathbf{x}'$ is equivalent to one satisfying

$$\begin{cases} c_{11} \le c_{22}, \\ 0 \le 2c_{12} \le c_{11}, \end{cases} \tag{68}$$

which marked the birth of the reduction theory. In other words, every 2-dimensional lattice has a basis $\{\mathbf{a}_1, \mathbf{a}_2\}$ such that the angle between $\mathbf{a}_1$ and $\mathbf{a}_2$ is at least $\pi/3$ and at most $\pi/2$. Then, one can deduce that $\gamma_2 = 2/\sqrt{3}$ and $\delta^*(B^2) = \pi/\sqrt{12}$.

Reduction theory has been further developed by Seeber, Gauss, Hermite, Korkin, Zolotarev, Minkowski, Voronoi, and many modern authors (see [14,36]). We introduce 3 reductions as examples.

Korkin–Zolotarev reduction

In 1873, Korkin and Zolotarev proposed the following reduction: A positive definite quadratic form $Q(\mathbf{x})$ is said to be K–Z reduced if

$$Q(\mathbf{x}) = \sum_{i=1}^{n} c_i \left(x_i + \sum_{j=i+1}^{n} t_{ij} x_j \right)^2, \tag{69}$$

where $|\ t_{ij}\ | \le 1/2$ and

$$c_i = \min_{(z_i, z_{i+1}, \ldots, z_n) \ne \mathbf{o}} \left\{ \sum_{j=i}^{n} c_j \left(z_j + \sum_{k=j+1}^{n} t_{jk} z_k \right)^2 \right\}. \tag{70}$$

Clearly, the first basis vector in the corresponding lattice of a K–Z reduced form is the shortest nonzero lattice vector. Then, they proved the following theorem.

Theorem 5.1. Every positive definite quadratic form is equivalent to a K–Z reduced one.

Korkin and Zolotarev were not able to explore further in this direction since Zolotarev died in 1878 at the age of 31. However, in 1934, Blichfeldt succeeded in determining the values of γ_6, γ_7, and γ_8 by Korkin and Zolotarev's reduction theory (see [14]). In particular, in 1987, Schnorr [39] developed a generalization of the LLL algorithm based on this reduction, known as block Korkin–Zolotarev (BKZ) algorithm, to approximate the SVP.

Minkowski reduction

As a generalization of Lagrange's pioneering work, in 1905, Minkowski discovered the following reduction: As usual, we denote the greatest common divisor of k integers $z_1, z_2, \ldots, z_k$ by $\gcd(z_1, z_2, \ldots, z_k)$. A positive definite quadratic form $Q(\mathbf{x}) = \mathbf{x}C\mathbf{x}'$ is said to be Minkowski reduced, if

$$c_{1j} \ge 0, \quad j = 2, 3, \ldots, n, \tag{71}$$

and

$$Q(\mathbf{z}) \ge c_{ii}, \quad i = 1, 2, \ldots, n, \tag{72}$$

for all integer vectors $\mathbf{z} = (z_1, z_2, \ldots, z_n)$ such that

$$\gcd(z_i, z_{i+1}, \ldots, z_n) = 1. \tag{73}$$

It is easy to see that the first basis vector in the corresponding lattice of a Minkowski reduced form is the shortest nonzero lattice vector. Then, he proved the following theorem.

Theorem 5.2. Every positive definite quadratic form is equivalent to a Minkowski reduced one.

Minkowski reduction has been studied by many authors, including B. L. van der Waerden, K. Mahler, and E. S. Barnes, in particular with respect to the orthogonality defect of a lattice, which is also useful in lattice-based cryptography.

Lenstra–Lenstra–Lovász reduction

Assume that $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ is a basis of an n-dimensional lattice Λ. We define the associated Gram–Schmidt orthogonal basis as

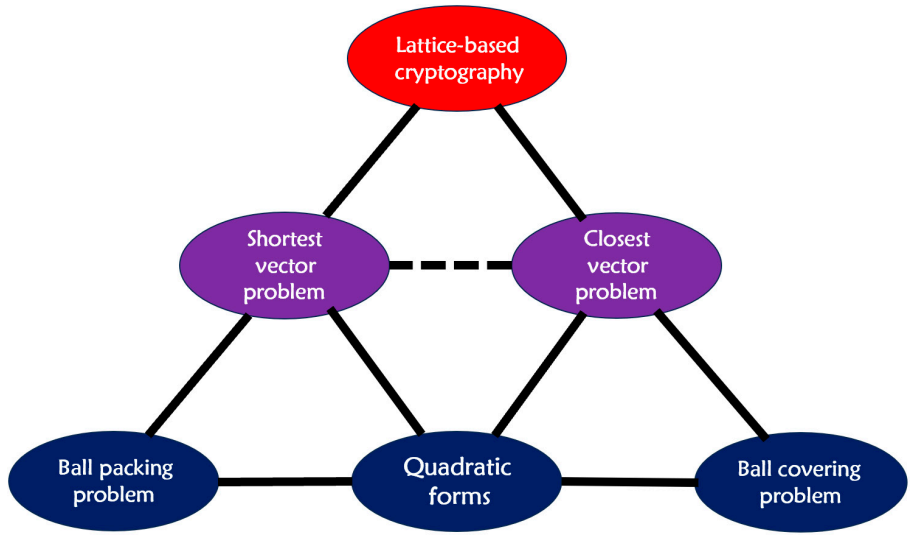

Fig. 4. Lattice-based cryptography is deeply rooted in mathematics.

$$\mathbf{a}_i^* = \mathbf{a}_i - \sum_{j<i} \mu_{ij} \mathbf{a}_j^*, \quad \text{where } \mu_{ij} = \frac{\left\langle \mathbf{a}_i, \mathbf{a}_j^* \right\rangle}{\left\langle \mathbf{a}_j^*, \mathbf{a}_j^* \right\rangle}. \tag{74}$$

In 1982, Lenstra, Lenstra Jr., and Lovász [37] introduced the LLL reduction: A basis $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n\}$ of an n-dimensional lattice Λ is called to be LLL reduced if

$$\left|\mu_{ij}\right| = \frac{\left|\left\langle \mathbf{a}_i\, \mathbf{a}_j^* \right\rangle\right|}{\left\langle \mathbf{a}_j^*\, \mathbf{a}_j^* \right\rangle} \le \frac{1}{2} \quad \text{for all } 1 \le j < i \le n \tag{75}$$

and

$$\|\mathbf{a}_i^*\|^2 \ge \sigma \|\mathbf{a}_{i-1}^*\|^2 \quad \text{for all } i = 2, 3, \ldots, n, \tag{76}$$

where

$$\sigma = \frac{1}{4} + \left(\frac{3}{4}\right)^{n/(n-1)}. \tag{77}$$

This time, there is no guarantee that $\mathbf{a}_1$ is the shortest nonzero lattice vector of Λ. However, it is an approximating shortest nonzero lattice vector. By inventing an algorithm that always can terminate at an LLL reduced basis in polynomial time, they proved Theorem 3.8.

Reduction theory has played a key role in the security analysis of lattice-based cryptography for the classical computer. Naturally, it will be the key tool for the security analysis of lattice-based cryptography for the quantum computer.

Summary and Outlook

Quantum computing is widely believed to be a revolutionary new technology. In fact, it is a double-edged sword. If efficient quantum computers can be manufactured in the near future, many of the current cryptosystems will be in danger and post-quantum cryptography will be crucial to the security of our communications. It is possible that better cryptosystems can be invented to deal with quantum computing attacks in the future. Nevertheless, up to now, lattice-based cryptosystems are the best candidates to defend the communication security in the forthcoming quantum computer era.

The security of the lattice-based cryptosystems relies on the computational complexity of some fundamental lattice problems such as the SVP, the CVP, and their generalizations, which are deeply rooted in the work of Gauss, Hermite, Korkin, Zolotarev, Minkowski, Siegel, van der Wearden, and many contemporary mathematicians, as shown by Fig. 4. This makes post-quantum cryptography one of the few distinguished examples of crucial modern technology growing up from pure mathematics.

If a new technology can create not only revolutionary progresses but also disastrous harms, preventing the disasters should be much more important and urgent than gaining the benefits. Therefore, post-quantum cryptography provides unprecedented opportunities for mathematicians to make contributions in modern technology (see [52]).

If we compare lattice-based cryptography as a fruit tree, the mathematics discussed in this article should be regarded as its roots. No matter how the post-quantum cryptography will develop in the future, mathematics is inevitable since it needs complicated models just like lattices. Of course, only mathematics is not enough. Successful post-quantum cryptography must be a joint work of mathematicians, cryptographers, and quantum computing scientists.

Acknowledgments

I thank G. Tian and X. Wang for their constant support for this field and R. Gardner, J. Pipher, L. Lovász, and the referees for their helpful suggestions and comments to this paper.
Funding: This work is supported by the National Natural Science Foundation of China (NSFC12226006 and NSFC11921001) and the Natural Key Research and Development Program of China (2018YFA0704701).
Competing interests: The author declares that he has no competing interests.

References

1. Diffie W, Hellman ME. New directions in cryptography. *IEEE Trans Inform Theory*. 1976;22(6):644–654.
2. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Commun ACM*. 1978;21(2):120–126.
3. Goldwasser S. *Mathematical foundations of modern cryptography: Computational complexity perspective*. Beijing: Proc. ICM. Higher Education Press; 2002. p. 245–272.
4. Hoffstein J, Pipher J, Silverman JH. *An introduction to mathematical cryptography*. New York: Springer-Verlag; 2008.
5. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans Inform Theory*. 1985;31(4):469–472.
6. Miller VS. Use of elliptic curves in cryptography. Advances in cryptology. Santa Barbara. *LNCS*. 1986;218:417–426.
7. Koblitz N. Elliptic curve cryptosystems. *Math Comput*. 1987;48(177):203–209.
8. Ajtai M, Dwork C. A public-key cryptosystem with worst-case/average-case equivalence. Paper presented at: Proceedings of the 29th Annual ACM Symposium on Theory of Computing; 1997; El Paso, TX, USA.
9. Goldreich O, Goldwasser S, Halevi S. Public-key cryptosystems from lattice reduction problems. In: Kaliski BS, editor. *Advances in Cryptology—CRYPTO '97. CRYPTO 1997. Lecture Notes in Computer Science, vol 1294*. Berlin, Heidelberg: Springer, Berlin, Heidelberg; 1997. p. 112–131.
10. Hoffstein J, Pipher J, Silverman JH. NTRU: A ring-based public key cryptosystem. *Algorithmic Number Theory LNCS*. 1998;1423:267–288.
11. Regev O. On lattices, learning with errors, random linear codes, and cryptography. In: *Proceedings of the 37th ACM Symposium on Theory of Computing*. New York (NY): ACM Press; 2005. p. 84–93.
12. Gentry C. Fully homomorphic encryption using ideal lattices. In: *Proceedings of the ACM International Symposium on Theory of Computing*. New York (NY): ACM Press; 2009. p. 169–178.
13. Micciancio D, Goldwasser S. *Complexity of lattice problems: A cryptographic perspective*. Boston: Kluwer Academic; 2002.
14. Zong C. *Sphere packings*. New York: Springer-Verlag; 1999.
15. Peikert C. A decade of lattice cryptography. *Found Trends Theor Comput Sci*. 2014;10(4):283–424.
16. Baaquie BE, Kwek LC. *Quantum computers: Theory and algorithms*. Singapore: Springer; 2023.

17. Landsberg JM. *Quantum computation and quantum information*. Providence: AMS; 2024.
18. Deutsch D, Jozsa R. Rapid solution of problems by quantum computation. *Proc R Soc London Ser A*. 1992;439(1907):553–558.
19. Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. Paper presented at: 35th Annual Symposium on Foundations of Computer Science; 1994; Los Alamitos, CA, USA.
20. Proos J, Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Inform Comput*. 2003;3:317–344.
21. Regev O. An efficient quantum factoring algorithm. *J ACM*. 2025;72(1):1–3.
22. Alvarado M, Gayler L, Seals A, Wang T, Hou T. A survey on post-quantum cryptography: State-of-the-art and challenges. arXiv. 2023. https://doi.org/10.48550/arXiv.2312.10430
23. Bisheh-Niasar M, Azarderakhsh R, Mozaffari-Kermani M. Instruction-set accelerated implementation of CRYSTALS-Kyber. *IEEE Trans Circuits Syst I Regular Papers*. 2021;68(11):4648–4659.
24. Canto AC, Kaur J, Mozaffari-Kermani M, Azarderakhsh R. Algorithmic security is insufficient: A comprehensive survey on implementation attacks haunting post-quantum security. arXiv. 2023. https://doi.org/10.48550/arXiv.2305.13544
25. Sanal P, Karagoz E, Seo H, Azarderakhsh R, Mozaffari-Kermani M. Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM cortex-a processors. In: *Security and privacy in communication networks*. Switzerland: Springer; 2021. p. 424–440.
26. Micciancio D, Regev O. Lattice-based cryptography. In: *Post-quantum cryptography*. Berlin: Springer-Verlag; 2009.
27. Wang X, Xu G, Yu Y. Lattice-based cryptography: A survey. *Chin Ann Math Ser B*. 2023;44:945–960.
28. Zhang J, Zhang Z. *Lattice-based cryptosystems: a design perspective*. Singapore: Springer-Verlag; 2020.
29. Södergren A. On the distribution of angles between the N shortest vectors in a random lattice. *J Lond Math Soc*. 2011;84(3):749–764.
30. van Emde Boas P. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical Report. Math. Institute: University of Amsterdam; 1981. p. 81–04.
31. Ajtai M. The shortest vector problem in L2 is NP-hard for randomized reductions. Paper presented at: Proceedings of the 30th Annual ACM Symposium on Theory of Computing; 1998; Dallas, TX, USA.
32. Khot S. Hardness of approximating the shortest vector problem in lattices. *J ACM*. 2005;52(5):789–808.
33. Ajtai M. Generating hard instances of lattice problems. *Quad Mat*. 2004;13:1–32.
34. Dinur I, Kindler G, Raz R, Safra S. Approximating CVP to within almost-polynomial factors is NP-hard. *Combinatorica*. 2003;23:205–243.
35. Goldreich O, Micciancio D, Safra S, Seifert JP. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Inf Process Lett*. 1999;71(2):55–61.
36. Nguyen PO, Stehlé D. Low-dimensional lattice basis reduction revisited. *ACM Trans Algorithms*. 2009;5:1–48.
37. Lenstra AK, Lenstra HW Jr, Lovász L. Factoring polynomials with rational coefficients. *Math Ann*. 1982;261(4):515–534.
38. Babai L. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*. 1986;6(1):1–13.
39. Schnorr CP. A hierarchy of polynomial time lattice basis reduction algorithms. *Theor Comput Sci*. 1987;53(2-3):201–224.
40. Malygina ES, Kutsenko AV, Novoselov SA, Kolesnikov NS, Bakharev AO, Khilchuk IS, Shaporenko AS, Tokareva NN. Post-quantum cryptosystems: Open problems and solutions. Lattice-based cryptosystems. *J Appl Ind Math*. 2023;17(4):767–790.
41. Aggarwal D, Chen Y, Kumar R, Shen Y. Improved classical and quantum algorithms for the shortest vector problem via bounded distance decoding. *SIAM J Comput*. 2025;54(2):233–278.
42. Cohn H, Kumar A, Miller SD, Radchenko D, Viazovska M. The sphere packing problem in dimension 24. *Ann Math*. 2017;185(3):1017–1033.
43. Viazovska M. The sphere packing problem in dimension 8. *Ann Math*. 2017;185:991–1015.
44. Klartag B. Lattice packing of spheres in high dimensions using a stochastically evolving ellipsoid. arXiv. 2025. https://doi.org/10.48550/arXiv.2504.05042
45. Ordentlich O, Regev O, Weiss B. New bounds on the density of lattice coverings. *J Am Math Soc*. 2022;35(1):295–308.
46. Rogers CA. *Packing and covering*. Cambridge: Cambridge University Press; 1964.
47. Micciancio D. Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor. *SIAM J Comput*. 2004;34(1):118–169.
48. Kannan R, Lovász L. Covering minima and lattice-point-free convex bodies. *Ann Math*. 1988;128:577–602.
49. Zong C. From deep holes to free planes. *Bull Amer Math Soc*. 2002;39:533–555.
50. Zong C. Some mathematical mysteries in lattices (abstract of a plenary talk). ASIACRYPT 2012. *LNCS*. 2012;7658:2–3.
51. Rankin RA. On positive definite quadratic forms. *J Lond Math Soc*. 1953;28(3):309–314.
52. Ding J, Smith-Tone D. Post-quantum cryptography—A new opportunity and challenge for the mathematical community. *Not Am Math Soc*. 2017;64(7):709–710.