

University of Technology Darmstadt
Department of Computer Science
Cryptography and Computeralgebra

Diploma Thesis

December 2008

On a Special Class of Lattices, Computational Problems, and Hash Functions



Kevin Schelten

University of Technology Darmstadt
Department of Mathematics

Supervised by Prof. Dr. Johannes Buchmann,
Dipl.-Math. Richard Lindner,
Dipl.-Inf. Markus Rückert.

Acknowledgements

I would like to thank the following people.

- Prof. Dr. Johannes Buchmann, for a fascinating thesis.
- Dipl.-Math. Richard Lindner and Dipl.-Inf. Markus Rückert, for inspiring scientific guidance.

Warranty

I hereby warrant that the content of this thesis is the direct result of my own work and that any use made in it of published or unpublished material is fully and correctly referenced.

Date: Signature:

Contents

Introduction	1
1 Preliminaries	4
1.1 Lattices	4
1.2 Basic Algebraic Number Theory	5
Algebraic Numbers	5
Canonical Embedding	7
Ring of Integers and Geometry	9
2 A Worst-Case to Average-Case Lattice Problem Reduction with a Logarithmic Connection Factor	14
2.1 Notation	14
2.2 Overview	15
2.3 Cryptographic Background	15
2.4 Main Result	16
2.4.1 Setting and Main Result	16
2.4.2 Proof Overview	19
3 Further Ideas	23
3.1 An Alternate Canonical Embedding	23
3.2 Cryptographic Hardness	24
3.3 Relating K -ISVP $_{\gamma}^{\infty}$ to f -SPP $_{\gamma}$ for Monogenic Number Fields	26
Conclusion	34

Introduction

As an introduction, we explain the notion and significance of hash functions in cryptography. Moreover, we sketch the development of lattice based hash functions in cryptography from 1996 to 2008.

We begin by introducing the most important concepts (the following definitions are taken from [3], [17]). A *hash function* is a computationally efficient function that maps a bit string of arbitrary length to a bit string of fixed length. In cryptography, a hash function h typically maps from a message space \mathcal{M} into a space of hash values \mathcal{C} . For a message $m \in \mathcal{M}$, the hash value $h(m) \in \mathcal{C}$ is also referred to as the message *digest*. Further, we call a function *one way*, if it is computationally efficient, but given a randomly chosen element of the image, it is computationally infeasible to compute a pre-image. One way hash functions prevent unauthorized reconstruction of the original message from the message digest. Additionally, a *collision* of a hash function is a distinct pair of inputs which are mapped to the same hash value. Since the domain of a hash function is typically much larger than the space of hash values, the pigeonhole principle yields that collisions exist. We define a *collision resistant* hash function as a one way hash function for which it is computationally hard to find collisions. Finally, we mention without further explanation that hash functions tend to be specified as keyed function families $\{h_k : \mathcal{M} \rightarrow \mathcal{C}\}$, see [15], p. 8.

In this paragraph, we rely on [12] to sketch the role of hash functions in cryptography. Note that typically, cryptographic tools are called *primitives*. In modern cryptography, hash functions are one of the most important cryptographic primitives. Hash functions are most commonly applied with *digital signatures* and *data integrity*. We shed further light on the former; the reader can find material on the latter in [12], p. 33. In the context of digital signatures, hash functions enhance efficiency by saving time and space. Instead of signing a (potentially long) message, the hash value of the message is signed. Collision resistance of the hash function is imperative for this purpose.

We carry on with lattices. A lattice is a discrete additive subgroup of \mathbb{R}^m . One of the most studied computational problems for lattices is the Shortest Vector Problem (SVP). Regarding this problem, cryptographers consider the following *conjectures* ([15], p. 2-3):

1. There is no polynomial time algorithm that approximates SVP to within polynomial factors.
2. There is no polynomial time *quantum* algorithm that approximates SVP to within polynomial factors.

The above conjectures make cryptography based on the hardness of lattice

problems attractive, especially since the same conjectures cannot be made for cryptography based on traditional number theory such as RSA: A polynomial time quantum algorithm for integer factoring has already been found [23].

Now, we sketch the development of lattice based hash functions in cryptography from 1996 to 2008. Ajtai initiated lattice based cryptography with a groundbreaking result in 1996 [1]. In this paper, Ajtai introduced a family of one way functions of which the security is based on the worst case hardness of n^c -approximate SVP, where $c \in \mathbb{R}_{>0}$. A remarkable property of Ajtai's work is that the security is based on the *worst case hardness* of lattice problems. The meaning of this is that if one succeeds in breaking the security of Ajtai's construction, then one can solve an arbitrary instance of the lattice problem. Regev ([22], p. 2) writes that "this remarkable property is what makes lattice based cryptographic constructions so attractive" and that "virtually all other cryptographic constructions are based on some *average case* assumption".

In Ajtai's paradigm, the central statement is that for numbers $n, m \in \mathbb{Z}_{>0}$, finding short vectors in m -dimensional space on the average is at least as hard as solving lattice problems in n -dimensional space in the worst case. Thereby, the choice of n establishes the security of the construction. It is moreover feasible ([15], p. 8) to choose $m = \Omega(n \log n)$.

In subsequent work, Goldreich et al. improved Ajtai's construction by attaining collision resistant hash functions [7]. Moreover in 2004, Micciancio and Regev achieved a constant c (for the approximation factor n^c) which is essentially 1 [14]. However, the hash functions were still inefficient due to quadratic growth of the key size. To address this problem, Micciancio [13] studied a special class of lattices, so-called cyclic lattices, which are invariant under cyclic rotation of the coordinates. The result was an efficient one way function, which however lacked collision resistance. Efficient collision resistant hash functions were independently provided in 2006 by Peikert and Rosen [20] and Lyubashevsky and Micciancio [10]. A practical instantiation was proposed in form of the SWIFFT hash function in 2008 [11].

In this thesis, we study a paper written by Peikert and Rosen in 2007 [21], where the object of interest is a special class of lattices with number theoretic structure. Using this class of lattices, and following Ajtai's paradigm, the authors obtain a hardness statement for an average case problem. As stated in the paper, the result is of a somewhat theoretic nature, since it is not demonstrated how to derive collision resistant hash functions.

This thesis is ordered as follows.

- In chapter 1, we provide a background in lattices and algebraic number theory.
- In chapter 2, we explain the main result of the paper by Peikert and Rosen [21].
- In chapter 3, we illustrate two additional items which may provide a different viewpoint, and we explain the difficulty of obtaining cryptographic hardness from the special class of lattices which we consider.

In the conclusion, we summarize the effort of the thesis and suggest a further avenue of thought.

1 Preliminaries

In this section, we provide a background in lattices and algebraic number theory. We begin by clarifying the notion of a lattice.

1.1 Lattices

The following material originates from [15] and [22]. Let $m, n \in \mathbb{Z}_{>0}$. Given n linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$, a *lattice* is defined as the set of vectors

$$\mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n) := \left\{ \sum_{i=1}^n x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}.$$

The set of vectors $\mathbf{b}_1, \dots, \mathbf{b}_n$ is called a *basis* of the lattice. A basis must be specified by a matrix $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n] \in \mathbb{R}^{m \times n}$, where the basis vectors form the columns of \mathbf{B} . We write $\mathcal{L}(\mathbf{B})$ as shorthand for $\{\mathbf{B}\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\}$, and we call $\mathcal{L}(\mathbf{B})$ the lattice generated by \mathbf{B} . One of the most studied computational problems for lattices is the Shortest Vector Problem (SVP). Given a lattice basis \mathbf{B} , the objective is to find the shortest nonzero vector in $\mathcal{L}(\mathbf{B})$. The difficulty of this problem arises from the fact that in dimension greater than or equal two, a lattice has infinitely many different bases, and the given lattice basis generally contains very long basis vectors. In practice, one often concentrates on the approximation variant of SVP: Given a lattice basis \mathbf{B} and some approximation factor $\gamma \geq 1$, the objective is to find a nonzero vector in $\mathcal{L}(\mathbf{B})$ with norm less than or equal a γ -multiple of the norm of the shortest nonzero vector in $\mathcal{L}(\mathbf{B})$. A famous polynomial time algorithm for SVP is the *LLL algorithm*, which Lenstra, Lenstra, and Lovász devised in 1982 [9]. If n denotes the dimension of the lattice, then the LLL algorithm attains an approximation factor of $2^{O(n)}$. Although improved algorithms exist ([15], p. 2), no efficient algorithm achieving a polynomial approximation factor has yet been discovered. Similarly, no efficient *quantum* algorithm achieving a polynomial approximation factor has yet been discovered. One may therefore consider the following *conjectures* ([15], p. 2-3):

1. There is no polynomial time algorithm that approximates SVP to within polynomial factors.
2. There is no polynomial time *quantum* algorithm that approximates SVP to within polynomial factors.

The above conjectures make cryptography based on the hardness of lattice problems attractive, especially since the same conjectures cannot be made for cryptography based on traditional number theory such as RSA: A polynomial time quantum algorithm for integer factoring has already been found [23].

Definition 1.1.1. For a lattice basis $\mathbf{B} \in \mathbb{R}^{m \times n}$, we call

$$\mathcal{P}(\mathbf{B}) = \left\{ \sum_{i=1}^n c_i \mathbf{b}_i : c_i \in [0, 1) \right\}$$

the *fundamental region* of \mathbf{B} .

Remark 1.1. Assume that $\mathbf{B}, \mathbf{B}' \in \mathbb{R}^{m \times n}$ are bases of the same lattice, in other words assume that $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{B}') =: \Lambda$. Then if $\text{vol}(\cdot)$ stands for the n -dimensional volume in \mathbb{R}^m , the equality $\text{vol}(\mathcal{P}(\mathbf{B})) = \text{vol}(\mathcal{P}(\mathbf{B}'))$ is true. In other words, the quantity $\text{vol}(\mathcal{P}(\mathbf{B}))$ is invariant over the choice of lattice basis \mathbf{B} , and is dependent only on Λ . We denote the n -dimensional volume $\text{vol}(\mathcal{P}(\mathbf{B}))$ by $\det \Lambda$, and we refer to it as the *fundamental volume* of Λ .

To prepare the next theorem, we clarify two items.

Definition 1.1.2. Let X be a subset of \mathbb{R}^n .

1. The set X is called *convex*, if for all $x, y \in X$ and for all $\lambda \in [0, 1]$, the point $\lambda x + (1 - \lambda)y$ is also contained in X .
2. The set X is called *symmetric*, if for all $x \in X$, the point $-x$ is also contained in X .

The following is a very important result of lattice theory.

Theorem 1.1.3 (Minkowski's Theorem). *Let $\mathcal{L}(\mathbf{B}) \subseteq \mathbb{R}^m$ denote an n -dimensional lattice with basis $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$. Moreover let $C \subseteq \text{span}(\{\mathbf{b}_1, \dots, \mathbf{b}_n\})$ denote a convex, symmetric set with n -dimensional volume greater than $2^n \cdot \det \mathcal{L}(\mathbf{B})$. Then C contains a nonzero lattice point.*

We carry on with a rough overview of pertinent number theoretic material.

1.2 Basic Algebraic Number Theory

In this subsection, we use material which originates from [2], [8], [18] and [21].

Algebraic Numbers

In this part, we rely primarily on [2]. We begin by defining a central concept. Note for the following definition that a *monic polynomial* is a polynomial with highest order coefficient 1, in other words, a polynomial of the form $\sum_{k=0}^{n-1} a_k x^k + x^n$, where $n \in \mathbb{Z}_{>0}$.

Definitions 1.2.1. 1. A number $\alpha \in \mathbb{C}$ is called *algebraic*, if it is a root of a nonzero polynomial with rational coefficients.

2. Given an algebraic number $\alpha \in \mathbb{C}$, the *minimal polynomial* of α is the unique, monic, irreducible polynomial in $\mathbb{Q}[x]$ of minimal degree having α as a root.
3. An *algebraic integer* is an algebraic number for which the minimal polynomial has integer coefficients.

Remark 1.2.2. As an interesting and useful fact, note that the minimal polynomial $f(x) \in \mathbb{Q}[x]$ of an algebraic number $\alpha \in \mathbb{C}$ is a generator of the ideal $\{g \in \mathbb{Q}[x] : g(\alpha) = 0\} \subseteq \mathbb{Q}[x]$.

Examples 1.2.3. 1. The number $\sqrt{2}$ is an algebraic integer with minimal polynomial $x^2 - 2$.

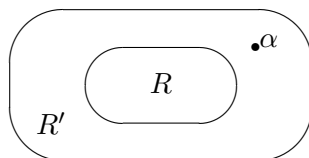
2. The number $\sqrt{2}/3$ is an algebraic number, but not an algebraic integer. The minimal polynomial of $\sqrt{2}/3$ is $x^2 - 2/9$.

To explain the concept of a number field, we need to provide a broader, more abstract background by explaining the practice of adjoining new elements to a ring.

Definitions 1.2.4. Let R' be a ring.

1. A *subring* R of R' is a subset of R' which satisfies the ring axioms: it is closed under addition, subtraction and multiplication, and it contains the unit element of R' . In this constellation, R' is called a *ring extension* of R .
2. Let R be a subring of R' and let $\alpha \in R'$. The smallest subring of R' containing R and α is denoted by $R[\alpha]$, and we call it the ring generated by *adjoining* α to R . Here, we mean “smallest” in the sense of inclusion.

The picture below provides an intuition for Definitions 1.2.4.



For the duration of this paragraph, let R, R' and α be defined as in the previous Definition 1.2.4. Then we remark that, using only the basic ring properties, it can be argued that $R[\alpha]$ consists of all elements of R' which can be written in the form of a sum $r_n\alpha^n + \dots + r_1\alpha + r_0$, where $n \in \mathbb{Z}_{>0}$ and $r_i \in R$ for $i = 0, \dots, n$.

Definition 1.2.5. For $\alpha \in \mathbb{C}$ let $\mathbb{Q}(\alpha) \subseteq \mathbb{C}$ denote the smallest field which contains both \mathbb{Q} and α (where we mean “smallest” in the sense of inclusion). If α is an algebraic number, we call $\mathbb{Q}(\alpha)$ a *number field*. If α is an algebraic integer, we call $\mathbb{Q}(\alpha)$ an *algebraic number field*.

The following theorem sheds light on the structure of a number field.

Theorem 1.2.6. *Let $\alpha \in \mathbb{C}$ be an algebraic number, and let $f(x)$ denote the minimal polynomial of α . Then $\mathbb{Q}[x]/\langle f \rangle$ is isomorphic to $\mathbb{Q}[\alpha] \subseteq \mathbb{C}$. As a consequence, $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.*

Proof. We give an outline of the argumentation. Using the First Isomorphism Theorem for ring homomorphisms, it is possible to argue $\mathbb{Q}[x]/\langle f \rangle \cong \mathbb{Q}[\alpha]$. Since f is irreducible, $\mathbb{Q}[x]/\langle f \rangle$ is a field. The isomorphism yields that also $\mathbb{Q}[\alpha]$ is a field. Since any field which contains \mathbb{Q} and α must also contain $\mathbb{Q}[\alpha]$, it follows by Definition 1.2.5 that $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. \square

We observe that a number field $\mathbb{Q}(\alpha)$ can always be viewed as a vector space over \mathbb{Q} in the following sense. Addition of vectors may be interpreted as addition of elements in $\mathbb{Q}(\alpha)$. The product $c \cdot \beta$ of a scalar $c \in \mathbb{Q}$ and a vector $\beta \in \mathbb{Q}(\alpha)$ may be interpreted as multiplication of elements in $\mathbb{Q}(\alpha)$. In this context, the following definition is immediate.

Definition 1.2.7. Let $\mathbb{Q}(\alpha)$ be a number field. The dimension of $\mathbb{Q}(\alpha)$ as a vector space over \mathbb{Q} is called the *degree* of $\mathbb{Q}(\alpha)$ and is denoted by $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Theorem 1.2.6 provides a hint at how to prove the following result.

Theorem 1.2.8. *Let $\alpha \in \mathbb{C}$ be an algebraic number, and let $f(x) \in \mathbb{Q}[x]$ denote the minimal polynomial of α . Then if $f(x)$ has degree n , the ordered set $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$ is a basis for $\mathbb{Q}(\alpha)$ as a vector space over \mathbb{Q} .*

Corollary 1.2.9. *Let $\alpha \in \mathbb{C}$ be an algebraic number, and let $f(x) \in \mathbb{Q}[x]$ denote the minimal polynomial of α . Then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is the degree of the minimal polynomial $f(x)$.*

The following remarks (see [8]) can be viewed as a summary of items which may be instructive.

- Remarks 1.2.10.*
1. If $f(x) \in \mathbb{Q}[x]$ is monic and irreducible of degree n , then f is the minimal polynomial for each of its n roots.
 2. If $f(x) \in \mathbb{Q}[x]$ is irreducible of degree n , then $f(x)$ does not have repeated roots.
 3. The set of all algebraic numbers forms a field.
 4. The set of all algebraic integers forms a ring.

Canonical Embedding

In this part, we rely primarily on [21]. For the following definition note that for a polynomial in $\mathbb{Q}[x]$, all roots which lie in \mathbb{C}/\mathbb{R} always occur in pairs of complex conjugates.

Definitions 1.2.11. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n , and let $f(x)$ denote the minimal polynomial of α .

1. The other roots $\alpha_2, \dots, \alpha_n \in \mathbb{C}$ of $f(x)$ are called the *conjugates* of $\alpha =: \alpha_1$.
2. Assume that $f(x)$ has r_1 roots which lie in \mathbb{R} and $2r_2$ roots which lie in \mathbb{C}/\mathbb{R} (so $r_1 + 2r_2 = n$). Then the pair (r_1, r_2) is called the *signature* of the number field K .

Now, we recall the definition of structure preserving field mappings.

Definitions 1.2.12. Let K, L denote fields.

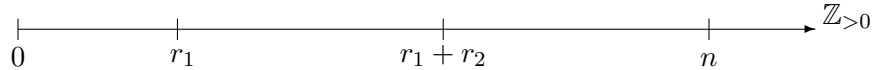
1. A *homomorphism* $\varphi : K \rightarrow L$ is a map which preserves the operations and which maps the unit element of K to the unit element of L . In other words, $\varphi(x +_K y) = \varphi(x) +_L \varphi(y)$, $\varphi(x \cdot_K y) = \varphi(x) \cdot_L \varphi(y)$ and $\varphi(1_L) = 1_K$, for all $x, y \in K$.
2. An *embedding* $\varphi : K \rightarrow L$ is an injective homomorphism.
3. Let $\varphi : K \rightarrow \mathbb{C}$ be an embedding. Then we say that φ is a *real embedding*, if $\varphi(K) \subseteq \mathbb{R}$. Otherwise, φ is called a *complex embedding*.

Theorem 1.2.13. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n . Then there are exactly n distinct embeddings $\sigma_j : K \rightarrow \mathbb{C}$, where $1 \leq j \leq n$.

Remark 1.2.14. Each embedding σ_j of $K = \mathbb{Q}(\alpha)$, where $1 \leq j \leq n$, can be specified as follows. Assume that $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ denote the n complex roots of the minimal polynomial $f(x)$ of α . Let $\theta \in K$ have the representation $\theta = \sum_{i=0}^{n-1} q_i \alpha^i$, where $q_i \in \mathbb{Q}$ for $0 \leq i \leq n-1$. Then $\sigma_j(\theta)$ is given as $\sum_{i=0}^{n-1} q_i \alpha_j^i$.

Next, we establish a rule on how to order the embeddings of a number field.

Convention 1.2.15. If $\zeta, \bar{\zeta} \in \mathbb{C}/\mathbb{R}$ are roots of the minimal polynomial $f(x)$ of an algebraic integer α , then the two embeddings of $K = \mathbb{Q}(\alpha)$ which correspond to ζ and $\bar{\zeta}$ can be viewed as a pair $\sigma, \bar{\sigma}$, where $\bar{\sigma}(x) = \overline{\sigma(x)}$ for all $x \in K$. We let the first r_1 embeddings $\{\sigma_j\}_{j \in [r_1]}$ denote the real embeddings. We number the remaining complex embeddings such that $\sigma_{(r_1+r_2)+j} = \overline{\sigma_{r_1+j}}$ for all $1 \leq j \leq r_2$.



Definition 1.2.16. The *canonical embedding* $\sigma : K \rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ is defined by $\sigma(x) = (\sigma_1(x), \dots, \sigma_n(x))$.

Remarks 1.2.17. 1. The space $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ fulfills the field axioms, if we endow it with component-wise multiplication. Moreover, it is possible to prove the homomorphism properties and injectivity of σ using the homomorphism properties and injectivity of the component functions σ_i , where $1 \leq i \leq n$. This justifies the use of the term “embedding”, which we defined for field homomorphisms.

2. Due to the r_2 pairs of conjugate embeddings, $\sigma(K)$ lies in $H := \{(x_1, \dots, x_n) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : x_{(r_1+r_2)+j} = \overline{x_{r_1+j}} \text{ for all } 1 \leq j \leq r_2\}$. Moreover, especially for volume computations, we may identify \mathbb{C} with \mathbb{R}^2 . In this case, we view H as a corresponding subset of $\mathbb{R}^{r_1} \times \mathbb{R}^{4r_2} = \mathbb{R}^{r_1+4r_2} = \mathbb{R}^{n+2r_2}$.

Using the canonical embedding, it is possible to define geometric norms on K .

Definition 1.2.18. For any $x \in K$ and $p \in [1, \infty]$, we define the l_p length of x as $\|x\|_p = \|\sigma(x)\|_p = (\sum_{i=1}^n |\sigma_i(x)|^p)^{1/p}$ for $p < \infty$, and as $\max\{|\sigma_i(x)| : 1 \leq i \leq n\}$ for $p = \infty$.

Ring of Integers and Geometry

In this part, we rely primarily on [5]. A fundamental concept in number theory is the following.

Definition 1.2.19. Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field. Then we call the set of all algebraic integers contained in K the *ring of integers* in K , and denote it by \mathcal{O}_K . To restate it in formula,

$$\mathcal{O}_K := \{\theta \in K : \theta \text{ is an algebraic integer}\}.$$

It is possible to show that for any algebraic number field K , the subset $\mathcal{O}_K \subseteq K$ fulfills the ring properties. Moreover it is possible to view \mathcal{O}_K as a generalization of the integers \mathbb{Z} ¹. This justifies the fact that \mathcal{O}_K is referred to as the *ring of integers* in K .

Now, we consider ideals of \mathcal{O}_K .

Definitions 1.2.20. Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field of degree n .

1. Let R be a ring, and $\mathcal{I} \subseteq R$. Then \mathcal{I} is called an *ideal*, if it is closed under addition of ideal elements, and closed under multiplication of ideal elements with arbitrary ring elements. In other words, for all $a, b \in \mathcal{I}$, we have $a + b \in \mathcal{I}$, and for all $a \in \mathcal{I}$ and $r \in R$, also $r \cdot a \in \mathcal{I}$.
2. Let $\mathcal{I} \neq \{0\}$ be an ideal in \mathcal{O}_K . Then we say that an ordered set of elements $(b_1, \dots, b_n) \subseteq \mathcal{I}$ is a *basis* for \mathcal{I} , if for any element $\theta \in \mathcal{I}$ there exists a unique representation

$$\theta = z_1 b_1 + \dots + z_n b_n,$$

such that $z_i \in \mathbb{Z}$ for $1 \leq i \leq n$.

¹It is clear that $\mathcal{O}_K \supseteq \mathbb{Z}$ is a ring contained in the field $K \supseteq \mathbb{Q}$, and \mathbb{Z} is a ring contained in the field \mathbb{Q} . It will become more evident in the following that \mathbb{Z} and \mathcal{O}_K may be seen as structurally related. Moreover, the structural similarity could be explained in more detail using the concept of an *order*, a fact that we mention without further deliberation.

3. A basis for the ideal $\mathcal{I} = \mathcal{O}_K$ is called an *integral basis*.

Remarks 1.2.21. Let K denote an algebraic number field of degree n , and let $\mathcal{I} \subseteq \mathcal{O}_K$ be a nonzero ideal.

1. It is possible to show that any such \mathcal{I} has a basis. Therefore in particular, an algebraic number field always has an integral basis.
2. Let $B := (b_1, \dots, b_n) \subseteq \mathcal{I}$ be a basis of \mathcal{I} . Then it is not hard to prove that B is also a basis of K as a vector space over \mathbb{Q} .

We carry on by generalizing the concept of an ideal. The following definition requires the notion of a quotient field. There is a nice explanation of quotient fields in [2], p. 422.

Definition 1.2.22. Let K be an algebraic number field, and let $Q \subseteq K$ denote the quotient field of \mathcal{O}_K . Then a nonempty subset \mathcal{I} of Q is called a *fractional ideal* of \mathcal{O}_K , if the following three conditions are fulfilled.

1. For elements $\theta_1, \theta_2 \in \mathcal{I}$, the sum $\theta_1 + \theta_2$ is contained in \mathcal{I} .
2. For elements $\theta \in \mathcal{I}$ and $\lambda \in \mathcal{O}_K$, the product $\lambda \cdot \theta$ is contained in \mathcal{I} .
3. There exists a nonzero $\gamma \in \mathcal{O}_K$ such that $\gamma \cdot \mathcal{I}$ is a subset of \mathcal{O}_K .

Remarks 1.2.23. 1. Any ideal of \mathcal{O}_K is also a fractional ideal of \mathcal{O}_K : Simply choose $\gamma = 1$ in Definition 1.2.22.

2. We may view the elements of a fractional ideal \mathcal{I} of \mathcal{O}_K as fractions with entries from \mathcal{O}_K and with common denominator γ .
3. Let K be an algebraic number field of degree n . By Remarks 1.2.21, any ideal of \mathcal{O}_K has a basis. It is not hard to show that this property carries over to fractional ideals. In other words, any fractional ideal \mathcal{I} of \mathcal{O}_K contains elements b_1, \dots, b_n such that for any $\alpha \in \mathcal{I}$ there exists a unique representation

$$\alpha = z_1 b_1 + \dots + z_n b_n,$$

such that $z_i \in \mathbb{Z}$ for $1 \leq i \leq n$. Moreover, it can be shown that such a *basis* $B = (b_1, \dots, b_n)$ of a fractional ideal also forms a basis of K as a vector space over \mathbb{Q} .

Next, we need another important concept.

Definition 1.2.24. Let K be an algebraic number field of degree n with signature (r_1, r_2) . Then the *discriminant of n elements* $\theta_1, \dots, \theta_n \in K$ is defined as $D(\theta_1, \dots, \theta_n) = \left(\left| [\sigma(\theta_1), \dots, \sigma(\theta_n)] \right| \right)^2$, where $|\cdot|$ denotes the determinant of a matrix, and the $\sigma(\theta_i) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ are to be viewed as column vectors for $1 \leq i \leq n$.

A useful property of the discriminant of n elements is that it can be used to test linear independence, as stated below.

Lemma 1.2.25. *Let K be an algebraic number field of degree n . Then $\theta_1, \dots, \theta_n \in K$ are linearly independent as elements of K as a vector space over \mathbb{Q} if and only if $D(\theta_1, \dots, \theta_n) \neq 0$.*

Now, we are prepared to argue an important geometric result.

Theorem 1.2.26. *Let K be an algebraic number field of degree n , with signature (r_1, r_2) . Let $B = (b_1, \dots, b_n)$ be a basis of K as a vector space over \mathbb{Q} . Then $\sigma(b_1), \dots, \sigma(b_n)$ are linearly independent vectors in $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ and \mathbb{R}^{n+2r_2} , where linear independence is to be understood with respect to scalars from \mathbb{R} .*

Proof. We give a lax description of the argumentation. As a notational convention, let $\sigma_{\mathbb{C}}(b_i)$ denote the vector in $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$, and let $\sigma_{\mathbb{R}}(b_i)$ be the corresponding vector in \mathbb{R}^{n+2r_2} , obtained by identifying \mathbb{C} with \mathbb{R}^2 . Assume there exist scalars $\lambda_i \in \mathbb{R}$ for $1 \leq i \leq n$ such that

$$\sum_{i=1}^n \lambda_i \sigma_{\mathbb{R}}(b_i) = \mathbf{0}. \quad (1)$$

It is not hard to see that equation 1 is equivalent to $\sum_{i=1}^n \lambda_i \sigma_{\mathbb{C}}(b_i) = \mathbf{0}$. Therefore $0 = \left| [\sigma_{\mathbb{C}}(b_1), \dots, \sigma_{\mathbb{C}}(b_n)] \right|$, where $|\cdot|$ denotes the determinant of a matrix. As a consequence, $D(b_1, \dots, b_n) = 0$, which according to Lemma 1.2.25 contradicts the linear independence of the integral basis (b_1, \dots, b_n) of K . \square

For the next corollary, note that a sublattice Λ' of a lattice Λ is simply a lattice such that $\Lambda' \subseteq \Lambda$.

Corollary 1.2.27. *Let K be an algebraic number field of degree n , with signature (r_1, r_2) . Then the following statements are true.*

1. *The ring of integers \mathcal{O}_K embeds as an n -dimensional lattice $\sigma(\mathcal{O}_K)$ in $\mathbb{R}^{n+2r_2} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$.*
2. *Any ideal \mathcal{I} of \mathcal{O}_K embeds as an n -dimensional sublattice $\sigma(\mathcal{I})$ of $\sigma(\mathcal{O}_K)$ in $\mathbb{R}^{n+2r_2} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$.*
3. *Any fractional ideal \mathcal{I} of \mathcal{O}_K embeds as an n -dimensional lattice $\sigma(\mathcal{I})$ in $\mathbb{R}^{n+2r_2} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$.*

Remark 1.2.28. Note from the above Corollary that we identify \mathbb{C} with \mathbb{R}^2 when considering lattices in complex-valued geometric space. In the following, this identification will be implicitly assumed, but no longer mentioned.

Finally, we require two more concepts.

Definition 1.2.29. Let K be an algebraic number field of degree n with signature (r_1, r_2) . Then the squared fundamental volume $(\det(\sigma(\mathcal{O}_K)))^2$ of the n -dimensional lattice $\sigma(\mathcal{O}_K) \in \mathbb{R}^{n+2r_2}$ is called the *absolute discriminant* of K and is denoted by Δ_K . The *root discriminant* of K is defined as $\Delta_K^{1/n}$ and is denoted by \mathcal{D}_K .

Remark 1.2.30. For an algebraic number field K , the constant \mathcal{D}_K offers a geometric intuition. Namely, the smaller \mathcal{D}_K is, the denser the elements of \mathcal{O}_K lie when embedded as a lattice in geometric space.

Example 1.2.31. We give a simple example of how the ring of integers \mathcal{O}_K of an algebraic number field K of degree n with signature (r_1, r_2) embeds as an n -dimensional lattice $\sigma(\mathcal{O}_K)$ in \mathbb{R}^{n+2r_2} . We follow an example on ideal bases given in [5], p. 134-135, where more detailed explanations can be found. Figure 1 illustrates the example. Consider $K = \mathbb{Q}(\sqrt{7})$. The minimal polynomial of $\sqrt{7} =: \alpha$ is given as $x^2 - 7 = (x - \sqrt{7})(x + \sqrt{7})$, with roots $\alpha_1 := \sqrt{7} = \alpha$ and $\alpha_2 := -\sqrt{7}$. As a consequence, the signature of K is $(r_1, r_2) = (2, 0)$. Hence for $\theta = q_1 + q_2\alpha \in \mathcal{O}_K$, where $q_1, q_2 \in \mathbb{Q}$, the canonical embedding $\sigma : K \rightarrow \mathbb{R}^{r_1+2r_2} = \mathbb{R}^2$ is defined by the component functions

$$\begin{aligned}\sigma_1(\theta) &= \sigma_1(q_1 + q_2\alpha) = \sigma_1(q_1 + q_2\sqrt{7}) = q_1 + q_2\alpha_1 = q_1 + q_2\sqrt{7}, \text{ and} \\ \sigma_2(\theta) &= \sigma_2(q_1 + q_2\alpha) = \sigma_2(q_1 + q_2\sqrt{7}) = q_1 + q_2\alpha_2 = q_1 - q_2\sqrt{7}.\end{aligned}$$

It is possible to argue that $(1, \sqrt{7})$ forms an integral basis of \mathcal{O}_K , in other words, $\mathcal{O}_K = \mathbb{Z} + \sqrt{7}\mathbb{Z} = \{z_1 + \sqrt{7}z_2 : z_1, z_2 \in \mathbb{Z}\}$. The basis elements embed as $\sigma(1) = (1, 1) =: \mathbf{a}$ and $\sigma(\sqrt{7}) = (\sqrt{7}, -\sqrt{7}) =: \mathbf{b}$. Now consider the ideal $\mathcal{I} = \{r \cdot (2 + \sqrt{7}) : r \in \mathcal{O}_K\} \subseteq \mathcal{O}_K$. It is possible to argue that $(3, 2 + \sqrt{7})$ forms a basis of \mathcal{I} , in other words, $\mathcal{I} = 3\mathbb{Z} + (2 + \sqrt{7})\mathbb{Z} = \{3z_1 + (2 + \sqrt{7})z_2 : z_1, z_2 \in \mathbb{Z}\}$. The basis elements embed as $\sigma(3) = (3, 3) =: \mathbf{c}$ and $\sigma(2 + \sqrt{7}) = (2 + \sqrt{7}, 2 - \sqrt{7}) =: \mathbf{d}$. To compute the fundamental volume $\det(\sigma(\mathcal{O}_K))$, we take the absolute value of the determinant of the matrix $\begin{pmatrix} 1 & \sqrt{7} \\ 1 & -\sqrt{7} \end{pmatrix}$, which yields $2\sqrt{7}$. The absolute discriminant Δ_K therefore equals the squared fundamental volume $(\det(\sigma(\mathcal{O}_K)))^2 = 28$, and the root discriminant of K is given as $\mathcal{D}_K = \Delta_K^{\frac{1}{n}} = \Delta_K^{\frac{1}{2}} = 2\sqrt{7}$.

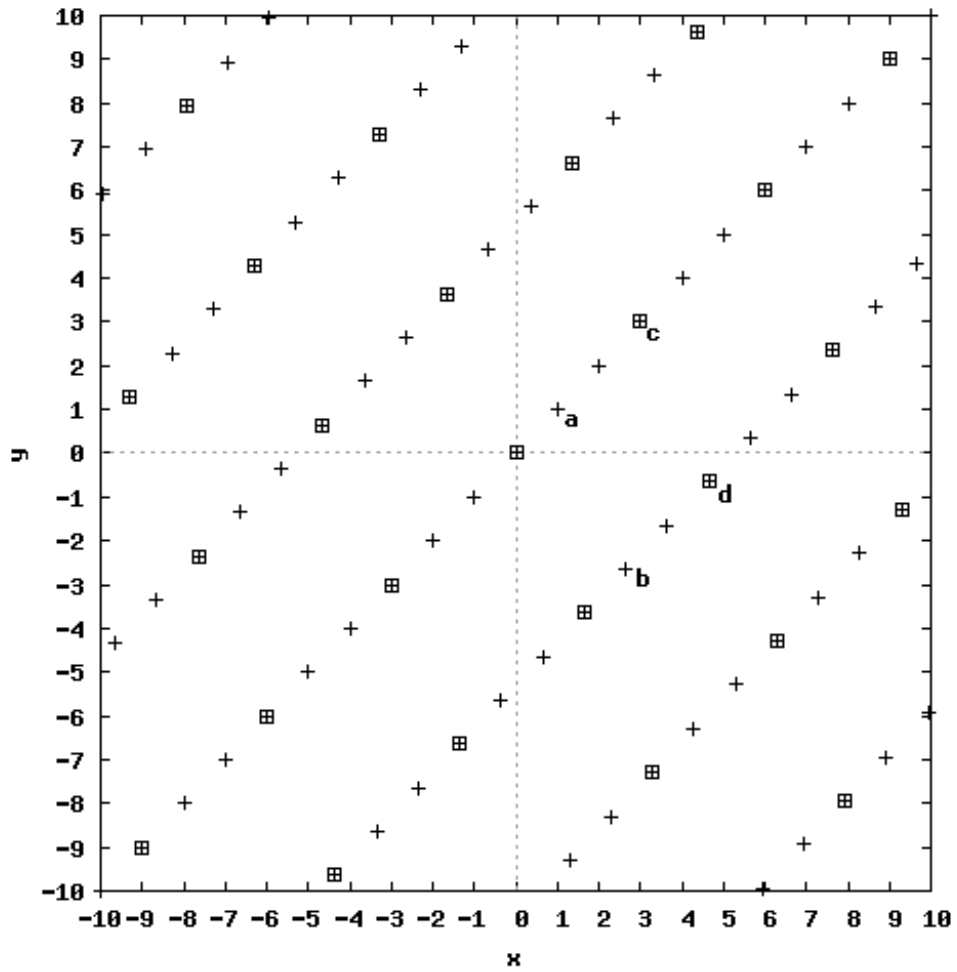


Figure 1: Embedded ring of integers \mathcal{O}_K and ideal $\mathcal{I} = \{r \cdot (2 + \sqrt{7}) : r \in \mathcal{O}_K\}$ of the algebraic number field $K = \mathbb{Q}(\sqrt{7})$. The crosses are the elements of \mathcal{O}_K . If an element is also contained in \mathcal{I} , the cross is framed by a rectangle.

2 A Worst-Case to Average-Case Lattice Problem Reduction with a Logarithmic Connection Factor

In this section, we explain the results established in the paper entitled “Lattices that admit Logarithmic Worst-Case to Average-Case Connection Factors”, by Peikert and Rosen [21].

Structure. In subsection 2.1, we begin by clarifying some notation. In subsection 2.2, we briefly summarize the content of the paper. Subsection 2.3 sheds light on the larger cryptographic context of the result which is demonstrated in the paper. Finally, subsection 2.4 provides a more detailed account of the arguments.

2.1 Notation

We use the following notation.

- For $n \in \mathbb{Z}_{>0}$, let $[n]$ denote the set $\{1, \dots, n\}$.
- We write $\text{poly}(\cdot)$ for some unspecified polynomial function in its parameter.
- We call a function $\nu : \mathbb{Z}_{>0} \rightarrow \mathbb{R}$ *negligible*, if for every positive polynomial p there exists an $n_0 \in \mathbb{Z}_{>0}$ such that $\nu(n) < 1/p(n)$ for all $n > n_0$ ([6], p. 16). Hence a negligible function is one that decreases faster than the reciprocal of any polynomial in n .
- A *non-negligible* function is a function which is not negligible.
- We say that a sequence of events $\{A_n\}_{n \in \mathbb{Z}_{>0}}$ occurs with *overwhelming probability*, if there exists a negligible function $g : \mathbb{Z}_{>0} \rightarrow [0, 1]$ such that $P(A_n) = 1 - g(n)$, where $n \in \mathbb{Z}_{>0}$.
- Let K be an algebraic number field with integral basis B . Consider an element $w \in K$ having representation $w = \sum_{i \in [n]} c_i b_i$ with respect to B , where $c_i \in \mathbb{Q}$ for $i \in [n]$. For $q \in \mathbb{Q}$, let $\lfloor q \rfloor \in \mathbb{Z}_{>0}$ denote the integer nearest to q . Then we define $\lfloor w \rfloor_B := \sum_{i \in [n]} \lfloor c_i \rfloor b_i$. Intuitively, $\lfloor w \rfloor_B$ can be viewed as an algebraic integer of K which lies nearby w ([21], p. 23).
- Given a lattice Λ , the *smoothing parameter* $\eta_\epsilon(\Lambda)$ denotes a certain probabilistic lattice quantity (see [21], p. 10).
- Given a lattice Λ , the *minimum distance* in l_p length is defined as $\lambda_1^p(\Lambda) = \min_{x \in \Lambda, x \neq \mathbf{0}} \|x\|_p$. For an ideal \mathcal{I} of the ring of integers \mathcal{O}_K of an algebraic number field K , the quantity $\lambda_1^p(\mathcal{I})$ is defined as $\lambda_1^p(\sigma(\mathcal{I}))$.
- Given an algebraic number field K , real $s > 0$ and $x \in K$, we define the *continuous Gaussian probability distribution* over K as $D_s^K(x) = s^{-n} \cdot \rho_s(x)$, where $\rho_s(x)$ denotes the Gaussian function $\exp(-\pi \|x\|^2 / s^2)$, see [21], p. 9,13.

- For any $x \in \mathbb{R}_{>0}$, let $x^{1/\infty} := 1$.

2.2 Overview

This subsection summarizes the content of the paper [21]. Note that proper definitions and further explanations are given in 2.4.

The main result of the paper is a hardness statement for an average-case problem, which is proved by a reduction from the worst-case problem of finding $\gamma(n)$ -approximate shortest vectors in special n -dimensional lattices. The result is remarkable, since $\gamma(n)$ has size $O(\sqrt{\log n})$ and the previously best known size for such a connection factor was $\tilde{O}(n)$. Observe that a smaller connection factor enhances the result, since it signifies that the reduction in the paper could be seen as solving a harder problem ([21], p. 4).

Notably, the main result is obtained by using families of lattices that correspond to ideals in the ring of integers of an algebraic number field. The authors utilize families of algebraic number fields for which the existence is guaranteed; an efficient method of construction however remains unknown.

2.3 Cryptographic Background

In this subsection, our aim is to set the stage for the main result by explaining the cryptographic terminology. We begin by clarifying the purpose of reductions.

Reductions. This paragraph is based on [6], p. 23. Consider the following situation. Given a computational problem A , assume our goal is to make a statement regarding the hardness of A . Further, let B denote a computational problem that is thought to be intractable.

Then a polynomial-time reduction of problem B to problem A allows us to make a statement regarding the hardness of A . Namely, in case of such a reduction A *is at least as hard as* B , since if A can be solved in polynomial time, then due to the reduction, B can be solved in polynomial time. Naturally, such a hardness statement hinges on the intractability of B : The advent of an efficient algorithm to solve B renders the result useless for cryptographic purposes. Hence problems assumed to be intractable must be carefully chosen.

Example. Retaining the above notation, problem A might be the breaking of an encryption scheme (such as RSA), and B the problem of integer factorization. Then based on the assumed intractability of integer factorization, a polynomial-time reduction from B to A would demonstrate a certain level of security of the encryption scheme. Note that in the case of RSA, such a result has not entirely been established yet.

Furthermore, Goldreich (see [6], p. 50) distinguishes between two types of reduction. Assume as above that we want to reduce the task of solving B to the task of solving A. Consider the following cases.

1. *Standard reduction*: We presuppose the existence of an algorithm \mathcal{F} which solves A on any instance (we say that \mathcal{F} solves A *on the worst case*).²
2. *Reducibility argument*: We presuppose the existence of an algorithm which solves A with certain probability with respect to a given distribution on the set of instances.

Remark 2.1. The second type of reduction, the reducibility argument, gives rise to an added complexity: Assume that \mathcal{F} is the algorithm postulated to solve A with certain probability. Moreover, let \mathcal{R} denote the reduction. Generally, \mathcal{F} will receive inputs with probability according to a distribution engendered by \mathcal{R} . Therefore, it is an added difficulty to determine the success probability of \mathcal{F} in the reduction, and it typically involves examining the “distance” between distributions.

The next paragraph restates a remark in [6] (p. 20) on the significance of average-case problems in cryptography.

Average-case Problems. Average-case problems are of eminent importance in cryptography, since a cryptographic scheme must be unbreakable for most, for typical cases. The problem of breaking a cryptographic scheme must be hard on the average. This motivates the main result of the paper, which is a hardness statement for an average-case problem.

2.4 Main Result

Structure. This subsection is divided into two parts. The first part (2.4.1) provides the definitions and facts necessary to establish a suitable setting, as well as the main result as an isolated theorem. The second part (2.4.2) sheds light on the main steps and the structure of the proof.

2.4.1 Setting and Main Result

We begin by determining appropriate computational problems between which we later construct reductions. We follow the presentation in [21] (p. 19, 20).

²The algorithm \mathcal{F} is also referred to as an *oracle*. Moreover, following the terminology of Goldreich [6], the reduction itself is called an *oracle machine*. As Goldreich ([6], p. 20) writes, the concept of an oracle machine was first devised to study notions of reducibility. In this context, consider an interesting paragraph in [19], p. 339, where *Turing machines with oracle* are introduced in order to capture how known problems could be approached in an “alternative universe”, where certain computation is “free”.

Computational Problems. For simplicity, the problems are first defined on fixed algebraic number fields. Afterwards we introduce a natural generalization to families of algebraic number fields.

Definitions 2.2. Let K be an algebraic number field, and $\phi : K \rightarrow \mathbb{R}$ a function. Then fix the following terminology:

1. K -IGVP $_{\gamma}^{p,\phi}$ stands for the **I**deal **G**eneralized **V**ector **P**roblem:
Let $p \in [1, \infty]$, and let $\gamma \in \mathbb{R}, \gamma > 0$. An input to K -IGVP $_{\gamma}^{p,\phi}$ is an ideal $\mathcal{I} \subseteq \mathcal{O}_K$. The goal is to output a nonzero $x \in \mathcal{I}$ such that $\|x\|_p \leq \gamma \cdot \phi(\mathcal{I})$.
2. K -ISVP $_{\gamma}^p$ stands for the the **I**deal **S**hortest **V**ector **P**roblem:
This is the special case of K -IGVP $_{\gamma}^{p,\phi}$, where $\phi = \lambda_1^p$.
3. K -SAIS $_{q,m,\beta}^r$ stands for the **S**hort **A**lgebraic **I**nteger **S**olution problem:
Let $q, m \in \mathbb{Z}_{>0}$, and let $\beta \in \mathbb{R}_{>0}$, and $r \in [1, \infty]$. Then an input to K -SAIS $_{q,m,\beta}^r$ is a vector $\mathbf{a} \in \mathcal{O}_K^m$. The goal is to output nonzero $\mathbf{z} \in \Psi_q^K(\mathbf{a}) := \left\{ \mathbf{z} \in \mathcal{O}_K^m : \sum_{j \in [m]} a_j z_j \in \langle q \rangle \right\}$ such that $\|\mathbf{z}\|_r \leq \beta \cdot (mn)^{1/r}$.

The following definition establishes a structure which allows to capture a certain type of asymptotic hardness.

Definition. Let $T \subseteq \mathbb{Z}_{>0}$ be an infinite set. Then an *infinite family of algebraic number fields* \mathcal{K} is a parameterized set $\{K_n\}_{n \in T}$, such that K_n has degree n .

Now, we generalize the problems introduced in Definition 2.2 to infinite families of algebraic number fields.

Definitions 2.3. Let \mathcal{K} be an infinite family of algebraic number fields.

1. Let $p \in [1, \infty]$, and let $\gamma : \mathbb{Z}_{>0} \rightarrow \mathbb{R}_{>0}$. Then define \mathcal{K} -IGVP $_{\gamma}^{p,\phi}$ as the ensemble of instances from $\left\{ K_n\text{-IGVP}_{\gamma(n)}^{p,\phi} : n \in \mathbb{Z}_{>0} \right\}$.
2. Let $r \in [1, \infty]$, and let $q : \mathbb{Z}_{>0} \rightarrow \mathbb{Z}_{>0}$, and also $m : \mathbb{Z}_{>0} \rightarrow \mathbb{Z}_{>0}$. Moreover fix $\beta : \mathbb{Z}_{>0} \rightarrow \mathbb{R}_{>0}$. Then define \mathcal{K} -SAIS $_{q,m,\beta}^r$ as the ensemble of instances from $\left\{ K_n\text{-SAIS}_{q(n),m(n),\beta(n)}^r : n \in \mathbb{Z}_{>0} \right\}$.

The introduction of problems defined on families of algebraic number fields raises questions on the exact nature of the reductions we aspire to formulate. The next paragraph addresses these questions.

Reductions between Families of Algebraic Number Fields. First, consider issues pertaining to the *representation of algebraic number fields* and *algorithm complexity*. By convention, an algebraic number field K is represented by an integral basis B . Furthermore, given an algorithm that performs operations on an algebraic number field K of degree n , *polynomial*

run time is taken to mean that the number of operations carried out is bounded above by some polynomial in both n and $\log(\Delta_K)$.

Moreover, all computational problems defined on algebraic number fields must be viewed under the condition of *preprocessing*. This means that any algorithm may appeal to a polynomial-length (in the representation of K) auxiliary input containing arbitrary information on K (see [21], p. 19).

Example. The auxiliary input needed by a reduction on an algebraic number field K might be an integral basis that is as short as possible in l_∞ length. This means that for an integral basis $B = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ of K , the value $\max\{\|\mathbf{b}_i\|_\infty : 1 \leq i \leq n\}$ is smaller than or equal the corresponding value for any other integral basis B' of K .

Finally, we define an essential property of reductions on problems involving families of algebraic number fields ([21], p. 20).

Definition. Let P and P' be computational problems defined for fixed algebraic number fields, and let \mathcal{K} denote an infinite family of algebraic number fields. Suppose further that $\mathcal{K}\text{-}\mathsf{P}$ as well as $\mathcal{K}\text{-}\mathsf{P}'$ stand for the respective problem generalizations, analogous to Definitions 2.3. Then a reduction from $\mathcal{K}\text{-}\mathsf{P}$ to $\mathcal{K}\text{-}\mathsf{P}'$ is called *number field-preserving* if, given an input instance of the problem $K_n\text{-}\mathsf{P}$, the reduction algorithm only makes requests for solutions on instances of the problem $K_n\text{-}\mathsf{P}'$.

Before we carry on, we gain an understanding of average-case problems in the context of families of algebraic number fields \mathcal{K} . Specifically, consider $\mathcal{K}\text{-SAIS}_{q,m,\beta}^r$.

Definition 2.4. Let $\mu : \mathbb{Z}_{>0} \rightarrow [0, 1]$ be a non-negligible function. Then we say that an algorithm \mathcal{A} solves $\mathcal{K}\text{-SAIS}_{q,m,\beta}^r$ *on the average with non-negligible probability*, if for any $n \in \mathbb{Z}_{>0}$, \mathcal{A} solves $K_n\text{-SAIS}_{q(n),m(n),\beta(n)}^r$ with probability $\mu(n)$ on input $\mathbf{a} = (a_1, \dots, a_{m(n)})$, where the a_i are random components which are chosen uniformly and independently from a predetermined set of representatives of $\mathcal{O}_{K_n}/\langle q(n) \rangle$.

Now we are able to state the main theorem, which is given as Corollary 9.8 in [21], p. 27.

Theorem 2.5 (Main Theorem). *There exists an infinite family $\mathcal{K} = \{K_n\}$ of algebraic number fields such that for any $p \in [1, \infty)$ and any $m(n) = \Theta(\log n)$, there exist parameters*

$$q(n) = O(n \log^{1.5} n), \quad \beta = O(1), \quad \gamma(n) = O(\sqrt{\log n})$$

as functions of n for which solving $\mathcal{K}\text{-SAIS}_{q,m,\beta}^\infty$ on the average with non-negligible probability is at least as hard as solving $\mathcal{K}\text{-ISVP}_\gamma^p$ in the worst case.

For $p = \infty$, there exists $\gamma(n) = O(\log n)$ for which the same claim applies.

2.4.2 Proof Overview

We carry on by depicting the essential features of the proof of the above Main Theorem 2.5 (the proof is in [21], p. 23-27). For the proof, an additional problem on ideal lattices is defined, which is derived from $K\text{-IGVP}_\gamma^{p,\eta_\epsilon}$ (see [21], p. 19).

Definition 2.6. Let K be a fixed algebraic number field. Then $K\text{-InclIGVP}_\gamma^{p,\phi}$ denotes an incremental version of IGVP: Let $p \in [1, \infty]$ and $\gamma \in \mathbb{R}_{>0}$. Then an input to $K\text{-InclIGVP}_\gamma^{p,\phi}$ is a pair (\mathcal{I}, x) , such that $\mathcal{I} \subseteq \mathcal{O}_K$ is an ideal and the element $x \in \mathcal{I}$ satisfies $\|x\|_p > \gamma \cdot \phi(\mathcal{I})$. The goal is to output a nonzero $x' \in \mathcal{I}$ such that $\|x'\|_p \leq \|x\|_p/2$.

Concretely, we consider $K\text{-InclIGVP}_\gamma^{p,\phi}$ for the case $\phi = \eta_\epsilon$. It is worth mentioning a few facts in this regard.

- Remarks 2.7.*
1. There is a straightforward polynomial-time standard reduction from $K\text{-IGVP}_\gamma^{p,\eta_\epsilon}$ to $K\text{-InclIGVP}_\gamma^{p,\eta_\epsilon}$ ([21], p. 19).
 2. Note that $K\text{-InclIGVP}_\gamma^{p,\eta_\epsilon}$ is the worst-case problem which we actually reduce to the average-case problem (Theorem 2.8 below). The aim of introducing this incremental problem is to facilitate the worst-case to average-case reduction that needs to be performed to prove the Main Theorem 2.5.

Generalizing the problems of Definition 2.6 to problems on infinite families of algebraic number fields works analogous to Definition 2.3. Hence for example, $\mathcal{K}\text{-IGVP}_\gamma^{p,\eta_\epsilon}$ denotes a corresponding ensemble of instances for a family of algebraic number fields $\mathcal{K} = \{K_n\}_{n \in T}$, where γ and η_ϵ are functions of n .

The following theorem (see [21], p. 23) bears the main burden of the workload involved in proving the main result.

Theorem 2.8. *Let \mathcal{K} be an infinite family of algebraic number fields, $p \in [1, \infty]$, and let $m(n), q(n), \beta(n) = \text{poly}(n)$ and $\gamma(n)$ satisfy the following conditions:*

1. *For $p \in [1, \infty)$, $\gamma(n) \geq c_p \cdot \beta(n) \cdot \sqrt{m(n)} \cdot n^{1/p}$, where c_p depends only on p ;*
For $p = \infty$, $\gamma(n) \geq c_\infty \cdot \beta(n) \cdot \sqrt{m(n)} \cdot \sqrt{\log n}$, where c_∞ is a universal constant.
2. *$q(n) \geq 2 \cdot \beta(n) \cdot m(n) \cdot n \cdot g^\infty(\mathcal{O}_{K_n})$.*

Then there is a polynomial-time number field-preserving reduction from solving $\mathcal{K}\text{-InclIGVP}_\gamma^{p,\eta_\epsilon}$ in the worst case to solving $\mathcal{K}\text{-SAIS}_{q,m,\beta}^\infty$ on the average with non-negligible probability.

With the aim of avoiding too much technical detail, we provide a rough but comprehensive sketch of the proof (see [21], p. 23-26).

Proof Outline (of Theorem 2.8). According to the terminology introduced in 2.3, the proof is a reducibility argument. Hence we presuppose an algorithm \mathcal{F} which solves $\mathcal{K}\text{-SAIS}_{q,m,\beta}^\infty$ on the average with non-negligible probability. Using \mathcal{F} , we design a reduction algorithm \mathcal{R} solving $\mathcal{K}\text{-InclGVP}_{\gamma}^{p,\eta_\epsilon}$.

Note that the input to \mathcal{R} is an algebraic number field $K_n \in \mathcal{K}$ for some fixed $n \in \mathbb{Z}_{>0}$, as well as a pair (\mathcal{I}, x) , where \mathcal{I} is an ideal of \mathcal{O}_{K_n} and $x \in \mathcal{I}$ such that $\|x\|_p > \gamma(n) \cdot \eta_\epsilon(\mathcal{I})$. For ease of notation, let $K := K_n$, $\gamma := \gamma(n)$ and $q := q(n)$. The reduction algorithm \mathcal{R} is given as follows:

1. For $j = 1, \dots, m$ carry out the following steps:
 - Sample a uniform $v_j \in \mathcal{I}/\langle x \rangle$.
 - Sample $y_j \sim D_s^K$, where $s = 2\|x\|_p/\gamma \geq 2\eta_\epsilon(\mathcal{I})$. Set $y'_j = y_j \bmod \mathcal{I}$.
 - Let $w_j = qx^{-1}(v_j + y'_j) \bmod \langle q \rangle$. Further, let $a_j = \lfloor w_j \rfloor_B \bmod \langle q \rangle$.
2. Let $\mathbf{a} = (a_1, \dots, a_m)$ and let $\mathbf{z} = (z_1, \dots, z_m) \leftarrow \mathcal{F}(\mathbf{a})$. Finally, output

$$x' = \sum_{j \in [m]} \left(\frac{x(w_j - \lfloor w_j \rfloor_B)}{q} - y_j \right) \cdot z_j.$$

To demonstrate the correctness of \mathcal{R} , the authors prove a succession of auxiliary claims which in their entirety establish the result. We list these claims in the following, and subsequently we explain how the result follows by combination of these claims.

1. The probability that $\mathbf{z} \in \Psi_q^K(\mathbf{a})$ is non-negligible in n .
2. If $\mathbf{z} \in \Psi_q^K(\mathbf{a})$, then $x' \in \mathcal{I}$.
3. Conditioned on $\mathbf{z} \in \Psi_q^K(\mathbf{a})$, one has $\|x'\|_p \leq \frac{\|x\|_p}{2}$ with probability at least $1/2$.
4. Conditioned on $\mathbf{z} \in \Psi_q^K(\mathbf{a})$, it holds that $x' \neq 0$ with overwhelming probability.

Note that assertion 1 addresses the complication which we mention in Remark 2.1. By assumption, \mathcal{F} solves $\mathcal{K}\text{-SAIS}_{q,m,\beta}^\infty$ on the average with non-negligible probability. By Definition 2.4, this means that \mathbf{z} is contained in $\Psi_q^K(\mathbf{a})$ with non-negligible probability if the a_i are sampled independently and uniformly. Therefore it must be demonstrated that the reduction samples the a_i according to a distribution that is sufficiently close to an independent and uniform distribution over a canonical set of residues representing $\mathcal{O}_K/\langle q \rangle$.

Now we clarify that claims 1 to 4 establish the result. For ease of notation, we introduce a few names for probabilistic events:

- Let A denote the event $[\mathbf{z} \in \Psi_q^K(\mathbf{a})]$,

- let B denote the event $\left[\|x'\|_p \leq \frac{\|x\|_p}{2}\right]$,
- and let C denote the event $[x' \neq 0]$.

Moreover let P_A denote the probability conditioned on A .

We begin by arguing that claims 1 to 4 imply that the success probability of \mathcal{R} is non-negligible. Observe that to prove that \mathcal{R} solves $\mathcal{K}\text{-InclGVP}_{\gamma}^{P,\eta\epsilon}$ with non-negligible probability, it suffices to show that $P(A \cap B \cap C)$ is non-negligible (also because claim 2 ensures that $x' \in \mathcal{I}$, if the event A is fulfilled). This result can be proved in two steps.

First, we establish $P_A(B \cap C) \geq \frac{1}{2} - \nu(n)$, where $\nu(n) : \mathbb{Z}_{>0} \rightarrow \mathbb{R}_{\geq 0}$ is a negligible function. To show this inequality, check that $P_A(B \cap C) \geq 1 - P_A(\overline{B}) - P_A(\overline{C})$. Assertion 3 and 4 yield that $P_A(\overline{B}) \leq \frac{1}{2}$ and $P_A(\overline{C}) = \nu(n)$, for a negligible function $\nu : \mathbb{Z}_{>0} \rightarrow \mathbb{R}_{\geq 0}$. Hence $P_A(B \cap C) \geq \frac{1}{2} - \nu(n)$.

As the second step, recall $P_A(B \cap C) = \frac{P(A \cap B \cap C)}{P(A)}$. Hence to prove that $P(A \cap B \cap C)$ is non-negligible, consider $P_A(B \cap C) \cdot P(A)$. Assertion 1 provides that $P(A)$ is non-negligible and by the first step of our argumentation, we can reason that $P_A(B \cap C)$ is sufficiently bounded in order to not violate the non-negligibility. Namely, by the first step of our argumentation, $P_A(B \cap C) \geq \frac{1}{2} - \nu(n)$, where ν is a negligible function. Since $\nu(n) \rightarrow 0$ for $n \rightarrow \infty$, certainly $P_A(B \cap C) \geq \frac{1}{4}$ for large n . Hence we have $P_A(B \cap C) \cdot P(A) \geq \frac{1}{4}P(A)$ for large n . If $P(A) =: \alpha(n)$, where α is non-negligible, it remains to argue that $\frac{1}{4}\alpha$ is non-negligible. By definition of non-negligibility, there exists a positive polynomial p_α such that $\alpha(n) \geq \frac{1}{p_\alpha(n)}$ for infinitely many $n \in \mathbb{Z}_{>0}$. Then obviously $\frac{1}{4}\alpha(n) \geq \frac{1}{4p_\alpha(n)}$ for infinitely many $n \in \mathbb{Z}_{>0}$, which establishes the argument.

All in all therefore claims 1 through 4 establish that \mathcal{R} solves $\mathcal{K}\text{-InclGVP}_{\gamma}^{P,\eta\epsilon}$ with non-negligible probability.

If the procedure happens to fail, we simply repeat it. By such repetition, the probability of success for any given n can be amplified to overwhelming probability. To see this, let $\mu(n)$ denote the success probability of \mathcal{R} for $n \in \mathbb{Z}_{>0}$. Then the probability for success after k independent runs of the algorithm is $1 - (1 - \mu(n))^k$. Obviously, we achieve overwhelming probability for k large enough, since $(1 - \mu(n)) < 1$ implies $(1 - \mu(n))^k \rightarrow 0$ for $k \rightarrow 0$.

Moreover, at least for infinitely many $n \in \mathbb{Z}_{>0}$, it suffices to repeat the algorithm polynomially many times in order to achieve overwhelming probability. To argue this point, we proceed as follows. Surely in order to argue overwhelming probability, it suffices to find $k = k(n)$ for which $((1 - \mu(n))^k = 2^{-n})$. Hence $k = \frac{\log(2) \cdot (-n)}{\log(1 - \mu(n))} = \frac{C \cdot n}{-\log(1 - \mu(n))}$, where we replaced

$\log(2)$ by C . Now recall that for all $x \in \mathbb{R}_{>0}$, the inequality $\log(x) \leq x - 1$ transforms to $-\log(x) \geq 1 - x$. This yields $k \leq \frac{C \cdot n}{1 - (1 - \mu(n))} = \frac{C \cdot n}{\mu(n)}$. Since $\mu(n)$ is non-negligible, there exists a positive polynomial p such that $\mu(n) \geq \frac{1}{p(n)}$ for infinitely many $n \in \mathbb{Z}_{>0}$. As a consequence, k is bounded above by $C \cdot n \cdot p(n)$ for infinitely many $n \in \mathbb{Z}_{>0}$, where this upper bound obviously constitutes a polynomial. \square

Remark. By Remark 2.7, item 1, and Theorem 2.8, it follows that there is a polynomial-time number field-preserving reduction from solving \mathcal{K} -IGVP $_{\gamma}^{p, \eta \epsilon}$ in the worst case to solving \mathcal{K} -SAIS $_{q, m, \beta}^{\infty}$ on the average with non-negligible probability.

The following theorem (see [21], p. 26) establishes the main result. The following theorem is proved using Theorem 2.8 and other results from [21].

Theorem 2.9. *For $p \in [1, \infty)$, any $m(n) = \Theta(\log n)$ and for any family of algebraic number fields $\mathcal{K} = \{K_n\}$ such that $\mathcal{D}_{K_n} = \text{poly}(n)$, there exist*

$$q(n) = O(n \cdot \log^{1.5} n) \cdot \mathcal{D}_{K_n}, \quad \beta(n) = O(1) \cdot \sqrt{\mathcal{D}_{K_n}}, \quad \gamma(n) = O(\sqrt{\log n}) \cdot \mathcal{D}_{K_n}^{1.5}$$

such that there is a polynomial-time number field-preserving reduction from solving \mathcal{K} -ISVP $_{\gamma}^p$ in the worst case to solving \mathcal{K} -SAIS $_{q, m, \beta}^{\infty}$ on the average with non-negligible probability.

For $p = \infty$, there exists $\gamma(n) = O(\log n) \cdot \mathcal{D}_{K_n}^{1.5}$ for which the same applies.

The main result follows from Theorem 2.9, since by the theory of infinite towers of Hilbert class fields (see [21], p. 27), there exists an infinite family of algebraic number fields $\mathcal{K} = \{K_n\}$ such that $\limsup_{n \rightarrow \infty} \mathcal{D}_{K_n} = C$ for some constant C . This establishes the claim of the main result (Theorem 2.5).

3 Further Ideas

In the following, we reflect on the main result of the paper [21], and we investigate further avenues of thought. Each idea is summarized in a separate subsection. We begin by contemplating the canonical embedding.

3.1 An Alternate Canonical Embedding

Throughout this subsection, let K denote an algebraic number field of degree n with signature (r_1, r_2) , such that $n = r_1 + 2r_2$. In [21], p. 11, the authors define the canonical embedding as $\sigma : K \rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$, where $\sigma(x) = (\sigma_1(x), \dots, \sigma_n(x))$. In Definition 1.2.16, we also adhere to this form of canonical embedding. Under σ , any fractional ideal \mathcal{I} of K corresponds to an n -dimensional lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$. For volume computations, we identify \mathbb{C} with \mathbb{R}^2 , which yields $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} \cong \mathbb{R}^{r_1+2 \cdot 2r_2} = \mathbb{R}^{n+2r_2}$. In that sense, the n -dimensional lattice $\sigma(K)$ is therefore contained in the higher-dimensional space \mathbb{R}^{n+2r_2} . This may be seen as a source of complication for volume computations. We give an example of a volume computation in the paper.

Example. Consider Lemma 6.1 in [21], p. 14. In this lemma, the authors assert that for any fractional ideal \mathcal{I} of \mathcal{O}_K and for any $p \in [1, \infty]$, it holds that

$$\lambda_1^p(\mathcal{I}) \leq n^{1/p} \cdot N^{1/n}(\mathcal{I}) \cdot \sqrt{\mathcal{D}_K} \cdot (2/\pi)^{r_2/n},$$

where we mention that

1. $n^{1/\infty} := 1$ as a notational convention (see 2.1), and
2. $N^{1/n}(\mathcal{I}) = N(\mathcal{I})^{1/n}$ is an expression involving the *norm* $N(\mathcal{I})$ of a fractional ideal, a concept which is defined in [21], p. 12. We do not require this concept for the following, so we omit an explanation.

The idea of the proof ([21], p.15) revolves around applying Minkowski's Theorem to derive an upper bound for $\lambda_1^\infty(\mathcal{I})$. Recall from Remark 1.2.17 that the lattice $\sigma(\mathcal{I})$ lies in an n -dimensional subspace H of $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$. Employing Minkowski's Theorem involves computing the n -dimensional volume of the unit cube in H (measured in l_∞ -norm). More precisely, the subspace containing $\sigma(\mathcal{I})$ can be specified as $H = \{(z_1, \dots, z_n) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : \overline{z_{r_1+j}} = z_{(r_1+r_2)+j} \text{ for all } 1 \leq j \leq r_2\}$. Hence the corresponding unit cube in l_∞ -norm can be specified as $\mathcal{C} := \{\mathbf{z} \in H : \|\mathbf{z}\|_\infty \leq 1\}$. To work out the n -dimensional volume of \mathcal{C} , the authors view \mathcal{C} as the cartesian product $\mathcal{C}_1^{r_1} \times \mathcal{C}_2^{r_2}$, where $\mathcal{C}_1 := \{x \in \mathbb{R} : |x| \leq 1\}$ and $\mathcal{C}_2 := \{(z, \bar{z}) \in \mathbb{C}^2 : |z| \leq 1\}$. By computing the one-dimensional volume of \mathcal{C}_1 and the two-dimensional volume of \mathcal{C}_2 , the volume of \mathcal{C} is derived by multiplication. Evidently, $\text{vol}(\mathcal{C}_1) = 2$. Observe

that

$$\begin{aligned}\mathcal{C}_2 &= \{(z, \bar{z}) \in \mathbb{C}^2 : |z| \leq 1\} \equiv \{(a, b, a, -b) \in \mathbb{R}^4 : a^2 + b^2 \leq 1\} \\ &= \{a \cdot (1, 0, 1, 0) + b \cdot (0, 1, 0, -1) : a^2 + b^2 \leq 1\}.\end{aligned}$$

For the practised reader, it may be evident that \mathcal{C}_2 constitutes a two-dimensional sphere with radius $\sqrt{2}$ on a plane in four-dimensional space. Applying an orthogonal matrix permits us to further clarify the geometric situation without altering the volume of \mathcal{C}_2 . Choose

$$\mathbf{B} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \in \mathbb{R}^{4 \times 4}.$$

Then $\mathbf{B} \cdot \mathcal{C}_2 = \{\mathbf{B}x : x \in \mathcal{C}_2\} = \{a \cdot \mathbf{B}(1, 0, 1, 0) + b \cdot \mathbf{B}(0, 1, 0, -1) : a^2 + b^2 \leq 1\} = \{a \cdot (\sqrt{2}, 0, 0, 0) + b \cdot (0, \sqrt{2}, 0, 0) : a^2 + b^2 \leq 1\}$. It is fairly evident that $\mathbf{B} \cdot \mathcal{C}_2$ is a two-dimensional sphere with radius $\sqrt{2}$ in the x_1 - x_2 -plane. Consequentially, $\text{vol}(\mathcal{C}_2) = \text{vol}(\mathbf{B} \cdot \mathcal{C}_2) = 2\pi$. The unit cube \mathcal{C} in H therefore has n -dimensional volume $2^{r_1} \cdot (2\pi)^{r_2}$.

Volume computations for lattices which lie in higher-dimensional space may be seen as requiring some care. It seems worth mentioning that in the literature on number theory, the canonical embedding is often defined differently. The following definition is adapted from [16], p.100.

Definition 3.1.1. Let θ_j for $j = 1, \dots, r_1$ denote the real embeddings of K . For $j = r_1 + 1, \dots, r_1 + r_2$ choose complex embeddings θ_j of K such that exactly one θ_j is taken from each complex conjugate pair $\theta_j, \overline{\theta_j}$ of such embeddings. Then define the *number theoretic canonical embedding* as $\Theta : K \rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, where $\Theta(x) = (\theta_1(x), \dots, \theta_{r_1}(x), \theta_{r_1+1}(x), \dots, \theta_{r_1+r_2}(x))$.

We remark that for any fractional ideal \mathcal{I} of \mathcal{O}_K , the lattice $\Theta(\mathcal{I})$ is of full rank due to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1+2r_2} = \mathbb{R}^n$. It seems possible that usage of Θ could facilitate lattice theoretic observations.

3.2 Cryptographic Hardness

We now focus on the problem of obtaining cryptographic hardness from the ideal lattices which we consider. We explain the difficulty which arises when trying to design collision resistant hash functions based on worst case computational assumptions on such ideal lattices. Throughout this subsection, let $\mathcal{K}, m(n), q(n), \beta$ and $\gamma(n)$ be as specified in the Main Theorem 2.5.

It seems instructive to begin by considering the following (very simple) compression function family. This family is missing an essential information which is needed to easily establish collision resistance.

Definition 3.2.1. Dependent on $n \in \mathbb{Z}_{>0}$, we define the compression function family

$$\mathcal{H}_n := \left\{ h_{\mathbf{a}} : \mathcal{O}_{K_n}^{m(n)} \rightarrow \mathcal{O}_{K_n}/\langle q(n) \rangle, \quad h_{\mathbf{a}}(z) = \sum_{i=1}^{m(n)} a_i \cdot z_i \quad : \quad \mathbf{a} \in \mathcal{O}_{K_n}^{m(n)} \right\}.$$

Moreover, define $\mathcal{H} := \bigcup \mathcal{H}_n$.

To establish a notion of collision resistance, we make the following definition.

Definition 3.2.2. The problem $\text{Collision}_{\mathcal{H}}$ is defined as follows. Given $n \in \mathbb{Z}_{>0}$, an input is a function $h_{\mathbf{a}} \in \mathcal{H}_n$, where the a_i are random components which are chosen uniformly and independently from a predetermined set of representatives of $\mathcal{O}_{K_n}/\langle q(n) \rangle$. The problem is to find $\mathbf{b}, \mathbf{c} \in \mathcal{O}_{K_n}^{m(n)}$ such that $\mathbf{b} \neq \mathbf{c}$, but $h_{\mathbf{a}}(\mathbf{b}) = h_{\mathbf{a}}(\mathbf{c})$.

We view the compression function family \mathcal{H} as *collision resistant*, if there exists no polynomial-time algorithm that can solve $\text{Collision}_{\mathcal{H}}$ with non-negligible probability.

Our aim is to base the collision resistance of \mathcal{H} on the assumption that $\mathcal{K}\text{-ISVP}_{\gamma}^p$ is hard in the worst case: We would like to show that solving $\text{Collision}_{\mathcal{H}}$ with non-negligible probability is at least as hard as solving $\mathcal{K}\text{-ISVP}_{\gamma}^p$ in the worst case.

To this end, it seems immediate to use the assertion of the Main Theorem 2.5. Namely, the idea is to show that solving $\text{Collision}_{\mathcal{H}}$ with non-negligible probability is at least as hard as solving $\mathcal{K}\text{-SAIS}_{q,m,\beta}^{\infty}$ on the average with non-negligible probability. This is desirable, since the Main Theorem 2.5 states that solving $\mathcal{K}\text{-SAIS}_{q,m,\beta}^{\infty}$ on the average with non-negligible probability is at least as hard as solving $\mathcal{K}\text{-ISVP}_{\gamma}^p$ in the worst case.

Pursuing this idea, assume that the algorithm \mathcal{F} solves $\text{Collision}_{\mathcal{H}}$ with non-negligible probability. Then using \mathcal{F} , our goal is to construct an algorithm that solves $\mathcal{K}\text{-SAIS}_{q,m,\beta}^{\infty}$ on the average with non-negligible probability.

Let $n \in \mathbb{Z}_{>0}$ be given. On input $\mathbf{a} \in \mathcal{O}_{K_n}^{m(n)}$, chosen uniformly at random, algorithm \mathcal{F} provides $\mathbf{b}, \mathbf{c} \in \mathcal{O}_{K_n}^{m(n)}$ such that $\mathbf{b} \neq \mathbf{c}$ but $h_{\mathbf{a}}(\mathbf{b}) = h_{\mathbf{a}}(\mathbf{c})$ with non-negligible probability. Observe that $h_{\mathbf{a}}(\mathbf{b}) = h_{\mathbf{a}}(\mathbf{c}) \iff h_{\mathbf{a}}(\mathbf{b} - \mathbf{c}) = 0 \iff \mathbf{b} - \mathbf{c} \in \Psi_{q(n)}^{K_n}(\mathbf{a})$, where $\mathbf{b} - \mathbf{c} \neq 0$. Hence the missing information of \mathcal{H} is a guarantee that $\|\mathbf{b} - \mathbf{c}\|_{\infty} \leq \beta(n)$.

To address this difficulty, Peikert and Rosen suggest developing an injective, efficient mapping from bit strings to sufficiently short vectors in $\mathcal{O}_{K_n}^{m(n)}$.

We explain the impact of such a mapping in the following.

Assume that for some $k \in \mathbb{Z}_{>0}$, the function $z : \{0, 1\}^k \rightarrow \mathcal{O}_{K_n}^{m(n)}$ is such a mapping³. Then dependent on $n \in \mathbb{Z}_{>0}$, define the function family

$$\mathcal{H}'_n := \left\{ h'_{\mathbf{a}} : \{0, 1\}^k \rightarrow \mathcal{O}_{K_n}/\langle q(n) \rangle, \quad h'_{\mathbf{a}}(\mathbf{b}) := h_{\mathbf{a}}(z(\mathbf{b})) \quad : \quad \mathbf{a} \in \mathcal{O}_{K_n}^{m(n)} \right\}.$$

Moreover, define $\mathcal{H}' := \bigcup \mathcal{H}'_n$. Let $\text{Collision}_{\mathcal{H}'}$ be defined analogous to Definition 3.2.2. Then an algorithm \mathcal{F}' which solves $\text{Collision}_{\mathcal{H}'}$ with non-negligible probability provides short vectors $z(\mathbf{b}_1) \neq z(\mathbf{b}_2) \in \mathcal{O}_{K_n}^{m(n)}$ such that $z(\mathbf{b}_1) - z(\mathbf{b}_2)$ is a nonzero element of $\Psi_{q(n)}^{K_n}(\mathbf{a})$, where this can be argued just as above. As a consequence, we would be able to ensure the condition $\|z(\mathbf{b}_1) - z(\mathbf{b}_2)\|_{\infty} \leq \beta(n)$, which would yield the result.

3.3 Relating K -ISVP $_{\gamma}^{\infty}$ to f -SPP $_{\gamma}$ for Monogenic Number Fields

In this subsection, we rewrite a result from the work of Lyubashevsky and Micciancio ([10], p.15-18), where we adopt the viewpoint of the work of Peikert and Rosen [21]. We consider algebraic number fields of the following type.

Definition 3.3.1. An algebraic number field K of degree n is called *monogenic* if there exists $\theta \in \mathcal{O}_K$ such that the ordered set $(1, \theta, \dots, \theta^{n-1})$ is an integral basis for K . In other words, $\mathcal{O}_K = \mathbb{Z}[\theta]$. In this case, the integral basis $(1, \theta, \dots, \theta^{n-1})$ is called a *power basis* for K . ([5], p.158)

As an example for a monogenic algebraic number field, we consider cyclotomic fields, which we introduce now. All of the following facts on cyclotomic fields can be verified in [5], p. 186-187.

Definition 3.3.2. Let $m \in \mathbb{Z}_{>0}$. Let ζ_m be any *primitive m -th root of unity*, which means $(\zeta_m)^m = 1$ and $(\zeta_m)^k \neq 1$ for $k = 1, \dots, m-1$. Then the field $K_m = \mathbb{Q}(\zeta_m)$ is called the *m -th cyclotomic field*.

Remarks 3.3.3. 1. It can be shown that for $m \in \mathbb{Z}_{>0}$, there are $\phi(m)$ primitive roots of unity, where ϕ denotes Euler's totient function. Namely if ζ_m is a primitive m -th root of unity, it can be shown that for any $r \in \{1, \dots, m\}$ such that $\gcd(r, m) = 1$, the number ζ_m^r is also a primitive m -th root of unity. Despite the fact that there are several m -th roots of unity, the m -th cyclotomic field is well-defined, since it is possible to prove that $K_m = \mathbb{Q}(\zeta_m^r)$ for any r such that $\gcd(r, m) = 1$.

2. The minimal polynomial of ζ_m is $f_m(x) = \prod_{\substack{1 \leq r \leq m: \\ \gcd(r, m) = 1}} (x - \zeta_m^r)$. It can be proved that $f_m \in \mathbb{Z}[x]$, so $\zeta_m \in \mathcal{O}_{K_m}$. As a consequence, $K_m = \mathbb{Q}(\zeta_m)$

³For example, a sufficient property is $\|z(\mathbf{b})\|_{\infty} \leq \beta(n)/2$ for $\mathbf{b} \in \{0, 1\}^k$.

is an algebraic number field. And since the degree of f_m is $\phi(m)$, it follows that $[K_m : \mathbb{Q}] = \phi(m)$.

3. An integral basis for $K_m = \mathbb{Q}(\zeta_m)$ is given by the set

$$\left(1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{\phi(m)-1}\right).$$

Hence for any $m \in \mathbb{Z}_{>0}$, the m -th cyclotomic field K_m is monogenic.

We collect a few further examples of monogenic algebraic number fields ([5], p.158-159).

Examples 3.3.4. 1. Every *quadratic*⁴ number field is monogenic.

2. A monogenic *cubic*⁵ number field is $K = \mathbb{Q}(2^{\frac{1}{3}})$.

3. A monogenic *quartic*⁶ algebraic number field is $K = \mathbb{Q}\left(\frac{\sqrt{2+i\sqrt{2}}}{2}\right)$.

In [10], p. 8, Lyubashevsky and Micciancio define the problem f -SPP $_{\gamma}$. For the convenience of the reader, we repeat the definition. First, we require a certain norm for polynomials.

Definition 3.3.5. For a polynomial $f = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{Z}[x]$, we define the norm $\|f\|_{\infty} := \|(a_0, \dots, a_{n-1})\|_{\infty}$. In other words, $\|f\|_{\infty}$ is defined as the corresponding norm of the coefficient vector of f .

Definition 3.3.6. Let f be a monic polynomial of degree n . Then in the approximate Shortest Polynomial Problem f -SPP $_{\gamma}(\mathcal{I})$ we are given an ideal $\mathcal{I} \subseteq \mathbb{Z}[x]/\langle f \rangle$. We are asked to find a $g \in \mathcal{I}$ such that $g \neq 0$ and $\|g\|_f \leq \gamma \lambda_1^{\infty}(\mathcal{I})$, where for $g = g + \langle f \rangle \in \mathbb{Z}[x]/\langle f \rangle$, the norm $\|g\|_f$ is defined as $\|g \bmod f\|_{\infty}$.

Moreover, the two following items, which are taken from [10], p.16, play an important role.

Definitions 3.3.7. 1. For any algebraic number $\alpha \in \mathbb{C}$, define the function $\max\text{Conj}(\alpha)$ to be $\max\{|\phi_i| : 1 \leq i \leq n\}$, where the ϕ_i are the roots of the minimal polynomial of α over \mathbb{Q} .

2. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field. Then in the approximate Smallest Conjugate Problem SCP $_{\gamma}(\mathcal{I})$, we are given an ideal \mathcal{I} of \mathcal{O}_K and we are asked to find a nonzero element $\alpha \in \mathcal{I}$ such that $\max\text{Conj}(\alpha) \leq \gamma \cdot \max\text{Conj}(\alpha')$ for all $\alpha' \in \mathcal{I}$.

The following lemma establishes a connection to the work of Peikert and Rosen.

Lemma 3.3.8. *Let K be an algebraic number field of degree n with signature (r_1, r_2) . Let $\sigma : K \rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2}$ denote the canonical embedding. Then for all $\alpha \in K$, the infinity norm $\|\sigma(\alpha)\|_{\infty}$ of the vector $\sigma(\alpha)$ equals $\max\text{Conj}(\alpha)$. In formula, $\|\sigma(\alpha)\|_{\infty} = \max\text{Conj}(\alpha)$ for all $\alpha \in K$.*

⁴of degree 2

⁵of degree 3

⁶of degree 4

Proof. For $\alpha \in K$, Consider the field polynomial of α over K , which is given by $\text{fld}_K^\alpha(x) = \prod_{k=1}^n (x - \sigma_k(\alpha))$, where the σ_k denote the n embeddings of K into \mathbb{C} ([5], p.117). A theorem from number theory ([5], p.120) states that if f is the minimal polynomial of α , then $\text{fld}_K^\alpha(x) = f(x)^s$ for some $s \in \mathbb{Z}_{>0}$. In other words, the field polynomial is a power of the minimal polynomial. Therefore the set of roots of the field polynomial of α coincides with the set of roots of the minimal polynomial of α . Thus to determine $\text{maxConj}(\alpha)$, we may take the maximum over the set of roots of the field polynomial, which is $\max\{|\sigma_i(\alpha)| : 1 \leq i \leq n\} = \|\sigma(\alpha)\|_\infty$. \square

Recall the problem $K\text{-ISVP}_\gamma^\infty$ from Definition 2.2. We may now formulate an equivalence result for this problem.

Corollary 3.3.9. *Given an algebraic number field K , the problems $K\text{-ISVP}_\gamma^\infty$ and SCP_γ are equivalent. In other words, a solution to one problem solves the other.*

Proof. Let \mathcal{I} denote an ideal of \mathcal{O}_K . Then using Lemma 3.3.8, we argue as follows: $\alpha \in \mathcal{I}$ solves $K\text{-ISVP}_\gamma^\infty$ on input $\mathcal{I} \iff \|\sigma(\alpha)\|_\infty \leq \gamma \cdot \lambda_1^\infty(\sigma(\mathcal{I})) \iff \|\sigma(\alpha)\|_\infty \leq \gamma \cdot \|\sigma(\alpha')\|_\infty$ for all $\alpha' \in \mathcal{I} \iff \text{maxConj}(\alpha) \leq \gamma \cdot \text{maxConj}(\alpha')$ for all $\alpha' \in \mathcal{I} \iff \alpha \in \mathcal{I}$ solves SCP_γ on input \mathcal{I} . \square

The next lemma mainly clarifies notation.

Lemma 3.3.10. *Let K be a monogenic algebraic number field of degree n with integral basis $(1, \theta, \dots, \theta^{n-1})$ for some $\theta \in \mathcal{O}_K$. Further, let $f \in \mathbb{Z}[x]$ denote the minimal polynomial of θ . Then the map $\varphi : \mathbb{Z}[x]/\langle f \rangle \rightarrow \mathcal{O}_K$, defined by $\sum_{i=0}^{n-1} z_i x^i + \langle f \rangle \mapsto \sum_{i=0}^{n-1} z_i \theta^i$, is an isomorphism.*

Proof. Consider the ring homomorphism $\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[\theta] = \mathcal{O}_K$, defined by $\sum_{i=0}^l z'_i x^i \mapsto \sum_{i=0}^l z'_i \theta^i = \sum_{i=0}^{n-1} z_i \theta^i$. Moreover, let $\pi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[x]/\langle f \rangle$ denote the canonical map defined by $\sum_{i=0}^l z'_i x^i \mapsto \sum_{i=0}^l z'_i x^i + \langle f \rangle = \sum_{i=0}^{n-1} z_i x^i + \langle f \rangle$. It can be argued that $\ker \phi = \langle f \rangle \subseteq \mathbb{Z}[x]$ ([2], p. 471). Applying the first isomorphism theorem ([2], p.412) yields the existence and uniqueness of a ring isomorphism $\varphi : \mathbb{Z}[x]/\langle f \rangle \rightarrow \mathbb{Z}[\theta] = \mathcal{O}_K$ such that $\varphi \circ \pi = \phi$. Therefore, φ maps $\sum_{i=0}^{n-1} z_i x^i + \langle f \rangle$ to $\sum_{i=0}^{n-1} z_i \theta^i$, as desired. \square

The following diagram clarifies the situation in the proof of Lemma 3.3.10.

$$\begin{array}{ccc}
 \mathbb{Z}[x] & \xrightarrow{\phi} & \mathbb{Z}[\theta] = \mathcal{O}_K \\
 \downarrow \pi & \nearrow \varphi & \\
 \mathbb{Z}[x]/\langle f \rangle & &
 \end{array}$$

Remarks 3.3.11. Retain the notation of Lemma 3.3.10. The following items are worth mentioning.

1. The proof of the above Lemma 3.3.10 strongly relies on the fact that K is a monogenic algebraic number field, in other words, that $\mathbb{Z}[\theta] = \mathcal{O}_K$.
2. Note that the isomorphism φ in the above Lemma 3.3.10 actually depends on θ . However, we choose not to incorporate this dependence into the notation, and trust that it is clear from the context.
3. The above Lemma 3.3.10 establishes that for ideals \mathcal{I} in \mathcal{O}_K , there is a bijective correspondence to ideals $\varphi^{-1}(\mathcal{I})$ in $\mathbb{Z}[x]/\langle f \rangle$, which hints at how we later establish a connection between K -ISVP $_{\gamma}^{\infty}$ and f -SPP $_{\gamma}$.

Next, we introduce an auxiliary function.

Definition 3.3.12. Let θ be an algebraic integer of degree n . Then for any $\alpha = \sum_{i=0}^{n-1} \alpha_i \theta^i \in \mathbb{Q}(\theta)$, we define the function $\max\text{Coeff}_{\theta} : \mathbb{Q}(\theta) \rightarrow \mathbb{R}_{\geq 0}$ as $\alpha \mapsto \max\{|\alpha_i| : i = 0, \dots, n-1\}$.

For the convenience of the reader, we include three lemmas from [10], p.17, which are used in the argumentation to come. The first two lemmas are slightly modified from the original.

Lemma 3.3.13 (corresponds to Lemma B.8 in [10]). *Let $f \in \mathbb{Z}[x]$ be a monic irreducible⁷ polynomial of degree n with roots $\theta_1, \dots, \theta_n \in \mathbb{C}$. Assume that there exists a real t such that for all $1 \leq i \leq n$, we have $|\theta_i^j| \leq t$ for all $0 \leq j \leq n-1$. Let $K = \mathbb{Q}(\theta_1)$ and $\alpha = \alpha_0 + \alpha_1 \theta_1 + \dots + \alpha_{n-1} \theta_1^{n-1} \in K$. Then $\max\text{Conj}(\alpha) \leq nt \cdot \max\text{Coeff}_{\theta_1}(\alpha)$.*

Proof. Using Lemma 3.3.8 and $\sigma_i(\theta_1) = \theta_i$, we may write

$$\begin{aligned} \max\text{Conj}(\alpha) &= \|\sigma(\alpha)\|_{\infty} = \max\{|\sigma_i(\alpha)| : 1 \leq i \leq n\} \\ &= \max\{|\alpha_0 + \alpha_1 \theta_i + \dots + \alpha_{n-1} \theta_i^{n-1}| : 1 \leq i \leq n\} \\ &\leq \max\text{Coeff}_{\theta_1}(\alpha) \cdot \max\{1 + |\theta_i| + \dots + |\theta_i^{n-1}| : 1 \leq i \leq n\}. \end{aligned} \quad (2)$$

By assumption, we have $|\theta_i^j| \leq t$ for all $0 \leq j \leq n-1$ and $1 \leq i \leq n$. This yields $\sum_{j=0}^{n-1} |\theta_i^j| \leq n \cdot t$ for all $1 \leq i \leq n$. Therefore by inequality 2, $\max\text{Conj}(\alpha) \leq nt \cdot \max\text{Coeff}_{\theta_1}(\alpha)$. \square

Remark 3.3.14. The formulation of Lemma 3.3.13 differs slightly from the formulation of Lemma B.8 in [10] in the sense that Lemma B.8 in [10] contains the weaker assumption that there exists a real t for which

$$|\theta_i^{n-1}| \leq t \text{ for all } 1 \leq i \leq n. \quad (3)$$

In Lemma 3.3.13, we assume the existence of a real t such that

$$|\theta_i^j| \leq t \text{ for all } 1 \leq i \leq n \text{ and for all } 0 \leq j \leq n-1. \quad (4)$$

⁷over \mathbb{Q}

Assumption 4 implies $t \geq 1$, which makes it easy to argue that

$$\max \{1 + |\theta_i| + \dots + |\theta_i^{n-1}| : 1 \leq i \leq n\} \leq nt$$

in the proof of Lemma 3.3.13. However, the author does not know whether every monic irreducible integer polynomial has at least one root of absolute value greater or equal 1; together with such a statement, assumption 3 would equally imply $t \geq 1$. Incidentally, not every monic irreducible integer polynomial has only roots of absolute value greater or equal 1. Consider $x^2 - x - 1$, the roots of which are the golden ratio $\Phi = \frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$, where the latter has absolute value smaller than 1.

Lemma 3.3.15 (corresponds to Lemma B.9 in [10]). *Let $f \in \mathbb{Z}[x]$ be a monic irreducible⁸ polynomial of degree n with roots $\theta_1, \dots, \theta_n \in \mathbb{C}$. Let $K = \mathbb{Q}(\theta_1)$ be an algebraic number field. Assume that there exists an integer $m \geq n$ and a real t such that for all $1 \leq i \leq n$ and $0 \leq j \leq m-1$, we have*

- $1 \leq |\theta_i^j| \leq t$, and
- $|\sum_{i=1}^n \theta_i^m| \geq n$.

To ease notation, define the index set $T := \{l \in \mathbb{Z}_{>0} : m - n + 1 \leq l \leq m + n - 1, l \neq m\}$. We further assume that for all numbers $l \in T$, we have $|\sum_{i=1}^n \theta_i^l| \leq 1$. Then for $s := \max \{|\sum_{i=1}^n \theta_i^l| : l \in T\}$, we have for all $\alpha \in K$, that

$$\max \text{Coeff}_{\theta_1}(\alpha) \leq \frac{nt}{n(1-s) + s} \max \text{Conj}(\alpha).$$

Remark 3.3.16. The above version of Lemma B.9 is slightly modified from the original in the following way. Lemma B.9 in [10], p.17, contains the assumption

$$\left| \sum_{i=1}^n \theta_i^l \right| \leq s \leq 1 \text{ for all } l \neq 0 \pmod{m}. \quad (5)$$

To the author, it seems that this assumption can be stated in a more precise way (and perhaps weakened) by limiting l to the set $T = \{m - n + 1, \dots, m + n - 1\} / \{m\}$, as formulated in Lemma 3.3.15. The reader will appreciate a short justification. In the proof of Lemma B.9 in [10], we consider an element $\alpha = \alpha_0 + \alpha_1 \theta_1 + \dots + \alpha_{n-1} \theta_1^{n-1} \in K$, where $\alpha_h \in \mathbb{Q}$ for $0 \leq h \leq n-1$. Set $S_k := \sum_{i=1}^n \theta_i^{m-n+k}$ for $k \in \mathbb{Z}_{>0}$. Then together with the assumption $S_n = |\sum_{i=1}^n \theta_i^m| \geq n$ (as stated in Lemma 3.3.15), assumption 5 is used to argue the inequality

$$\begin{aligned} & n|\alpha_{n-j}| - s(|\alpha_0| + \dots + |\alpha_{n-j-1}| + |\alpha_{n-j+1}| + \dots + |\alpha_{n-1}|) \\ & \leq |\alpha_{n-j} S_n| - (|\alpha_0 S_j| + \dots + |\alpha_{n-j-1} S_{n-1}| + |\alpha_{n-j+1} S_{n+1}| \\ & \quad + \dots + |\alpha_{n-1} S_{n-1+j}|), \text{ where } 1 \leq j \leq n. \end{aligned} \quad (6)$$

⁸over \mathbb{Q}

We take a closer look at the way assumption 5 is applied to prove inequality 6. To this end, fix $j \in 1, \dots, n$. Then for inequality 6, we use that $|S_k| = \left| \sum_{i=1}^n \theta_i^{m-n+k} \right| \leq s$ for all k such that $j \leq k \leq j+n-1$, and $k \neq n$. This is true by assumption 5, since for such k , the exponents of the θ_i in the S_k expression lie in the range from $m-n+j$ to $m-n+(j+n-1) = m+j-1$, where the exponent m is skipped.

$$\begin{array}{ccccccc} | & | & | & | & | & & \rightarrow \mathbb{Z}_{>0} \\ 0 & m-n & m-n+j & m & m+j-1 & & \end{array}$$

Now observe that j ranges from 1 to n . Hence all possible exponents of the S_k expressions lie in the range from $m-n+1$ to $m+n-1$. Therefore it seems that it would suffice to formulate assumption 5 as

$$\left| \sum_{i=1}^n \theta_i^l \right| \leq s \leq 1 \text{ for all } l \in T.$$

The following lemma is proved in [10] using Lemma 3.3.13 (which is B.8 in [10]), and Lemma 3.3.15 (which is B.9 in [10]).

Lemma 3.3.17 (corresponds to Lemma B.10 in [10]). *Let $f = x^n + x^{n-1} + \dots + 1$ be an irreducible⁹ polynomial and let $\theta \in \mathbb{C}$ be one of its roots. Let $K = \mathbb{Q}(\theta)$ and let α be an element of K . Then $\max\text{Coeff}_\theta(\alpha) \leq n \cdot \max\text{Conj}(\alpha)$ and $\max\text{Conj}(\alpha) \leq n \cdot \max\text{Coeff}_\theta(\alpha)$.*

Now we can formulate a result for certain cyclotomic fields.

Theorem 3.3.18 (corresponds to Theorem B.7 in [10]). *Let p be a prime. Consider the p -th cyclotomic field $K_p = \mathbb{Q}(\zeta_p)$. Let f denote the minimal polynomial of ζ_p . Then*

$$f\text{-SPP}_{\gamma(p-1)^2} \leq K_p\text{-ISVP}_\gamma^\infty \text{ and } K_p\text{-ISVP}_{\gamma(p-1)^2}^\infty \leq f\text{-SPP}_\gamma.$$

Proof. We prove $K_p\text{-ISVP}_{\gamma(p-1)^2}^\infty \leq f\text{-SPP}_\gamma$. Thus let \mathcal{F} denote an oracle for $f\text{-SPP}_\gamma$. Then the reduction algorithm \mathcal{R} is given as follows. On input \mathcal{I} , where \mathcal{I} is an ideal of $\mathcal{O}_{K_p} = \mathbb{Z}[\zeta_p]$,

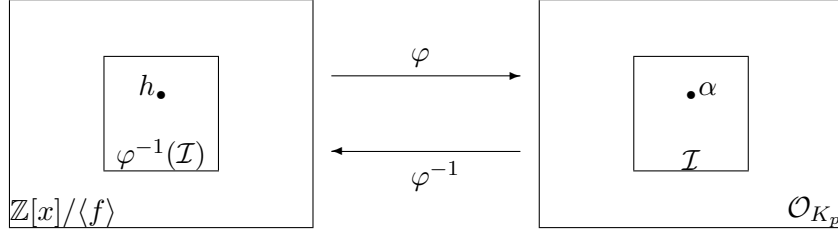
1. Let $h \leftarrow \mathcal{F}(\varphi^{-1}(\mathcal{I}))$.
2. Output $\varphi(h)$.

We show the correctness of \mathcal{R} . By definition, \mathcal{F} yields an element $h \in \varphi^{-1}(\mathcal{I})$ such that $\|h\|_f \leq \gamma \|h'\|_f$ for all $h' \in \varphi^{-1}(\mathcal{I})$. Let $\alpha := \varphi(h)$. Observe that for any $g \in \mathbb{Z}[x]/\langle f \rangle$, we have $\|g\|_f = \max\text{Coeff}_{\zeta_p}(\varphi(g))$. Therefore $\max\text{Coeff}_{\zeta_p}(\alpha) \leq \gamma \cdot \max\text{Coeff}_{\zeta_p}(\alpha')$ for all $\alpha' \in \mathcal{I}$. Using Remarks 3.3.3, we can verify that the minimal polynomial of ζ_p is given by $f(x) = x^{p-1} + x^{p-2} + \dots + 1$. Therefore we may use Lemma 3.3.17 in the following. Using

⁹over \mathbb{Q}

Lemma 3.3.17, we see that $\max\text{Conj}(\alpha) \leq (p-1) \cdot \max\text{Coeff}_{\zeta_p}(\alpha)$. Applying the above reasoning, it follows that $\max\text{Conj}(\alpha) \leq (p-1) \cdot \gamma \cdot \max\text{Coeff}_{\zeta_p}(\alpha')$ for all $\alpha' \in \mathcal{I}$. Using Lemma 3.3.17 again, we see that $\max\text{Conj}(\alpha) \leq (p-1)^2 \cdot \gamma \cdot \max\text{Conj}(\alpha')$ for all $\alpha' \in \mathcal{I}$. Hence \mathcal{R} is correct. The proof of the converse reduction is analogous. \square

The picture below provides an intuition for the proof of Theorem 3.3.18.



It is possible to generalize this result to a certain degree, at the price of further complication.

Theorem 3.3.19 (adapted from Theorem B.7 in [10]). *Let K be a monogenic algebraic number field of degree n such that $\mathcal{O}_K = \mathbb{Z}[\theta]$ for an appropriate $\theta \in \mathcal{O}_K$. Let $f \in \mathbb{Z}[x]$ denote the minimal polynomial of θ , where the roots of f are given as $\theta = \theta_1, \dots, \theta_n \in \mathbb{C}$. Assume that there exists an integer $m \geq n$ and a real t such that for all $1 \leq i \leq n$ and $0 \leq j \leq m-1$, we have*

- $1 \leq |\theta_i^j| \leq t$, and
- $|\sum_{i=1}^n \theta_i^m| \geq n$.

To ease notation, define the index set $T := \{l \in \mathbb{Z}_{>0} : m-n+1 \leq l \leq m+n-1, l \neq m\}$. We further assume that for all numbers $l \in T$, we have $|\sum_{i=1}^n \theta_i^l| \leq 1$. Then for $s := \max\{|\sum_{i=1}^n \theta_i^l| : l \in T\}$ and $c := \frac{(nt)^2}{n(1-s)+s}$, we have

$$f\text{-SPP}_{\gamma c} \leq K\text{-ISVP}_{\gamma}^{\infty} \text{ and } K\text{-ISVP}_{\gamma c}^{\infty} \leq f\text{-SPP}_{\gamma}.$$

Proof. We prove $K\text{-ISVP}_{\gamma c}^{\infty} \leq f\text{-SPP}_{\gamma}$. Thus let \mathcal{F} denote an oracle for $f\text{-SPP}_{\gamma}$. Then the reduction algorithm \mathcal{R} is given as follows. On input \mathcal{I} , where \mathcal{I} is an ideal of $\mathcal{O}_K = \mathbb{Z}[\theta]$,

1. Let $h \leftarrow \mathcal{F}(\varphi^{-1}(\mathcal{I}))$.
2. Output $\varphi(h)$.

We show the correctness of \mathcal{R} . By definition, \mathcal{F} yields an element $h \in \varphi^{-1}(\mathcal{I})$ such that $\|h\|_f \leq \gamma \|h'\|_f$ for all $h' \in \varphi^{-1}(\mathcal{I})$. Let $\alpha := \varphi(h)$. Observe that for any $g \in \mathbb{Z}[x]/\langle f \rangle$, we have $\|g\|_f = \max\text{Coeff}_{\theta}(\varphi(g))$. Therefore $\max\text{Coeff}_{\theta}(\alpha) \leq \gamma \cdot \max\text{Coeff}_{\theta}(\alpha')$ for all $\alpha' \in \mathcal{I}$. Note that by assumption, the minimal polynomial f of θ satisfies the conditions of Lemmas 3.3.13 and 3.3.15. Using Lemma 3.3.13, we see that $\max\text{Conj}(\alpha) \leq nt \cdot \max\text{Coeff}_{\theta}(\alpha)$. Applying the above reasoning, it follows that $\max\text{Conj}(\alpha) \leq nt\gamma \cdot \max\text{Coeff}_{\theta}(\alpha')$

for all $\alpha' \in \mathcal{I}$. Using Lemma 3.3.15, we see that

$$\max\text{Conj}(\alpha) \leq \frac{(nt)^2}{n(1-s) + s} \gamma \cdot \max\text{Conj}(\alpha') = c\gamma \cdot \max\text{Conj}(\alpha')$$

for all $\alpha' \in \mathcal{I}$. Hence \mathcal{R} is correct.

The proof of the converse reduction is analogous. □

Conclusion

In conclusion, we consider the following items worth mentioning.

An important effort of this thesis consists in making the reasoning of Peikert and Rosen [21] more easily accessible. Ideally, an undergraduate student may comprehend not only the gist of the paper, but also a few finer points of the reasoning.

In 3.1, we depict a difference between the canonical embedding chosen in [21], and the embedding that seems more commonly used in the literature on algebraic number theory. The embedding used in [21] may seem more complicated for certain purposes than the embedding used in the literature on algebraic number theory. Whether using the latter embedding facilitates or complicates the reasoning in general is hard to judge for the author. Indeed, the differences may also be minor.

In [10], p. 13, Lyubashevsky and Micciancio write that “Determining the hardness of the SCP problem ... is also an interesting problem”. In 3.3, we illustrate that from the viewpoint of Peikert and Rosen, an almost analogously defined problem SCP_γ corresponds to $K\text{-ISVP}_\gamma^\infty$, which is a lattice problem.

In 3.3, we consider monogenic number fields $K = \mathbb{Q}(\zeta)$ with minimal polynomial f of ζ . We rewrite a result from [10], which yields an equivalence result for $f\text{-SPP}_\gamma$ and $K\text{-ISVP}_\gamma^\infty$.

As a further idea, we mention that one can extend the idea of a power basis to an *order*¹⁰ of \mathcal{O}_K . Perhaps a similar equivalence as proved in 3.3 could be proved for such orders.

Finally, reiterating 3.2, we call attention to the fact that the result of [21] seems to be of limited practicability as yet. As Peikert and Rosen wrote, “we do not yet know how to obtain cryptographic hardness (e.g. collision resistant hash functions) from ideal lattices over an arbitrary good number field K ” ([21], p. 27). However, an application of techniques related to [21] can be found in the SWIFFT hash function [11].

¹⁰For a definition, see [4], p. 181.

References

- [1] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 99–108. ACM, 1996.
- [2] M. Artin. *Algebra*. Birkhäuser, 1998.
- [3] S. Bakhtiari, R. Safavi-Naini, and J. Pieprzyk. Cryptographic hash functions: a survey. Technical report, 1995.
- [4] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer, 1996.
- [5] Şaban Alaca and K. S. Williams. *Introductory Algebraic Number Theory*. Cambridge University Press, 2004.
- [6] O. Goldreich. *Foundations of Cryptography*. Cambridge University Press, 2004.
- [7] O. Goldreich, S. Goldwasser, and S. Halevi. Collision-free hashing from lattice problems. *Electronic Colloquium on Computational Complexity (ECCC)*, 3(042), 1996.
- [8] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 2000.
- [9] A. Lenstra, H. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.
- [10] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *ICALP (2)*, volume 4052 of *Lecture Notes in Computer Science*, pages 144–155. Springer, 2006.
- [11] V. Lyubashevsky, D. Micciancio, C. Peikert, and A. Rosen. SWIFFT: A modest proposal for FFT hashing. In *FSE*, volume 5086 of *Lecture Notes in Computer Science*, pages 54–72. Springer, 2008.
- [12] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1996.
- [13] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Computational Complexity*, 16(4):365–411, 2007.
- [14] D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. In *FOCS*, pages 372–381. IEEE Computer Society, 2004.

- [15] D. Micciancio and O. Regev. Lattice-based cryptography. In D. J. Bernstein and J. Buchmann, editors, *Post-quantum Cryptography*. Springer, 2008.
- [16] R. A. Mollin. *Algebraic Number Theory*. Chapman & Hall/CRC, 1999.
- [17] R. A. Mollin. *An Introduction to Cryptography*. Chapman & Hall/CRC, 2007.
- [18] M. R. Murty and J. Esmonde. *Problems in Algebraic Number Theory*. Springer, 2005.
- [19] C. H. Papadimitriou. *Computational Complexity*. Addison-Wesley Publishing Company, Inc., 1994.
- [20] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *TCC*, 2006.
- [21] C. Peikert and A. Rosen. Lattices that admit logarithmic worst-case to average-case connection factors. In *STOC*, pages 478–487, 2007.
- [22] O. Regev. Lattice-based cryptography. In *Proc. of the 26th Annual International Cryptology Conference (CRYPTO)*, pages 131–141, 2006.
- [23] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26:1484–1509, 1997.