CHICAGO JOURNAL OF THEORETICAL COMPUTER SCIENCE 2008, Article 2, pages 1–40
http://cjtcs.cs.uchicago.edu/

Representing Hard Lattices with $O(n \log n)$ Bits *

Miklós Ajtai

Received: November 29, 2004; published: May 12, 2008.

Abstract: We present a variant of the Ajtai-Dwork public-key cryptosystem where the size of the public-key is only $O(n \log n)$ bits and the encrypted text/clear text ratio is also $O(n \log n)$. This is true with the assumption that all of the participants in the cryptosystem share $O(n^2 \log n)$ random bits which have to be picked only once and the users of the cryptosystem get them e.g. together with the software implementing the protocol. The public key is a random lattice with an n^c-unique nonzero shortest vector, where the constant $c > \frac{1}{2}$ can be picked arbitrarily close to $\frac{1}{2}$, and we pick the lattice according to a distribution described in the paper. We do not prove a worst-case average-case equivalence but the security of the system follows from the hardness of an average-case diophantine approximation problem related to a well-known theorem of Dirichlet.

1 Introduction

1.1 Cryptosystems based on the hardness of the unique shortest vector problem

The first public-key cryptosystem based on the assumed hardness of the unique shortest vector problem was given by Ajtai and Dwork in [2]. In that paper three variants of the system have been provided. The present work is based on the second version of the system where the public key is a random lattice L with a distribution σ so that L has an n^c-unique nonzero shortest vector with high probability. (u is an α-unique nonzero shortest vector of L if $u \in L$, $u \neq 0$ and for every $v \in L$, $\|v\| \leq \alpha\|u\|$ implies that v and u are parallel.) The public key is a random basis of L picked from a large cube. (In [2] actually the dual of

*A preliminary version of this paper has appeared in the Proceedings of the 37th ACM Symposium on Theory of Computing, see [1]

DOI: 10.4086/cjtcs.2008.002

L is used as a public key.) It is proved in [2] that if the distribution σ has the property that a polynomial time algorithm cannot find a nonzero shortest vector in L with a polynomially large probability then the cryptosystem is secure. (For this version of the cryptosystem, there is no specific recommendation for σ, it works with any distribution σ with the property decsribed in the previous sentence.) In this paper we define a distribution σ which meets this requirement provided that an average-case diophantine approximation problem, related to a famous theorem of Dirichlet has no polynomial time solution. Moreover in the new system the public key consists of only $O(n\log n)$ bits and we encrypt a single bit by $O(n\log n)$ bits. (In the second system described in [2] the key has at least $n^2\log n$ bits. Systems with worst-case average case connection, the third system in [2] and Regev's system in [14], have key sizes $O(n^4)$. The number of encrypted bits needed for a clear text bit is $O(n^2\log n)$ in the second version of the Ajtai-Dwork system and $O(n\log n)$ in the first version, where the lattice is represented with a basis of polynomial length. In the systems with worst-case average case equivalence this number is at least $O(n^3)$.) The small key size of the present system is achieved in the following way. The randomization of L according to σ is done in two stages. In the first stage we randomize a sequence b of $O(n^2\log n)$ bits. The randomization of b is done only once and b is available for every participants of the system. Assume now that b is fixed. In the second stage of the randomization the only information that we have about the first-stage is the value of b. We pick a random sequence t (with a distribution defined later) consisting of $O(n\log n)$ bits. b and t together will determine a lattice $L(b,t)$ which has an n^c-unique shortest vector (with high probability). The crucial property of the second stage of the randomization is that it can be done together with randomizing an n^c-unique nonzero shortest vector u in the lattice.

With such a randomization a participant of the system is able to select the public key t together with the private key u. Since t determines the lattice $L(b,t)$ for a fixed publicly known b, t indeed can serve as the public key instead of a basis of the lattice $L(b,t)$. The present paper consists of the description of the distribution σ and the proof that it has all of the required properties.

The constant c (in the n^c-uniqueness) may have any value greater than $\frac{1}{2}$. This improvement on the original $c > 5$ of the second system of [2] can be proved by adapting the original proof of [2], about the second system, to the techniques introduced by Regev in [14] that are based on a lemma of Banaszczyk (see [4]). Regev has improved the same constant to $c = 1.5$ for cryptosystems whose security is based on the hardness of the worst-case n^c-unique shortest vector problem, where the previous best value was $c = 7$. In his system encryption and decryption are done by arithmetic on the real line, instead of the n-dimensional space. We do not use this part of Regev's improvement. The improvement in c in our cryptosystem is independent of the improvement in the size of the key and holds for any distribution σ so that the n^c-unique shortest vector problem is hard. Therefore the contribution of the present paper is the improvement in the size of the key.

This last improvement in the value of the constant c is possible only if we change the value of a parameter in the second cryptosystem of [2]. This is not an essential change in the cryptosystem, conceptually it works the same way as before. Yet, the original proof of the reduction of the security of the cryptosystem to the n^c-unique shortest vector problem about the lattices involved, does not remain valid without any modification. In the last section we will give a modified proof about the security of cryptosystem, namely we will show that if σ is an arbitrary distribution which takes its values on lattices with an n^c-unique shortest vector so that for this distribution the shortest vector problem is hard, then our cryptosystem using lattices generated with distribution σ is secure. The modified proof (described in the

last section) has the same overall structure as the original one. We include it here partly to make the paper more self-contained and partly because it is very difficult to check the correctness of the modified proof if only the original proof and a list of the necessary changes are given.

1.2 Notation, preliminaries

We will use the ■ symbol to denote the end of the proof of a theorem or a lemma, e.g. the end of the proof of Lemma X will be denoted by (Lemma X)■

Definition 1.1. • $\mathbf{R}$ denotes the set of realnumbers, and $\mathbf{Z}$ denotes the set of integers, and $\mathbf{Q}$ denotes the set of rationals.

• Assume that $\alpha \in \mathbf{R}$, $[\![\alpha]\!]$ will denote the smallest nonnegative realnumber so that there is an integer k with $|k-\alpha| = [\![\alpha]\!]$. In other words, $[\![\alpha]\!]$ is the distance of α from the closest integer.

• Assume that α is a realnumber and g is a positive integer. Let j be the unique integer so that $\frac{j}{g} \leq \alpha < \frac{j+1}{g}$. We will use the notation $\mathtt{fr}(\alpha, g) = \frac{j}{g}$.

• If $a \in \mathbf{R}^n$ then $\|a\|_p$ will denote the ℓ_p norm of the vector a and we will use the notation $\|a\|$ for the Euclidean norm. We will use without further references the inequalities $\|a\|_\infty \leq \|a\|_2 \leq n^{\frac{1}{2}}\|a\|_\infty$

• If $a_1, ..., a_n$ are linearly independent vectors in $\mathbf{R}^n$ then the set of their linear combinations with integer coefficients is called a lattice. $a_1, ..., a_n$ is a basis of the lattice. A lattice may have several different bases. The volume of the parallelepiped defined by the basis vectors is the determinant of the lattice. The dual L^* of the lattice L is the set of all $x \in \mathbf{R}^n$ so that $xa \in Z$ for all $a \in L$, where xa is the inner product of the vectors x and a. L^* is a lattice in $\mathbf{R}^n$.

• We say that u is a shortest nonzero vector (sh.n.v.) in the lattice L if $u \in L$, $u \neq 0$ and for all $v \in L$, $v \neq 0$ we have $\|v\| \geq \|u\|$. Assume $\alpha > 1$. The vector u is an α-unique shortest nonzero vector of L, if it is a shortest nonzero vector in L, and for all $v \in L$, $\|v\| \leq \alpha\|u\|$ implies that v and u are parallel. (In this definition we may use the ℓ_p norm $\|a\|_p$ for each $a \in L$ instead of the Euclidean norm. This way we get the definition of an α-unique sh.n.v. with respect to the ℓ_p norm.)

• $e_1, ..., e_n$ will denote the unit vectors in $\mathbf{R}^n$, that is, for all $i = 1, ..., n$ the ith component of e_i is 1, all of the other components of e_i are 0s.

• If $a_1, ..., a_n$ is a basis of L then the unique basis $f_1, ..., f_n$ of L^* so that for all $i = 1, ..., n$, $a_i f_i = 1$ and for all $i, j \in \{1, ..., n\}$ with $i \neq j$, $a_i f_j = 0$, is called the dual of $a_1, ..., a_n$. (See e.g. [13] for further details.)

• If $a_1, ..., a_n$ are linearly independent vectors in $\mathbf{R}^n$, then $\mathcal{P}(a_1, ..., a_n)$ is the set of all vectors of the form $\sum_{i=1}^n \alpha_i a_i$ where $\alpha_i \in [0, 1)$ for all $i = 1, ..., n$.

Most of the computational problems are usually formulated for lattices $L \subseteq \mathbf{Z}^n$. For the formulation of our results of algorithmic nature we will use lattices in $\mathbf{Q}^n$. This is not an essential difference (only a difference in scaling) since for every lattice $L \subseteq \mathbf{Q}^n$ there is an integer k so that $kL \subseteq \mathbf{Z}^n$. Some of our results were motivated by consideration about lattices in $\mathbf{R}^n$, e.g. when the components of the vectors generating the lattice are random reals taken with uniform distribution from an interval. In this case we will formulate the result both over the reals (and after a suitable approximation) over the rationals.

Computational questions involving realnumbers. In the formulation of our main result (in particular in the hardness assumption) we will allow realnumbers as inputs. We will treat this situation

in a simple way described in the definition below, which is good for this particular purpose, although it is not a good solution for the treatment of real input in general. In the last section, we will need a more sophisticated approach to this problem. We will use there (only in the last section) the oracle representation of reals as it has been defined by Lovász in [10]. The definition below will be used only in the Hardness Assumption.

Definition 1.2. • We will allow realnumbers as inputs for our algorithms. We assume the each realnumber occurring in the input is in the interval $[0,1]$. Every realnumber is represented by the sequence of its binary bits. The algorithm can read these bits only in their natural order and reading one bit is considered as one unit of time. Therefore a polynomial time algorithm can read only a polynomial size initial segment from the sequence of binary bits of a realnumber.

1.3 Highlevel description of the proposed cryptosystem

We describe now the second cryptosystem from [2] incorporating the following improvements: (a) the reduction in the size of the key which is the topic of the present paper. (b) an improved definition of the perturbation of lattice points by normal distribution as defined by Regev in [14], which makes possible the mentioned improvement in c. The original perturbation in [2] was an approximation of a normal distribution with different parameters. We may change the parameters since Regev's results based on Banaszczyk's lemma makes it possible to reach the same conclusions with the new values as with the original ones. (c) a simplified way of representing the encrypted text, by representing each point x in $\mathbf{R}^n$ by an $x' \in \mathcal{P}(a_1,...,a_n)$ with the property $x - x' \in L^*$, where $a_1,...,a_n$ is a basis of L^*, instead of taking x from a large cube. This improvement was introduced by Micciancio in [11]. Later we will describe a further improvement on the method of encryption introduced by Goldreich, Goldwasser, and Halevi in [5], but first we describe the system with the encryption method used in [2].

The participants of the cryptosystem share the following information. (i) An integer n which is the dimension of the lattices used by the cryptosystem, the constants $c = \frac{1}{2} + \varepsilon' > \frac{1}{2}$ and $\beta > 0$. (ii) A random sequence of integers b which altogether contains no more then $O(n^2 \log n)$ bits and which is chosen according to a distribution that we describe later. (iii) A deterministic polynomial time algorithm $\mathcal{B}$ which, if b and a sequence of integers t are given as input, computes a basis $B(b,t)$ of a lattice $L(b,t)$. (iv) A probabilistic polynomial time algorithm $\mathcal{D}$ which given b as an input generates t and u, where t is a random sequence of integers (with the distribution determined by $\mathcal{D}$) so that the total number of bits in t is $O(n \log n)$ and, with a probability exponentially close to 1, u is an n^c-unique sh.n.v. of $L(b,t)$ with $(n-1)^{\frac{1}{2}-\beta-\varepsilon'} \leq \|u\| \leq 2(n-1)^{\frac{1}{2}-\beta}$, where the probability is taken for the randomization of t only while b is considered as fixed. Moreover if our Hardness Assumption holds (we will describe it later), then there is no polynomial time probabilistic algorithm which finds a sh.n.v. in $L(b,t)$ with polynomially large probability, with respect to the same randomization and the random steps of the algorithm together.

Sometimes it will be more convenient to consider instead of the lattice $L(b,t)$ a normalized version of it. Assume that a a constant $\varepsilon > 0$ is fixed with $\varepsilon' < \frac{1}{12}\varepsilon$. The normalized version of $L(t,b)$ will the lattice $\tilde{L}(b,t) = n^{-(\frac{1}{2}-\beta)-\frac{\varepsilon}{3}} L(b,t)$. If $\tilde{u}$ is a shortest nonzero vector in $\tilde{L}(b,t)$ then $n^{-\frac{\varepsilon}{2}} \leq \|\tilde{u}\| \leq n^{-\frac{\varepsilon}{3}}$.

Remark 1.3. 1. We are not able to guarantee that the algorithm $\mathcal{D}$ satisfies property (iv) with an arbitrarily chosen fixed b. Still we will show that (iii) holds with a probability exponentially close to 1 for the randomization of b.

2. If b is computed by a pseudo random number generator, then the proof of security (based on the Hardness Assumption) breaks down, since a potential attacker knows the seed of this generator. Indeed the pseudo random generator provides a b so that for all polynomial time test T, if $T(b')=1$ with high probability for a random b', then $T(b)=1$ with high probability with the pseudo random b as well. (This guarantees that everything that we can prove about a random b' will also hold for the pseudo random b.) However, by the definition of a pseudo random number generator, the test T has this property only if the seed of the pseudo random number generator is not available for it. In other words, for an attacker who knows the seed, the sequences b will not look like a random sequence, so he may be able to utilize some of its non-random properties.

In spite of these potential dangers of a pseudo random b, it seems that if we use, for example, the binary bits of π as b, perhaps we do not increase the risk of failure too much.

The sequence b and the algorithms $\mathcal{B}$, and $\mathcal{D}$ must be known for all of the participants of the system. We may assume that e.g. they are all part of the software implementing the system. Assume now that all of the participants are already in the possession of the sequence b and the algorithms $\mathcal{B}$ and $\mathcal{D}$. Under these circumstances the selection of the public keys and encryption/decryption of the messages is done in the following way.

Selection of the public key. The participant A of the system generates a random t_A together with a sh.n.v. u in $L(b,t_A)$ using algorithm $\mathcal{D}$. The public key is t_A. The private key is u.

Encryption. To encrypt a 0,1-bit x, to be sent to A, the following steps are needed. (a) Determine $f_1,...,f_n$, the dual of $B(b,t)$. This is a basis of the lattice L^*. (b) if $x=0$ then let y be a random point chosen from the parallelepiped $\mathcal{P}(f_1,...,f_n)$ with uniform distribution. If $x=1$ then compute a random point z in $\mathbf{R}^n$ with the normal distribution whose density function is $e^{-\pi\|x\|^2}$ for $x\in\mathbf{R}^n$, and determine the unique element y of the parallelepiped $\mathcal{P}(f_1,...,f_n)$ so that $y-z\in L^*$. Find a rational approximation $\bar{y}_i$ of each coefficient of the vector $y=\langle y_1,...,y_n\rangle$ so that the denominator of $\bar{y}_i$ is n and $|y_i-\bar{y}_i|<\frac{1}{n}$. The vector $\bar{y}=\langle\bar{y}_1,...,\bar{y}_n\rangle$ is the encrypted message.

Decryption. A determines the inner product $\alpha=\bar{y}u$ and the closest integer k_α to α. If $|\alpha-k_\alpha|\geq\tilde{c}(\log n)^{\frac{1}{2}}$ then $x=0$ otherwise $x=1$, where $\tilde{c}$ is a large constant.

We will call the described public key cryptosystem System I. Its method of encryption has the disadvantage that with a probability of $p=2\tilde{c}(\log n)^{\frac{1}{2}}\|u\|$ the decryption may be wrong. Since $n^{-\frac{\varepsilon}{2}}\leq\|u\|\leq n^{-\frac{\varepsilon}{3}}$, p may be about $2\tilde{c}(\log n)^{\frac{1}{2}}n^{-\frac{\varepsilon}{3}}$. Indeed if $x=0$ then it may happen with a probability of $2\tilde{c}(\log n)^{\frac{1}{2}}\|u\|$that the point y chosen with uniform distribution from $\mathcal{P}$ is closer than $\tilde{c}(\log n)^{\frac{1}{2}}$ to a hyperplane $\{w\in\mathbf{R}^n\mid wu=k\}$ where $k\in\mathbf{Z}$. (The distance of neighboring hyperplanes of this type is $\|u\|^{-1}$). In this case the message $\bar{y}$ will be decrypted as 1. The probability of an error of the other type when a bit 1 is decrypted as a 0 is less than $n^{-c'}$, where c' is about $\tilde{c}^2$. Therefore with the right choice of $\tilde{c}$ we can make this probability less than polynomial.

An improved way of encryption, introduced by Goldreich, Goldwasser, and Halevi in [5] eliminates the described error. (Alternatively we may use error correcting codes, but this makes the system less efficient in terms of the lengths of the messages and the computational time.) Their solution is the following. Assume that u is an α-unique sh.n.v. in L where $\alpha>1$. The bit $x=0$ is represented by a perturbation $y=a+z$ of a lattice point $a\in L^*$, so that the inner product au is even, while for $x=1$, au is odd. More precisely the new protocol will be the following:

Selection of the public key. The participant A of the system generates a random t_A together with a sh.n.v. u in $L(b,t_A)$ using algorithm $\mathcal{D}$. The public key is a pair $\langle t_A, j_A\rangle$, where $j_A \in \{1,...,n\}$ so that if $f_1,...,f_n$ is the dual of the basis $B(b,t)$ then $f_{j_A}u$ is odd. The private key is u.

Encryption. To encrypt a 0,1-bit x, to be sent to A, the following steps are needed. (a) Determine $f_1,...,f_n$, the dual of $B(b,t)$. This is a basis of the lattice L^*. (b) if $x=0$ let $s=0\in\mathbf{R}^n$ if $x=1$ then let $s=f_{j_A}$. Compute a random point z in $\mathbf{R}^n$ with the normal distribution whose density function is $e^{-\pi\|w\|^2}$ for $w\in\mathbf{R}^n$, and determine the unique element y of the parallelepiped $\mathcal{P}(2f_1,...,2f_n)$ so that $y-(s+z)\in 2L^*$. Find a rational approximation $\bar{y}_i$ of each coefficient of the vector $y=\langle y_1,...,y_n\rangle$ so that the denominator of $\bar{y}_i$ is n and $|y_i-\bar{y}_i|<\frac{1}{n}$. The vector $\bar{y}=\langle\bar{y}_1,...,\bar{y}_n\rangle$ is the encrypted message.

Decryption. A determines the inner product $\alpha=\bar{y}u$. Let k_α be the closest integer to α. If k_α is even then $x=0$ otherwise $x=1$.

We will call this public key cryptosystem System II.

1.4 The values of the efficiency parameters

From the point of view of efficiency the most important parameters are the size of the public key and the ratio between the length of the encrypted text and the clear text. For encrypting a bit, the new system requires almost exactly the same computation than the Ajtai-Dwork cryptosystem or its variants with the various improvements, so we do not discuss this question here. We only note that from the point of view of practical implementations, this is the least problematic part of the systems.

The size of the public key. Both System I and System II has keys of length $O(n\log n)$.

The length of the encrypted message. The length of the encrypted messages in System I and System II are about the same and can be estimated in an identical way. The encrypted message is a point of the parallelepiped $\mathcal{P}=\mathcal{P}(f_1,...,f_n)$ ($\mathcal{P}(2f_1,...,2f_n)$ for System II) whose components are approximated by a precision of $\frac{1}{n}$. Therefore the total number of bits in the encrypted message depends on the lengths of the vectors in $\mathcal{P}$. Our construction will imply that each element of the basis $B(b,t)$ is of polynomial length. Unfortunately this does not imply that the lengths of the vectors in the dual basis also have a polynomial upper bound. However the special structure of the basis $B(b,t)$ will imply that there is a constant $\bar{c}$ so that for each i, if $f_i=\langle\varphi_1^{(i)},...,\varphi_n^{(i)}\rangle$ then $|\varphi_j^{(i)}|\le n^{\bar{c}}$ for $j=1,...,n-1$ and $|\varphi_n^{(i)}|\le n^{\bar{c}n}$. Consequently if $y=\langle y_1,...,y_n\rangle$ is a point of $\mathcal{P}$ then for all $j=1,...,n-1$, we have $|y_j|\le n^{\bar{c}+1}$ and $|y_n|\le n^{\bar{c}n+1}$. Therefore if $\bar{y}_i=\frac{z_i}{n}$, and we represent $\bar{y}_i$ by the binary form of the integer z_i then for each fixed $j=1,...,n-1$ the number of bits used is at most $(\bar{c}+1)\lceil\log_2 n\rceil+1$ bits, while for $j=n$ we need at most $(\bar{c}n+1)\lceil\log_2 n\rceil+1$ bits. This implies that the vector $\bar{y}$ can be encoded with at most $O(n\log n)$ bits.

The size of the keys in other lattice based cryptosystems. In all of the cryptosystems where the public key is a lattice presented by an arbitrary basis, the number of bits in the key must be at least $\Omega(n^2\log n)$. Indeed there are altogether n^2 coefficients of the n basis vectors and the way we use an n^c-unique shortest vector for decoding implies that these numbers must have at least $\Omega(\log n)$ bits. In this paper we save on the number of bits by presenting the lattice with a basis of special structure where the randomization of the coefficients can be done in two stages as mentioned earlier. The public-key systems based on the worst-case hardness of the n^c-unique sh.n.v. problem, the third Ajtai-Dwork cryptosystem and Regev's cryptosystem use a set of points in $\mathbf{R}^n$ resp. $\mathbf{R}$ as public keys. The total number of bits on both cases is

$O(n^4)$.

The improvement in the size of the public keys was possible because the participants share $O(n^2\log n)$ random bits. This idea does not seem to be applicable to the other mentioned cryptosystems. We need the specific properties of the lattices, that we use in the cryptosystem presented in this paper, for cutting the randomization into two part. It is not clear whether there is any analogue process in the case of the other systems.

1.5 Lattice based cryptosystems of other types

There are other possibilities to construct lattices with cryptographic applications which can be represented by relatively few bits. Micciancio proved a worst-case average-case connection for cyclic lattices (see [12]) which leads to a one-way function with $O(n\log n)$ key-size. For a description of the advantages and disadvantages of cyclic versus general lattices see [12]. Another lattice based system with small key-size is the commercial system NTRU (see [8]). The security of the cryptographic tools provided by either cyclic lattices or NTRU is not reduced to the hardness of an algorithmic problem in a well studied area of mathematics (like our hardness assumption.) On the other hand our approach, unlike the mentioned applications based on cyclic lattices does not have a worst-case average-case connection.

2 The Hardness Assumption

First we formulate the diophantine approximation problem that we will call our Hardness Assumption, and then we will describe the way of generating the lattices which will serve as keys in the public key system.

The following well-known theorem was proved by Dirichlet in 1842 (see [15]).

Theorem A (Dirichlet) *If $\alpha_1,\dots,\alpha_n$ are realnumbers in the interval $(0,1)$ and $M>0$ is an integer, then there is an integer $m\in[1,M^n]$ so that for all $i=1,\dots,n$ we have $[\![m\alpha_i]\!]\le\frac{1}{M}$.*

The theorem holds even if M is not necessarily an integer (see [15]). The proof is an application of the pigeonhole principle, and so it does not give an efficient way to find an integer m with the described property. We will be interested in algorithmic questions related to this theorem. Namely, we will be concerned with the case when $M=n^{c_1}$ and a positive integer m exists so that for all $i=1,\dots,n$, $[\![m\alpha_i]\!]\le n^{-c_2}M^{-1}$, where $c_1>0,c_2>0$ are constants and n is sufficiently large. Our hardness assumption will state that even if the numbers $\alpha_1,\dots,\alpha_n$ are chosen at random with the condition that there is such an m, still there is no efficient algorithm for finding the integer m.

Hardness Assumption. *For all $c>0,c'>0$, $c_1>0,c_2>0$ and for all probabilistic algorithms $\mathcal{A}$ the following holds: if n is sufficiently large and $\mathcal{A}$ provides an output in time n^{c_1} then the probability that $\mathcal{A}$ solves Problem* **Q1** *formulated below is smaller than n^{-c_2}, where the probability is taken both for the random steps of $\mathcal{A}$ and the randomization in the formulation of the input.*

Problem **Q1**. *Assume that $\alpha_1,\dots,\alpha_n$ are picked at random, independently, and with uniform distribution from the interval $(0,1)$ with the condition that there is an integer m so that*

(1). $1\le m\le n^{cn}$ and $[\![m\alpha_i]\!]\le n^{-c-c'}$ for $i=1,\dots,n$

Given $n,\alpha_1,\dots,\alpha_n,c,c'$ as input, find an integer m with property (1).

Remark 2.1. 3. As we will show later the distribution of the realnumbers $\alpha_1,...,\alpha_n$ described in Problem **Q1** can be generated in polynomial time, together with an integer m satisfying (1). (More precisely we generate an approximation of this distribution with exponentially small error, and, of course, we generate only a polynomial number of bits from the reals $\alpha_1,...,\alpha_n$.)

4. The assumption that problem **Q1** is hard in the described sense seems reasonable, since in the last one and a half century, after Dirichlet formulated and proved Theorem **A**, the problem of diophantine approximation was intensively studied in the framework that was created by this and similar theorems formulated due to Dirichlet. The best known algorithm for finding an approximate solution for this type of problems is the L^3 algorithm given by A. K. Lenstra, H. W. Lenstra, L. Lovász in [9] which approximates the shortest nonzero vector in a lattice up to an exponentially large factor. (For improvements on the original algorithm see [16] and [3].) To solve Problem **Q1** by lattice algorithms in a similar sense we would need a polynomial approximating factor. Of course it is possible that the formulated average case problem is easier than the worst-case lattice problem for approximating a shortest nonzero vector by a polynomial factor. Still, the long history of diophantine approximation problems suggests that it is very unlikely that an efficient solution will be found for Problem **Q1**.

3 The statement of the results

3.1 The distribution and encoding of the lattices used as public keys

In the definitions below we describe a way to choose b and t at random with the properties necessary for the security of the described cryptosystem.

The random construction will depend on three constants $\beta > 0$, $\xi > 0$, and $\gamma > \beta + \xi + 2$. We will prove our theorems under the additional condition $\beta - \frac{1}{2} > \xi$. The lattice generated with parameters ξ, β will have an $n^{\beta-\xi-\frac{1}{2}-\varepsilon}$-unique nonzero shortest vector with high probability and the hardness of the lattice will follow from our Hardness Assumption with parameters $c = \xi$ and $c' = \beta - \xi$. For the cryptographic protocol we need a lattice with an $n^{\frac{1}{2}+\varepsilon}$-unique sh.n.v. therefore we have to pick the parameters β, ξ with $\beta - 1 - 2\varepsilon > \xi$. The number of bits needed to represent a lattice will be $\lceil \gamma n \log_2 n \rceil$.

First we define a random variable κ whose value is a lattice L and another random variable $\bar{\kappa}$ whose value is a pair $\langle L, u \rangle$ where L is a lattice (with the same distribution as in κ) and $u \in L$. When defining κ we do not specify any representation of the lattice. Our next step will be to show that the lattices which are the values of κ can be represented by two sequences of integers $b = \langle b_1,...,b_{n-1} \rangle$ and $t = \langle t_1,...,t_{n-1} \rangle$, and the randomization can be performed in two stages first picking the sequence b and then the sequence t. After that we will formulate two theorems which say that this way of choosing a random lattice and a vector u in it has the properties described earlier which make it suitable for generating the public and private keys in the cryptosystem.

Definition 3.1. • Suppose that $X_i \subseteq \mathbf{R}$ for $i = 1,...,n$. $\prod_{i=1}^n X_i$ is the set of all $\langle x_1,...,x_n \rangle \in \mathbf{R}^n$ with $x_i \in X_i$ for $i = 1,...,n$. If $X \subseteq \mathbf{R}^n$ and α is a realnumber then $\alpha X = \{\alpha x \mid x \in X\}$.

• Suppose that $\lambda > 0$ is a realnumber. $\mathbf{I}_n(\lambda)$ will denote the set $\{\langle x_1,...,x_n \rangle \in \mathbf{R}^n \mid [\![x_i]\!] \leq \lambda, i = 1,...,n\}$

• If k is a positive integer then $\mathtt{part}_n(k)$ will denote the partition of the unit cube $[0,1)^n$ into subcubes of the form $\prod_{i=1}^n [\frac{b_i}{k}, \frac{b_i+1}{k})$ where $b_1,...,b_n$ are integers with $0 \leq b_i < k$. We will use the

notation $\mathcal{Q}_k(b_1,...,b_n) = \prod_{i=1}^{n}[\frac{b_i}{k}, \frac{b_i+1}{k})$.

The motivation for the definition of the random variable κ. Assume that the realnumbers $\alpha_1,...,\alpha_{n-1}$ are picked at random, independently, with uniform distribution from $(0,1)$, and with the condition that there is an integer $d \in [1,(n-1)^{\xi(n-1)}]$ with $[\![d\alpha_i]\!] \leq (n-1)^{-\beta}$ for $i = 1,...,n-1$, where $\beta > 0, \xi > 0$ are constants and $\beta > \xi$. Our Hardness Assumption, with $n \to n-1$, $c \to \xi$, $c' \to \beta - \xi$ implies that a polynomial time algorithm cannot find such an integer d with a polynomially large probability. We want to construct a lattice L depending on $\alpha_1,...,\alpha_{n-1}$ so that it contains an $n^{c''}$-unique sh.n.v. u, for some constant $c'' > 0$, and in the knowledge of u it is possible to find d in polynomial time. For the moment we will work with vectors with real coefficients and disregard the problem of rounding. The basis of L will be of the form $e_1,...,e_{n-1},v$ where

$$v = \rho e_n + \sum_{i=1}^{n-1} \alpha_i e_i$$

(the realnumber $\rho > 0$ will be defined later.) Assume now that an integer $d \in [1,(n-1)^{\xi(n-1)}]$ is given with $[\![d\alpha_i]\!] \leq n^{-\beta}$. Then we have $dv = d\rho e_n + \sum_{i=1}^{n-1} [\![d\alpha_i]\!] e_i + \sum_{i=1}^{n-1} a_i e_i$, where $a_1,...,a_{n-1}$ are integers. Therefore, if $\rho d \leq (n-1)^{-\beta}$ then we have $\|u\|_\infty \leq n^{-\beta}$ where $u = dv - \sum_{i=1}^{n-1} a_i e_i$. To meet this requirement we define ρ by $\rho = (n-1)^{-\xi(n-1)-\beta}$. At this point we know only that u is a short vector with respect to the ℓ_∞ norm (and if $\beta > \frac{1}{2}$ then with respect to the Euclidean norm as well). To show the $n^{c''}$-uniqueness of u for some constant $c'' > 0$ we will investigate the following question. Suppose that we randomize $\alpha_1,...,\alpha_{n-1}$ as described above. It is possible that with a nonnegligible probability there is an integer $d' \neq d$, $d' \in [1,(n-1)^{\xi(n-1)}]$ so that $d'[\![\alpha]\!] \leq (n-1)^{-\xi(n-1)-c_1}$ for some constant $c_1 > 0$. Without further restrictions on d' this really can happen e.g. with $d' = 2d$. However if we exclude these type of solutions, which in the lattice would lead only to a short vector parallel to u, then the answer is that with a probability exponentially close to 1 there is no d' with this property. The exact formulation of this and some related statements are given in Lemma 5.1, Lemma 4.2, and Lemma 4.3. These lemmata imply that u is indeed an $n^{c''}$-unique sh.n.v. with high probability. Clearly in the knowledge of u we can find d since $u = dv - \sum_{i=1}^{n-1} a_i e_i$ and $v, e_1,...,e_{n-1}$ are linearly independent.

Our next step is to show that this randomization of the lattice L with the basis $e_1,...,e_{n-1},v$ can be generated together with the vector u in L. It is easy to see that this is equivalent of saying that the randomization of the reals $\alpha_1,...,\alpha_{n-1}$ as defined above can be done together with randomizing a d. We prove this by showing, that with high probability, the integer d, with the given inequalities is unique, moreover we get the different possible integers d with about the same probability. With a slightly stronger statement, formulated in Lemma 5.1, it is possible to show that if we pick first d with uniform distribution from the integers of $[1,(n-1)^{\xi(n-1)}]$ and then $\alpha_1,...,\alpha_{n-1}$ with the condition $[\![d\alpha_i]\!] \leq (n-1)^{-\beta}$, then we get essentially the same distribution. (See Lemma 4.2.) This randomization yields the vector u while we randomize the lattice. To make the proof simpler we will pick the integer d from the interval $[\frac{1}{2}(n-1)^{\xi(n-1)}, (n-1)^{\xi(n-1)}]$ (this change in the distribution does not affect our conclusions).

Finally we show how can we cut the randomization in two parts randomizing first b and then t. The vector $\alpha_1,...,\alpha_{n-1}$ is in the unit cube $[0,1)^{n-1}$. First we pick a $Q \in \mathtt{part}_{n-1}(k)$ with uniform distribution where $k = \lfloor (n-1)^{\xi(n-1)-1} \rfloor$ and then we pick $\langle \alpha_1,...,\alpha_{n-1} \rangle \in Q$ with the condition $\exists d \in [1,(n-1)^{\xi(n-1)}] \forall i, [\![d\alpha_i]\!] \leq (n-1)^{-\beta}$. Of course this is a different distribution from the original one since we take into account the condition only in the second part of the randomization. However the choice

n	is the dimension of the lattice
β, γ, ξ	$\beta, \gamma, \xi > 0$, $\gamma > \beta + \xi + 2$, $\beta > \xi + \frac{1}{2}$
ξ, β	determine the parameters in the Hardness Assumption
	$c = \xi$, $c' = \beta - \xi$
γ	determines the precision of rounding
k	$= \lfloor (n-1)^{\xi(n-1)-1} \rfloor$, we cut each side of the cube Q into k intervals
Q	$= \prod_{i=1}^{n-1} [\frac{b_i}{k}, \frac{b_i+1}{k})$
d	is a random integer in $[\frac{1}{2}(n-1)^{-\xi(n-1)}, (n-1)^{-\xi(n-1)}]$
q	is a random point in $\mathbf{I}_{n-1}((n-1)^{-\beta}) \cap dQ$
v	$= (n-1)^{-\xi(n-1)-\beta} e_n + \sum_{i=1}^{n-1} \mathtt{fr}(\frac{q_i}{d}, kn^{\gamma}) e_i$
L	is the lattice generated by $e_1, ..., e_{n-1}, v$
u	$= dv + \sum_{i=1}^{n} a_i e_i$, $[\![u_i]\!] \leq (n-1)^{-\beta}$
	u is an $n^{\beta-\xi-\frac{1}{2}-\varepsilon}$-unique shortest nonzero vector in L

Table 1: *Frequently ocurring objects in the definition of the lattice L.*

of k will imply that for each fixed d the probability that $\alpha_1, ..., \alpha_{n-1}$ satisfies the conditions with this fixed d is independent of Q (at least up to a constant factor in the probability). This implies that in the new randomizations the probability of the events change by at most a constant factor which is acceptable for our purposes. Therefore b will be the random Q, and t will be the sequence $\alpha_1, ..., \alpha_{n-1}$ picked by the conditional distribution. As we have seen this can be generated by picking first d, (which will be denoted by d in the final definition), and then $\alpha_1, ..., \alpha_{n-1}$. Finally to get a finite number of bits we have to round the numbers α_i. The parameter controlling the precision of the rounding will be the constant $\gamma > 0$.

The construction of the lattice L depends on several parameters and also during the construction we use various realnumbers and vectors that are defined (sometimes in a probabilistic sense only) as a function of these parameters. Since all of these reals and vectors will appear repeatedly throughout the definitions and proofs we summarize in Table 1 their most important characteristics. (We have included some inequalities that will have a significance only in our theorems.) These are not definitions, the definitions will be given separately. Table 1 serves only as a reminder.

Definition 3.2. • Suppose that $n \geq 3$, is an integer $\xi > 0$, $\beta > 0$, $\gamma > 0$ are realnumbers, $k = \lfloor (n-1)^{\xi(n-1)-1} \rfloor$ and $Q \in \mathtt{part}_{n-1}(k)$. We define a random variable $\kappa = \kappa_{n,Q}(\xi, \beta, \gamma)$ whose each value is a lattice $L \subseteq \mathbf{R}^n$. First we pick an integer d at random, with uniform distribution from the set of all integers in the interval $[\frac{1}{2}(n-1)^{\xi(n-1)}, (n-1)^{\xi(n-1)}]$. Then we choose a point $q = \langle q_1, ..., q_{n-1} \rangle \in \mathbf{R}^{n-1}$ with uniform distribution from the set $\mathbf{I}_{n-1}((n-1)^{-\beta}) \cap dQ$. The lattice L is generated by the vectors $e_1, ..., e_{n-1}, v$, where

$$v = (n-1)^{-\xi(n-1)-\beta} e_n + \sum_{i=1}^{n-1} \mathtt{fr}(\frac{q_i}{d}, kn^{\gamma}) e_i$$

Figure 1 illustrates the position of the vector v with respect to the intervals $[\frac{b_i}{k}, \frac{b_i+1}{k}]$ on the ith axis of the coordinate system.

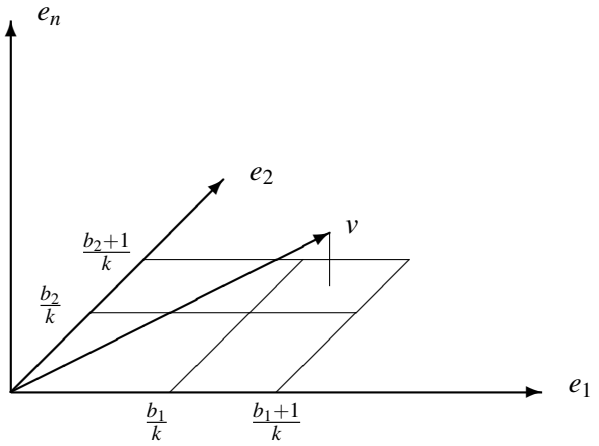

Figure 1: The orthogonal projection of the vector v to the $n-1$ dimensional subspace generated by $e_1,...,e_{n-1}$ is in a cube whose each side is of length $\frac{1}{k}$. We achieve the savings in the number of bits representing the lattice, by restricting the projection of v to this small cube.

- We define a random variable $\bar{\kappa}_{Q,n}(\xi,\beta,\gamma)$. First we pick a lattice L according to distribution $\kappa_{Q,n}(\xi,\beta,\gamma)$. Assume that L is a value of the random variable and d is the integer and v is the basis vector chosen during the randomization of L. We choose the integers $a_1,...,a_{n-1}$ so that $-\frac{1}{2} \le e_i(dv-\sum_{i=1}^{n-1} a_i e_i) < \frac{1}{2}$ for $i=1,...,n-1$. The value of the random variable $\bar{\kappa}_{Q,n}(\xi,\beta,\gamma)$ is the pair $\langle L,u\rangle$ where $u = dv-\sum_{i=1}^{n-1} a_i e_i$.

Remark 3.3. 5. The definition of κ and $\bar{\kappa}$ imply that with high probability $\|u\|_\infty \le (n-1)^{-\beta}$. (The probability is not 1 because of the rounding involved in the definition of v, that is, the substitution of $\frac{q_i}{d}$ by $\mathtt{fr}(\frac{q_i}{d_i},kn^\gamma)$.) As we will show later, under some conditions on the parameters involved, with high probability, u is a shortest nonzero vector of the lattice L.

Lemma 3.4. *Suppose that $n \ge 3$ is an integer, $\xi > 0$, $\beta > 0$, $\gamma > 0$ are realnumbers, $k = \lfloor (n-1)^{\xi(n-1)-1} \rfloor$, $b_1,...,b_{n-1} \in [0,k-1]$ are integers, $Q = \mathcal{Q}_k(b_1,...,b_{n-1})$, L is a random value of $\kappa_{n,Q}(\xi,\beta,\gamma)$, L is generated by $e_1,...,e_{n-1}$, and*

$$v = (n-1)^{-\xi(n-1)-\beta} e_n + \sum_{i=1}^{n-1} \mathtt{fr}(\frac{q_i}{d},kn^\gamma) e_i$$

where d,q_i were selected as described in the definition of κ.

Then v can be written in the form

$$v = (n-1)^{-\xi(n-1)-\beta} e_n + \sum_{i=1}^{n-1} (\frac{b_i}{k} + \frac{t_i}{kn^\gamma}) e_i$$

where t_i is an integer and $0 \le t_i < n^\gamma$. Moreover the integers t_i with the stated conditions are uniquely determined by the lattice L. Consequently if n,ξ,β,γ and $Q = \mathcal{Q}_k(b_1,...,b_{n-1})$ are fixed, then every value L of the random variable $\kappa_{n,Q}(\xi,\beta,\gamma)$ has a unique representation by at most $n\lceil \gamma \log_2 n \rceil$ bits.

Proof. By definition we have that $\langle q_1,...,q_{n-1}\rangle \in dQ = d\prod_{i=1}^{n-1}[\frac{b_i}{k},\frac{b_i+1}{k})$. Therefore $\frac{q_i}{d} \in [\frac{b_i}{k},\frac{b_i+1}{k}) = [\frac{b_i n^\gamma}{kn^\gamma},\frac{(b_i+1)n^\gamma}{kn^\gamma})$ for all $i=1,...,n$. Consequently the definition of $\mathtt{fr}(\frac{q_i}{d},kn^\gamma)$ implies that $\mathtt{fr}(\frac{q_i}{d},kn^\gamma) = \frac{b_i n^\gamma}{kn^\gamma}+\frac{t_i}{kn^\gamma}$ for a suitably chosen integer t_i in the interval $[0,n^\gamma)$.

To prove the uniqueness of the sequence $t_1,...,t_{n-1}$ assume that $t_1^{(j)},...,t_{n-1}^{(j)}$, $j=1,2$ are sequences of integers so that both for $j=1$ and for $j=2$, $e_1,...,e_{n-1}$, $v^{(j)} = (n-1)^{-\xi(n-1)-\beta}e_n + \sum_{i=1}^{n-1}(\frac{b_i}{k}+\frac{t_i^{(j)}}{kn^\gamma})e_i$ is a basis of L and $0 \le t_i < n^\gamma$. This implies that $v^{(1)}-v^{(2)} = \sum_{i=1}^{n-1}\frac{t_i^{(1)}-t_i^{(2)}}{kn^\gamma}e_i$ is an element of L and therefore $\frac{t_i^{(1)}-t_i^{(2)}}{kn^\gamma}$ are integers for $i=1,...,n-1$. Since $k>1$ and $0 \le t_i^{(j)} < n^\gamma$, this implies $t_i^{(1)} = t_i^{(2)}$. The lattice L can be represented by the binary bits of the nonnegative integers t_i. Everything else in the basis $e_1,...,e_{n-1}$, v depends only on parameters whose values has been fixed. (Lemma 3.4)■

Definition 3.5. • Suppose that n,Q,ξ,β,γ, satisfy the conditions of the definition of $\kappa_{n,Q}(\xi,\beta,\gamma)$. We define a random variable $\tau_{n,Q}(\xi,\beta,\gamma)$ in the following way. First we pick a lattice L with distribution $\kappa_{n,Q}(\xi,\beta,\gamma)$. As we have seen in Lemma 3.4 the lattice L uniquely determines the sequence of integers $t_1,...,t_{n-1}$ so that $0 \le t_i < n^\gamma$ and $e_1,...,e_{n-1}$, $(n-1)^{-\xi(n-1)-\beta}e_n + \sum_{i=1}^{n-1}(\frac{b_i}{k}+\frac{t_i}{kn^\gamma})e_i$ is a basis of L. The sequence $\langle t_1,...,t_{n-1}\rangle$ is the value of $\tau_{n,Q}(\xi,\beta,\gamma)$. If $t_1,...,t_{n-1}$ are given then the corresponding lattice L will be denoted by $\mathcal{L}(t_1,...,t_{n-1},b_1,...,b_{n-1},\xi,\beta,\gamma)$. With our earlier notation if ξ,β and γ are fixed, $b=\langle b_1,...,b_{n-1}\rangle$, $t=\langle t_1,...,t_{n-1}\rangle$ then $L(b,t) = \mathcal{L}(t_1,...,t_{n-1},b_1,...,b_{n-1},\xi,\beta,\gamma)$

• We define a random variable $\bar\tau_{Q,n}(\xi,\beta,\gamma)$. First we take a random value $\langle L,u\rangle$ of $\bar\kappa_{Q,n}(\xi,\beta,\gamma)$. From the lattice L we define the sequence of integers $t_1,...,t_{n-1}$ the same way as in the definition of $\tau_{Q,n}(\xi,\beta,\gamma)$. The value of the random variable is the pair $\langle\langle t_1,...,t_{n-1}\rangle,u\rangle$.

Remark 3.6. 6. The only difference between $\kappa,\bar\kappa$ on one hand and $\tau,\bar\tau$ on the other hand is that the values of $\tau,\bar\tau$ give the lattice L a representation by 0,1 bits namely the bits of the integers $t_1,...,t_{n-1}$. Therefore from a computational point of view the use of τ and $\bar\tau$ are more appropriate.

7. It is an immediate consequence of the definitions that if the pair $\langle\langle t_1,...,t_{n-1}\rangle,u\rangle$ is chosen with distribution $\bar\tau_{Q,n}(\xi,\beta,\gamma)$, then the distribution of $t_1,...,t_{n-1}$ is $\tau_{Q,n}(\xi,\beta,\gamma)$. The analogue of this observation holds for the random variables $\kappa,\bar\kappa$ as well.

Lemma 3.7. *There is a $c>0$ and a probabilistic algorithm $\mathcal{F}$ with the following properties. Suppose that $n\ge 3$ is an integer, $\xi>0$, $\beta>0$, $\gamma>0$ are realnumbers, $k=\lfloor(n-1)^{\xi(n-1)-1}\rfloor$, $b_1,...,b_{n-1}\in[0,k-1]$ are integers, $Q=\mathcal{Q}_k(b_1,...,b_{n-1})$. Given $n,\xi,\beta,\gamma,b_1,...,b_{n-1}$ as input, $\mathcal{F}$ generates in time n^c a random variable τ' so that the distance of the distributions of τ' and $\bar\tau_{Q,n}(\xi,\beta,\gamma)$ is at most 2^{-n}.*

The lemma is an immediate consequence of the definition of $\bar\tau$. $\mathcal{F}$ does not generate $\bar\tau$ exactly because of the rounding errors. 2^{-n} can be replaced by $2^{-n^{c'}}$ for any constants $c'>0$, if c may depend on c'.

Theorem 3.8. *For all realnumbers $\vartheta > \frac{1}{2}$ and for all realnumbers $\gamma,\beta,\xi>0$ with $\gamma > \beta+\xi+2$, $\beta > \xi+\frac{1}{2}$ and for all sufficiently small $\varepsilon>0,\varepsilon'>0$, if n is sufficiently large then the following holds. Suppose that $\langle b_1,...,b_{n-1}\rangle$ is a random sequence of positive integers taken independently and with uniform distribution from the interval $[0,k)$, where $k=\lfloor(n-1)^{\xi(n-1)-1}\rfloor$, and the sequence $\langle t_1,...,t_{n-1}\rangle$ is picked at random according to distribution $\tau_{Q,n}(\xi,\beta,\gamma)$, where $Q=\mathcal{Q}_k(b_1,...,b_{n-1})$. Then, with a probability of at least $1-\vartheta^n$, the lattice $L=\mathcal{L}(t_1,...,t_{n-1},b_1,...,b_{n-1},\xi,\beta,\gamma)$ has an $n^{\beta-\xi-\frac{1}{2}-\varepsilon}$-unique shortest*

nonzero vector. Moreover, if $\langle\langle t_1,...,t_{n-1}\rangle,u\rangle$ is a random value of $\bar{\tau}_{Q,n}(\xi,\beta,\gamma)$, then $t_1,...,t_{n-1}$ has the same distribution as $\tau_{Q,n}(\xi,\beta,\gamma)$, and with a probability of at least $1-\vartheta^n$ the vector u is a shortest nonzero vector in $L=\mathcal{L}(t_1,...,t_{n-1},b_1,...,b_{n-1},\xi,\beta,\gamma)$, with

(2). $(n-1)^{\frac{1}{2}-\beta-\varepsilon'} \le \|u\| \le 2(n-1)^{\frac{1}{2}-\beta}$

and the upper bound in the last inequality holds with probability 1.

Theorem 3.9. *The following statement is a consequence of the Hardness Assumption. For all realnumbers $\gamma>\beta>\xi>0$, with $\beta>\xi+\frac{1}{2}$, $\gamma>\beta+\xi+2$ for all $c_1>0,c_2>0$, and for all probabilistic algorithm $\mathcal{A}$ if n is sufficiently large and $\mathcal{A}$ gives an output in time n^{c_1}, then the probability that $\mathcal{A}$ solves the problem* **Q2** *formulated below is smaller than n^{-c_2}, where the probability is taken both for the random steps of the algorithm and for the randomization in the formulation of the problem.*

Problem **Q2**. *Assume that $\langle b_1,...,b_{n-1}\rangle$ is a random sequence of positive integers taken independently and with uniform distribution from the interval $[0,k)$, where $k=\lfloor(n-1)^{\xi(n-1)-1}\rfloor$. Suppose further the sequence of integers $\langle t_1,...,t_{n-1}\rangle$ is picked by distribution $\tau_{Q,n}(\xi,\beta,\gamma)$, where $Q=\mathcal{Q}_k(b_1,...,b_{n-1})$. Find a shortest nonzero vector in the lattice $L=\mathcal{L}(t_1,...,t_{n-1},b_1,...,b_{n-1},\xi,\beta,\gamma)$.*

Definition 3.10. • The normalized version of the lattice $L(b,t)$ is $\tilde{L}(b,t)$ defined by

$$\tilde{L}(b,t)=n^{-\frac{1}{2}+\beta-\frac{\varepsilon}{3}}L(b,t)$$

If we pick $\varepsilon'>0$ in Theorem 3.8 with $\varepsilon'<\frac{1}{12}\varepsilon$ then inequality (2) shows that the unique shortest nonzero vector $\tilde{u}$ in the lattice $\tilde{L}(b,t)=n^{-(\frac{1}{2}-\beta)-(\frac{\varepsilon}{3})}L(b,t)$ will meet the requirements $n^{-\frac{\varepsilon}{2}}\le\|\tilde{u}\|\le n^{-\frac{\varepsilon}{3}}$. $\tilde{B}(b,t)$ will be the basis $\nu e_1,....,\nu e_{n-1},\nu v$, where $\nu=n^{-\frac{1}{2}+\beta-\frac{\varepsilon}{3}}$ and $v=(n-1)^{-\xi(n-1)-\beta}e_n+\sum_{i=1}^{n-1}(\frac{b_i}{k}+\frac{t_i}{kn^\gamma})e_i$

Remark 3.11. 8. As we have seen, from the point of view of efficient encoding of the messages, the size of the coefficients in the dual basis of $B(b,t)$ is of great importance. We may use the following trivial lemma to estimate these coefficients.

Lemma 3.12. *Assume that $\vartheta_1,...,\vartheta_n$ are realnumbers and $\vartheta_n\neq 0$. Then $e_1,...,e_{n-1},\sum_{i=1}^n\vartheta_i e_i$ is a basis of $\mathbf{R}^n$ and if $f_1,...,f_n$ is the dual of this basis then $f_i=e_i-\frac{\vartheta_i}{\vartheta_n}e_n$ for $i=1,...,n-1$ and $f_n=\frac{1}{\vartheta_n}e_n$.*

Assume now that $\nu e_1,...,\nu e_{n-1},\nu\sum_{i=1}^n\vartheta_i e_i$ is the basis $\tilde{B}(b,t)$, where $\nu=n^{-\frac{1}{2}+\beta-\frac{\varepsilon}{3}}$. Then the coefficients $\vartheta_1,...,\vartheta_{n-1}$ are in the interval $[0,\nu]$ and $\vartheta_n^{-1}=O(\nu^{-1}2^{(\xi(n-1)+\beta)\log_2 n})$. Therefore the lemma implies that the coefficients in the dual basis $f_1,...,f_n$ remain below the bounds required for efficient encoding.

Finally we note that our theorems guarantee that for any fixed choice of the values parameters β,γ,ξ, satisfying the inequalities in the table above, if n is sufficiently large and the Hardness Assumption is true, then the corresponding cryptosystem is secure. Of course, this does not tell us anything about the choice of β,ξ,γ for a particular n. For an actual implementation when n is fixed, say $n=1000$, we must pick β and ξ in a way that the corresponding Diophantine approximation problem for this particular n cannot be solved in a reasonable amount of time. Our Hardness Assumption, being only an asymptotic statement,

does not help in this decision. Like in the case of other Hardness Assumption (e.g. about the hardness of factoring integers), apart from the asymptotic statement, we have to make a more or less arbitrary decision about the value of the parameters where the problem is already hard from a practical point of view. It seems likely that for $n \geq 1000$ the choices $\xi = 1$, $\beta = 3$, and $\gamma = 6$ meet these requirements.

3.2 The reduction of the security of the cryptosystem to the n^c-unique shortest vector problem.

The lattice $L(b,t)$, which is used as a public key in our cryptosystem was defined in two steps. First we randomized b and t according to a distribution described in the previous section and then as a function of b and t we have defined the lattice $L(b,t)$. For the results of this section the choice of distribution is not important we will only use the fact that there are constants $c > \frac{1}{2}$ and $\varepsilon \in (0, \frac{1}{4})$ so that for all sufficiently large n with a probability exponentially close to one the lattice $L = \tilde{L}(b,t) = n^{-(\frac{1}{2}-\beta)-\frac{\varepsilon}{3}} L(b,t)$ meets the following requirement.

(3). L has an n^c unique nonzero shortest vector u with the property $n^{-\frac{\varepsilon}{2}} \leq \|u\| \leq n^{-\frac{\varepsilon}{3}}$.

We will show that if an algorithm $\mathcal{A}$ breaks the crytposystem for a participant using a lattice L with property (3) as the public key, then using this algorithm as an oracle, we can find a nonzero shortest vector in L in polynomial time. Therefore in the same way as in the second cyptosystem of [2], our cryptosystem can be used with any distribution σ on the set of pairs of integers $\langle b,t \rangle$, provided that the lattice $\tilde{L}(b,t)$ is defined and satisfies condition (3) with high probability, and the average case shortest vector problem for the lattices $\tilde{L}(b,t)$, taken with this distribution, is hard. (As we have mentioned already earlier the proof of this fact is only slightly different from the corresponding proof in [2].) More precisely we have the following.

Theorem 3.13. *Supose that $c > \frac{1}{2}$, $\varepsilon \in (0, \frac{1}{4})$ and for each $n = 1, 2, ...$, σ_n is a distribution on pairs of integers $\langle b,t \rangle$ so that for all $c_2 > 0$ there is a $c_1 > 0$ with the following properties*

(i) with a probability of at least $1 - n^{-c_1}$ that lattice $L = \tilde{L}(b,t)$ is defined and satsifies condition (3) and

(ii) if $\mathcal{A}$ is a polynomial time algorithm then for all sufficiently large n with a probability of at least $1 - n^{c_1}$ the algorithm $\mathcal{A}$ does not find a nonzero shortest vector in the lattice L if it is presented by the basis $\tilde{B}(b,t)$.

Then there is no polynomial time algorithm which breaks either system I or system II with a probability of larger than n^{-c_2}.

The proof of this theorem togehter with a precise definition of the meaning of "breaking the cryptosystem" will be given in the last section.

4 Sketch of the proofs of the theorems

In the motivation for the definition of the random variable κ we have already described some of the ideas behind the proofs. Here we give a more detailed and technical outline. We start with Theorem 3.8 but a

large part of the proof this theorem will be used in the proof of Theorem 3.9 as well. According to the definition of the random variable κ the vectors $e_1,...,e_{n-1},v$ form a basis of the lattice L where

$$v=(n-1)^{-\xi(n-1)-\beta}e_n+\sum_{i=1}^{n-1}\mathtt{fr}(\frac{q_i}{d},kn^{\gamma})e_i$$

The rationals $\mathtt{fr}(\frac{q_i}{d},kn^{\gamma})$ are good approximations of the reals $\frac{q_i}{d}$. Since the numbers q_i, $i=1,...,n-1$ were picked with the property $[\![q_i]\!]\le(n-1)^{-\beta}$, all of the coefficients $d\mathtt{fr}(\frac{q_i}{d},kn^{\gamma})e_i$ of the vector dv will be either in the interval $[-(n-1)^{-\beta}-n^{-\gamma+1},(n-1)^{-\beta}+n^{-\gamma+1}]\subseteq[-2(n-1)^{-\beta},2(n-1)^{-\beta}]$

u was defined as $u=dv-\sum_{i=1}^{n-1}a_ie_i$ where the integers a_i are picked so that the first $n-1$ coefficients the vector u is between $-\frac{1}{2}$ and $\frac{1}{2}$. Therefore if $u=\langle u_1,...,u_{n-1},u_n\rangle$ then $\|u_i\|\le(n-1)^{-\beta}+n^{-\gamma+1}$ for $i=1,...,n-1$. By definition $u_n=d(n-1)^{-\xi(n-1)-\beta}$. Since we choose d from the interval $[\frac{1}{2}(n-1)^{\xi(n-1)},(n-1)^{\xi(n-1)}]$ we have that $\|u_n\|\le(n-1)^{-\beta}$. Therefore we have $\|u\|_\infty\le(n-1)^{-\beta}+n^{-\gamma+1}$. According to the assumptions in both theorems we have $\gamma>\beta+2$ this upper bound on $\|u\|_\infty$ is very close to $n^{-\beta}$.

Our next goal is to show that u is an $n^{\beta-\xi-\frac{1}{2}-\varepsilon}$-unique sh.n.v. with respect to the Euclidean norm. We will prove this by showing that it is a unique $n^{\beta-\xi-\varepsilon}$ shortest vector with respect to the ℓ_∞ norm. With the change of the norms we lose only a factor of $n^{\frac{1}{2}}$.

Assume now that $w\in L$ with $\|w\|_\infty\le n^{-\xi-\varepsilon}$. We want to show that w is parallel to u. (We will also have to show that u is primitive, that is, none of the vectors $\frac{1}{2}u,\frac{1}{3}u,...$ are in L.) According to the definition of L we have $w=hv+\sum_{i=1}^{n-1}a'_ie_i$ where $h,a'_1,...,a'_n$ are integers and $v=(n-1)^{-\xi(n-1)-\beta}e_n+\sum_{i=1}^{n-1}\mathtt{fr}(\frac{q_i}{d},kn^{\gamma})e_i$. Assume that e.g. h is positive. By the upper bound on $\|v\|_\infty$, the nth coordinate of v is at most $h(n-1)^{-\xi(n-1)-\beta}<1$ therefore $h\le(n-1)^{\xi(n-1)+\beta}$. The upper bounds on the other components of w, taking into account the rounding errors, yield $[\![h\frac{q_i}{d}]\!]\le(n-1)^{-\xi-\frac{\varepsilon}{2}}$.

We show that if $d|h$ and $\frac{h}{d}<\frac{1}{3}(n-1)^{\beta}$ then the vectors u and w are parallel. Assuming that $d|h$, using the upper bounds $\|u\|_\infty\le(n-1)^{-\beta}+n^{-\gamma+1}\le(1+\frac{1}{10})(n-1)^{-\beta}$, $h\le(n-1)^{\xi(n-1)+\beta}$, the equations $u=dv+\sum_{i=1}^{n-1}a_ie_i$, and $w=hv+\sum_{i=1}^{n-1}a'_ie_i$ we get that $w=\frac{h}{d}u$. (We may easily prove this by using the fact that any lattice point $w=dv+\sum_{i=1}^{n-1}a'_ie_i$ with $\|w\|<\frac{1}{2}$ is uniquely determined by d. Therefore, since $\frac{h}{d}u$ is a lattice vector, it must be w.)

So far we have shown that if we pick $d,q_1,...,q_{n-1}$ with the distribution defined by κ then the assumption that there is a $w\in L$ with $\|w\|_\infty\le(n-1)^{-\xi-\varepsilon}$ which is not parallel to u implies the following:

(4). there is a $h\in[1,(n-1)^{\xi(n-1)+\beta}]$ so that $[\![h\frac{q_i}{d}]\!]\le(n-1)^{-\xi-\frac{\varepsilon}{2}}$, $[\![d\frac{q_i}{d}]\!]=[\![q_i]\!]\le(n-1)^{-\beta}$ and either $d\not|h$ or $\frac{h}{d}\ge\frac{1}{3}(n-1)^{\beta}$

Assume now that u is not primitive, that is, $\frac{1}{r}u\in L$, for some integer $r\ge2$. Let $z=\frac{1}{r}u$. We have

$$z=\frac{1}{r}u=\frac{d}{r}v-\sum_{i=1}^{n-1}\frac{a_i}{r}\,e_{i'}\in L$$

so $\frac{d}{r}$, $\frac{a_i}{r}$, $i=1,...,n-1$ must be integers. h will denote now the integer $\frac{d}{r}$. Since $r\ge2$ we clearly have $d\not|h$. Moreover, since each component of z is smaller by a factor of r than the corresponding component of u, we get that $[\![h\frac{q_i}{d}]\!]\le(n-1)^{-\beta}\le(n-1)^{-\xi-\frac{\varepsilon}{2}}$. Consequently we got that if u is not primitive then

condition (4) is satisfied. Therefore we have shown that if u is not a unique n.sh.v., then the requirements of (4) are met.

We have to show that (4) holds only with a negligible probability (for the randomization of $d, q_1, ..., q_n$). When we speak about the random choice of d, and $\langle q_1, ..., q_n \rangle$ as defined in the definition of $\kappa_{Q,n}(\xi, \beta, \gamma)$ we consider n, ξ, β and γ as fixed but we include the randomization of Q in the random choice of q_i and d. Therefore our conclusion about w will not be valid for all $Q \in \mathtt{part}_{n-1}(k)$ but only for almost all Q.

Let Θ be the probability measure defined on the Borel subsets of $\mathbf{Z} \times \mathbf{R}^{n-1}$ defined by $\Theta(X) = \mathtt{prob}(\langle d, \langle \frac{q_1}{d}, ..., \frac{q_{n-1}}{d} \rangle \rangle \in X)$, where we randomize d, and $\langle q_1, ..., q_{n-1} \rangle$, as described above.

We are not able to prove directly about the distribution Θ that the probability of (4) is small. We will modify Θ in a way that it will be more manageable and so that the probabilities do not decrease very much. After a sequence of such modifications we get a probability measure Θ_3 so that for any event A if $\Theta(A)$ is nonnegligible then $\Theta_3(A)$ is also nonnegligible. Therefore it will be enough to show that (4) holds with a negligible probability with respect to Θ_3.

We modify the probability measure Θ by changing the randomization of d and $\langle q_1, ..., q_{n-1} \rangle$. In the original randomization we picked a $Q \in \mathtt{part}_{n-1}(k)$ first and then a $d \in [\frac{1}{2}(n-1)^{\xi(n-1)}, (n-1)^{\xi(n-1)}]$ and then a $\langle q_1, ..., q_{n-1} \rangle \in dQ$ so that $[\![q_i]\!] \leq (n-1)^{-\beta}$. Each time we picked with uniform distribution from the given set.

The first change is that we do not choose a random Q but, after picking d, we choose $\langle q_1, ..., q_{n-1} \rangle$ from $d \bigcup Q = d[0,1)^n = [0,d)^n$ so that $[\![q_i]\!] \leq (n-1)^{-\beta}$. This changes the distribution a little since the $n-1$ dimensional volumes of the sets of points $\{\langle q_1, ..., q_{n-1} \rangle \in Q \mid [\![q_i]\!] \leq (n-1)^{-\beta}\}$ are slightly different for different cubes Q. Still we will show that these differences are not large, so after this change in the randomization the nonnegligible sets remain nonnegligible.

The remaining change is only an extension of the interval from where we pick the integer d. Namely we will pick d from the interval $[1, (n-1)^{\xi(n-1)+\beta}]$ with uniform distribution instead of the original $[1, (n-1)^{\xi(n-1)}]$. Since the length of the interval has increased only by a factor of $2(n-1)^{\beta}$ the probabilities of the events may decrease by only with the same factor. Therefore nonnegligible sets remain nonnegligible.

Since we choose the realnumbers q_i from the interval $[0,d)$ with the additional condition $[\![q_i]\!] \leq (n-1)^{\beta}$, this is the same as if we choose that real $\alpha_i = \frac{q_i}{d} \in [0,1)$ with the additional condition $[\![d\alpha_i]\!] \leq (n-1)^{\beta}$.

Therefore we may reformulate the randomization and (4) using α_i instead of $\frac{q_i}{d}$. With this reformulation our goal is the following:

Assume that an integer d is picked with uniform distribution from the interval $[1, (n-1)^{\xi(n-1)+\beta}]$ and the reals $\alpha_1, ..., \alpha_{n-1}$ are picked independently, with uniform distribution and with the condition $[\![d\alpha_i]\!] \leq (n-1)^{-\beta}$ from the interval $[0,1)$ for $i = 1, ..., n-1$. Show that the probability of the following event is small:

(5). there is a $h \in [1, (n-1)^{\xi(n-1)+\beta}]$ so that $[\![h\alpha_i]\!] \leq (n-1)^{-\xi-\frac{\varepsilon}{2}}$, $[\![d\alpha_i]\!] \leq (n-1)^{-\beta}$ and either $d \not| h$ or $\frac{h}{d} \geq \frac{1}{3}(n-1)^{\beta}$

The next step in the proof is to show that we get essentially the same distribution if instead of randomizing d we pick $\alpha_1, ..., \alpha_{n-1}$ independently, with uniform distribution and with the condition

that there is a $j \in [1,(n-1)^{\xi(n-1)+\beta}]$ so that $[\![j\alpha_i]\!] \leq (n-1)^{\beta}$ and d is the smallest integer j with this property. (With high probability j is unique.) We will use the following lemma to prove this.

Definition 4.1. • Suppose that ν_1, ν_2 are probability measures on the σ-algebra $\mathcal{X}$. The distance of ν_1 and ν_2 is $\sup\{|\nu_1(A)-\nu_2(A)|+|\nu_1(B)-\nu_2(B)| \mid A,B \in \mathcal{X}, A\cap B = \emptyset\}$

Lemma 4.2. *Assume that $c_1 > c_2 > 0$, $\varepsilon > 0$, n is a sufficiently large integer, $\beta, c \in [c_2, c_1]$ are realnumbers with $\beta - c > c_2$. Suppose further that $\langle \alpha_1, ..., \alpha_n \rangle$ are realnumbers taken from the interval $(0,1)$ at random, independently, and with uniform distribution. Let B be the event that there is an $m \in [1, n^{cn}]$ so that $[\![m\alpha_i]\!] \leq n^{-\beta}$, for all $i = 1, ..., n$. Let D_1 be the conditional distribution of $\alpha_1, ..., \alpha_n$ with the condition B.*

We define a probability distribution D_2 in the following way. First we pick a random integer m with uniform distribution from the interval $[1, n^{cn}]$. Then we choose $\alpha_1, ..., \alpha_n$ at random, independently, and with uniform distribution from the interval $(0,1)$ with the condition $[\![m\alpha]\!] \leq n^{-\beta}$. This conditional distribution is D_2.

Then the distance of D_1 and D_2 is at most $(\frac{1}{2}+\varepsilon)^n$

We will sketch the proof of this lemma later. Lemma 4.2 gives only another way of randomizing the integer d and the realnumbers α_i but it does not provide any way to estimate the probability of the existence of the integer h with the properties given in (5). Lemma 4.3 below will give such an estimate.

Lemma 4.3. *Assume that $c_1 > c_2 > 0$, $\varepsilon > 0$, n is a sufficiently large integer, $\beta, \rho, c \in [c_2, c_1]$ are realnumbers with $\beta > \rho > c$, $\beta - c > c_2$. Suppose further that $\alpha_1, ..., \alpha_n$ are realnumbers taken from the interval $(0,1)$ at random independently and with uniform distribution. Let B be the event that there is an $m \in [1, n^{cn}]$ so that $[\![m\alpha_i]\!] \leq n^{-\beta}$, for all $i = 1, ..., n$.*

If k, l are positive integers then $q_{k,l}$ will denote the probability of the event

(6). $k\alpha_i \leq n^{-\beta}$, $l\alpha_i \leq n^{-\rho}$ for all $i = 1, ..., n-1$

Let $\Phi(x)$ be the set of all pairs $\langle k,l \rangle$ with the property that $k,l \in [1,x]$ and if k is a divisor of l then $\frac{l}{k} \geq \frac{1}{3}n^{\beta}$.

Then

(7). $\sum\{q_{k,l} \mid \langle k,l \rangle \in \Phi(n^{cn})\} \leq (\frac{1}{2}+\varepsilon)^n n^{cn} (2n^{-\beta})^n$

Moreover the conditional probability of the event "$\exists \langle k,l \rangle \in \Phi(n^{cn})$ so that (6) holds" with the condition B is at most $(\frac{1}{2}+\varepsilon)^n$.

Using Lemma 4.3 we can show that the probability of (5) is smaller than ϑ^n, if $\vartheta > \frac{1}{2}$ is a constant and n is sufficiently large. This completes the sketch of the proof of the fact that u is an $n^{\beta-\xi-\frac{1}{2}}$-unique n.sh.v. u. The estimate (2) on the length of $\|u\|$ will follow easily from the fact that if $u = \langle u_1, ..., u_n \rangle$ then the random variables $u_1, ..., u_{n-1}$ are independent and their values are in the interval $[-(n-1)^{-\beta}, (n-1)^{\beta}]$. This completes the sketch of the proof of Theorem 3.8

Sketch of the proof of Theorem 3.9. We show that if problem **Q2** in Theorem 3.9 has a polynomial time solution with a polynomially large probability then this is also true about Problem **Q1** of he Hardness Assumption. We modify the randomization of d and $q_1, ..., q_{n-1}$ in the same way as we have done it in the proof of Theorem 3.8, with the only difference that now we extend the interval from where we pick

the integer d only to $[1,(n-1)^{\xi-1}]$. We get that the modified randomization is the following. We pick the interval d with uniform distribution from $[1,(n-1)^{\xi-1}]$ and then $\alpha_1,...,\alpha_{n-1}$ with uniform distribution from $[0,1)$ with the condition that $[\![d\alpha_i]\!] \leq (n-1)^{-\beta}$ for $i=1,...,n-1$. (q_i is defined by $q_i = d\alpha_i$.) If Ψ is the probability measure defined on the Borel sets X of $d \times \mathbf{R}^{n-1}$ by $\Psi(X) = \mathtt{prob}(\langle d, \langle \alpha_1,...,\alpha_{n-1}\rangle\rangle \in X)$ then every nonnegligible set with respect the Θ is also a nonnegligible set with respect to Ψ. Using Lemma 4.2 we can show that the distribution Ψ is essentially the same (apart from an exponentially small error), as the following distribution: we pick $\alpha_1,...,\alpha_{n-1}$ independently and with uniform distribution from $[0,1)$ and with the condition that there exists a $j \in [1,(n-1)^{\xi-1}]$ so that $[\![j\alpha_i]\!] \leq (n-1)^{-\beta}$, $i=1,...,n-1$, and d is the smallest j with this property. This is however the same distribution that we get from problem **Q1** with parameters $n \to n-1$, $c \to \xi$, $c' \to \beta - \xi$. Therefore if we would be able to find a sh.n.v. $u = \langle u_1,...,u_n\rangle$ in the lattice then we could find the integer d (since $u_n = \pm d(n-1)^{-\xi(n-1)-\beta}$) and so the solution of the corresponding problem of Problem **Q1**. This completes the sketch of the proof of Theorem 3.9.

5 The proof of the main result

5.1 The proofs of Lemma 4.2 and Lemma 4.3

First we sketch the proof of Lemma 4.2. The lemma states that if we randomize the reals $\alpha_1,...,\alpha_n$ with the condition that there is an m so that $[\![m\alpha_i]\!]$ is small then we get the same distribution as if we first pick a value of m with uniform distribution from all of the possible values and then randomize α_i with the condition that $[\![m\alpha_i]\!]$ is small with that particular value of m for all $i=1,...,n$.

Such a switch in the order randomization would be clearly possible if the events $A_m \equiv$ "$[\![m\alpha_i]\!] \leq n^{-\beta}$ for all $i=1,...,n$" would be pairwise disjoint for the various values of m and would have the same probability with respect to choosing $\alpha_1,...,\alpha_{n-1}$ independently, with uniform distribution from $[0,1]$ and without any condition. Only the second statement holds that is the probabilities of the described events are equal, but the first one holds only in an approximate sense. Namely we will prove that the sum of the probabilities of the pairwise intersections of these events is small. Lemma 5.4, that we will formulate later, guarantees that we can reach the desired conclusion even from this approximate version of the condition. (Lemma 5.4 is a general statement about probabilities which does not use the specifics of the definition of the events A_m.) The remaining and more important part of the proof is to show that the events A_m are really pairwise disjoint in this approximate sense. The following lemma gives the exact formulation of this statement.

Lemma 5.1. *Assume that $c_1 > c_2 > 0$, $\varepsilon > 0$, n is a sufficiently large integer, $\beta, c \in [c_2, c_1]$ are realnumbers with $\beta - c > c_2$, and $\alpha_1,...,\alpha_n$ are realnumbers taken from the interval $(0,1)$ at random, independently, and with uniform distribution. Let B be the event that there is an $m \in [1,n^{cn}]$ so that $[\![m\alpha_i]\!] \leq n^{-\beta}$, for all $i=1,...,n$. Then*

(8). $P(B) \geq (1-(\frac{1}{2}+\varepsilon)^n)(2n^{-\beta})^n n^{cn}$

and the conditional probability, with condition B, that there exist $k,l \in [1,n^{cn}]$, $k \neq l$ so that

(9). $[\![k\alpha_i]\!] \leq n^{-\beta}$, $[\![l\alpha_i]\!] \leq n^{-\beta}$ for all $i=1,...,n$

is at most $(\frac{1}{2}+\varepsilon)^n$.

Let $p_{k,l}$ *be the probability of the event (9), if* k,l *are positive integers. Then* $p_{1,1}=(2n^{-\beta})^n$ *and*

(10). $\sum\{p_{k,l} \mid k,l\in[1,n^{cn}], k\neq l\} \leq (\frac{1}{2}+\varepsilon)^n n^{cn} p_{1,1}$

We will prove this lemma by showing that $\frac{2}{M}(\frac{2}{N}+\frac{1}{k})$ is an upper bound on the probability of the event "$[\![k\alpha]\!] \leq \frac{1}{M}$ and $[\![l\alpha]\!] \leq \frac{1}{N}$" where k,l are fixed integers with $(k,l)=1$, $N,M>1$ are also fixed and α is chosen with uniform distribution from $(0,1)$. Lemma 5.3, that we will formulate later, describes this statement. Using this upper bound we will be able to prove inequality (10) of Lemma 5.1. In (10) we estimate the sum of all of the probabilities $p_{k,l}$ where $p_{k,l}$ is the probability of "$[\![k\alpha_i]\!] \leq n^{-\beta}$ and $[\![l\alpha_i]\!] \leq n^{-\beta}$ for all $i=1,\ldots,n$". Here we may have $(k,l)>1$ so Lemma 5.3 cannot be applied directly. We group the terms in $\sum p_{k,l}$ according to the value of (k,l). In a fixed group where, $(k,l)=d$ we are able to give an upper bound on the sum using that the distribution of $d\alpha_i$ is the same as the distribution of α_i. This last observation makes it possible to reduce the general case to the $(k,l)=1$ special case and makes Lemma 5.3 applicable. We also use the fact that the different reals α_i are independent so the corresponding probabilities can be multiplied. This way we get an upper bound for each fixed $d=(k,l)$. The sum of these upper bounds yields the required estimate. The proof of Lemma 5.1 goes according to the same ideas. This completes the sketch of the proof of Lemma 4.2, Lemma 5.1, and Lemma 4.3. In the remaining part of this section we give these proofs in detail.

Lemma 5.2. *Assume that* $M>1$ *is an integer,* k *is a positive integer and* $x_1,x_2,\ldots$ *is a periodic infinite sequence of realnumbers with period* k*, that is,* $x_i=x_{i+k}$ *for all* $i=1,2,\ldots$*, and*

(11). $\forall i,j\in[1,k], i\neq j \rightarrow x_i \not\equiv x_j \pmod 1$.

Suppose further that

(12). $x_{i+1}-x_i \equiv x_{j+1}-x_j \pmod 1$ for all $i,j\in\{1,2,\ldots.\}$

Then, the number of integers $i\in[1,k]$ *with the property* $[\![x_i]\!] \leq \frac{1}{M}$ *is at most* $\frac{2k}{M}+1$.

Proof. For $k=1$ the conclusion of the lemma trivially holds so we may assume $k>1$. Let π be a permutation of the set $\{1,\ldots,k\}$, so that $x_{\pi(1)}<\ldots<x_{\pi(k)}$. We claim that conditions (11), (12) and the periodicity of the sequence x_i with period k imply that $x_{\pi(i+1)}-x_{\pi(i)}=\frac{1}{k}$ for $i=1,\ldots,k-1$, and $x_{\pi(1)}-x_{\pi(k)}\equiv\frac{1}{k} \pmod 1$. Indeed according to (12) if $x_{i+1}-x_i\equiv\nu \pmod 1$, then $k\nu\equiv 1 \pmod 1$ and so $\nu=\frac{a}{k}$ for some integer k. Therefore property (11) implies that $(a,k)=1$ and so the numbers $x_1,\ldots,x_k$ distributed modulo 1 in a way that the distance between the consecutive ones is $\frac{1}{k}$ as claimed above.

Assume that the number of integers j with " $\exists\gamma\in[-\frac{1}{M},\frac{1}{M}]$ so that $x_j\equiv\gamma_j \pmod 1$", is d. Since the modulo 1 distance of the neighboring points γ_j is $\frac{1}{k}$ we have that $(d-1)\frac{1}{k}\leq\frac{2}{M}$ which implies our assertion. (Lemma 5.2)■

Lemma 5.3. *Assume that* k,l,M,N *are positive integers,* $(k,l)=1$*,* $M>2,N>2$ *and* α *is a realnumber chosen with uniform distribution from the interval* $(0,1)$*. Let* A *be the event: "*$[\![k\alpha]\!]<\frac{1}{M}$ *and* $[\![l\alpha]\!]\leq\frac{1}{N}$*". Then*

$$\texttt{prob}(A)\leq\frac{2}{M}\left(\frac{2}{N}+\frac{1}{k}\right)$$

If $M = N$, then

$$\mathtt{prob}(A) \leq \frac{2}{M}\Big(\frac{2}{M} + \frac{1}{\max\{k,l\}}\Big)$$

Proof. Let $X = \{x \in [0,1) \mid [\![kx]\!] \leq \frac{1}{M}\}$, $Y = \{x \in [0,1) \mid [\![kx]\!] \leq \frac{1}{M}, [\![lx]\!] \leq \frac{1}{N}\}$. Clearly $x \in Y$ iff $x \in X$ and $[\![lx]\!] \leq \frac{1}{N}$. $\mathtt{prob}(A) = \lambda(Y)$, where λ is the one dimensional Lebesgue measure.

We randomize the number α in the following way. First we pick a random β from $[0,1)$ with uniform distribution and then we select an element of the set $\{\beta, \beta + \frac{1}{k}, ..., \beta + \frac{k-1}{k}\}$ at random and with uniform distribution. If the selected number is z then $\alpha = z - \lfloor z \rfloor$. Clearly α has uniform distribution on $[0,1)$. We estimate $\mathtt{prob}(A) = \mathtt{prob}(\alpha \in Y)$ in the following way. Let $\langle\langle x \rangle\rangle = x - \lfloor x \rfloor$ for all $x \in \mathbf{R}$. The definition of X implies that

(13). for a fixed β either all of the numbers $\langle\langle \beta \rangle\rangle, \langle\langle \beta + \frac{1}{k} \rangle\rangle, ..., \langle\langle \beta + \frac{k-1}{k} \rangle\rangle$ are in X or none of them.

This implies that

(14). $\lambda(X) = k\lambda(X \cap [0, \frac{1}{k}))$

If β has uniform distribution on $[0,1)$ then $\langle\langle k\beta \rangle\rangle$ also has uniform distribution on the same interval and therefore $\mathtt{prob}(\beta \in X) \leq \frac{2}{M}$ (if $M \geq 2$ then we have equality). We estimate for each fixed β with $\beta \in X$ the probability of $[\![l\alpha]\!] \leq \frac{1}{N}$, where according to the definition of the random variable α, if β is fixed α is picked from the set $\{\beta, \beta + \frac{1}{k}, ..., \beta + \frac{k-1}{k}\}$ with uniform distribution. We apply Lemma 5.2 with $x_{1+j} = l(\beta + \frac{j'}{k})$, $j = 0, 1, ...$, where j' is the least nonnegative residue of j modulo k. The assumption $(l,k) = 1$ implies that property (11) is satisfied and property (12) is an immediate consequence of the definition of x_i. Therefore we get that if the number of elements z in the set $\{\beta, \beta + \frac{1}{k}, ..., \beta + \frac{k-1}{k}\}$ with $[\![lz]\!] \leq \frac{1}{N}$ is ν, then $\nu \leq \frac{2k}{N} + 1$.

Let χ be the characteristic function of the set Y defined on the interval $[0,1)$ and let T be the set $\{0, \frac{1}{k}, ..., \frac{k-1}{k}\}$. We define a measure μ on the subsets of T by $\mu(S) = |S|$, for all $S \subseteq T$. We have

$\mathtt{prob}(\alpha \in Y) = \lambda(Y) = \int_0^1 \chi(x)dx = \sum_{i=0}^{k-1} \int_{\frac{i}{k}}^{\frac{i+1}{k}} \chi(x)dx = \sum_{i=0}^{k-1} \int_0^{\frac{1}{k}} \chi(x + \frac{i}{k})dx = \int_T \int_0^{\frac{1}{k}} \chi(x+y)dxd\mu_y$.
The function $\chi(x+y)$ is integrable on the product space $T \times [0,1)$ therefore Fubini's theorem (see [7]) implies that the order of integration can be reversed and so $\mathtt{prob}(\alpha \in Y) = \int_0^{\frac{1}{k}} \int_T \chi(x+y)d\mu_y dx = \int_{X \cap [0,\frac{1}{k})} \int_T \chi(x+y)d\mu_y dx + \int_{[0,\frac{1}{k}) \setminus X} \int_T \chi(x+y)d\mu_y dx$. By the definition of X and (13) the second term is 0. We estimate the first term using our upper bound on ν and (14). We get

$\int_{X \cap [0,\frac{1}{k})} \int_T \chi(x+y)d\mu_y dx \leq \int_{X \cap [0,\frac{1}{k})} (\frac{2k}{N} + \frac{1}{k})dx = \frac{2}{kM}(\frac{2k}{N} + 1) = \frac{2}{M}(\frac{2}{N} + \frac{1}{k})$

(Lemma 5.3)■

Proof of Lemma 5.1. Let $d \in [1, n^{cn}]$. We estimate the probability p_d of the event that there are $k, l \in [1, n^{cn}]$, $k \neq l$ with $(k,l) = d$ and with property (9). Since the distribution of $d\alpha_1, ..., d\alpha_n$ modulo 1 is the same as the distribution of $\alpha_1, ..., \alpha_n$, p_d is also the probability of the following event: there are $k, l \in [1, d^{-1}n^{cn}]$, $k \neq l$ with $(k,l) = 1$ and with property (9).

For each pair of positive integers k, l and for each fixed $i = 1, ..., n$ let $p_{k,l}^{(i)}$ be the probability of the event described in (9) with this particular i. Since the random variables α_i are independent, $p_{k,l} = \prod_{i=1}^n p_{k,l}^{(i)}$. Therefore according to Lemma 5.3 $p_{k,l} \leq (2n^{-\beta}(2n^{-\beta} + \frac{1}{\max\{k,l\}}))^n$.

The definition of p_d implies that $p_d \le \sum\{p_{k,l} \mid 1 < \max\{k,l\} \le n^\beta\} + \sum\{p_{k,l} \mid \max\{k,l\} > n^\beta\}$. The first term is at most $(n^\beta)^2((2n^{-\beta}(2n^{-\beta}+\frac{1}{2}))^n \le (2n^{-\beta})^n(\frac{1}{2}+\frac{\varepsilon}{4})^n$ if n is sufficiently large. The second term is at most $d^{-2}n^{2cn}(2n^{-\beta}(2n^{-\beta}+n^{-\beta}))^n = d^{-2}n^{2cn}6^n n^{-2\beta n} \le d^{-2}6^n n^{cn}n^{-\beta n}n^{(c-\beta)n} \le d^{-2}6^n n^{cn}n^{-\beta n}n^{-c_2 n} \le d^{-2}n^{cn}n^{-\beta n}n^{-\frac{c_2}{2}n}$ if n is sufficiently large. Adding the upper bounds of all p_d we get that the probability that there are $k,l \in [1,n^{cn}]$, $k \ne l$ with property (9) is at most $\sum_{d=1}^{n^{cn}}((2n^{-\beta})^n(\frac{1}{2}+\frac{\varepsilon}{4})^n + d^{-2}n^{cn}n^{-\beta n}n^{-\frac{c_2}{2}n}) \le n^{cn}(\frac{1}{2}+\frac{\varepsilon}{4})^n(2n^{-\beta})^n + \frac{\pi^2}{6}n^{cn}n^{-\beta n}n^{-\frac{c_2}{2}n} \le n^{cn}(\frac{1}{2}+\frac{\varepsilon}{2})^n(2n^{-\beta})^n$. This proves (10).

Now we prove the lower bound on $P(B)$. $P(B) \ge \sum_{i=1}^{n^{cn}} p_{i,i} - \sum\{p_{k,l} | k,l \in [1,n^{cn}], k \ne l\} \ge n^{cn}p_{1,1} - (\frac{1}{2}+\frac{\varepsilon}{2})^n n^{cn}p_{1,1} = (1-(\frac{1}{2}+\frac{\varepsilon}{2})^n)n^{cn}p_{1,1}$ as claimed in (8). (10) gives an upper bound on the probability of the event in (9) and together with (8) they yield the upper bound on the conditional probability of event (9). (Lemma 5.1)■

Lemma 5.4. *Assume that $A_1,\ldots,A_t$ are events in an arbitrary probability space with the following properties:*

(i) $\mathtt{prob}(\bigcup_{i=1}^t A_i) = 1$

(ii) $\mathtt{prob}(A_i) = \mathtt{prob}(A_j)$ *for all* $i,j \in [1,t]$

(iii) $\sum\{\mathtt{prob}(A_i \cap A_j) \mid i,j \in [1,t], i \ne j\} \le \sigma$

Then for an arbitrary event W we have $|\mathtt{prob}(W) - \sum_{i=1}^t \frac{1}{t}\mathtt{prob}(W|A_i)| \le 3\sigma$.

Proof. We define another probability measure $\mathtt{prob}'$ on the same σ-algebra where $\mathtt{prob}$ is defined by $\mathtt{prob}(Y) = \sum_{i=1}^t \frac{1}{t}\mathtt{prob}(Y|A_i)$. This is indeed a probability measure since it is the linear combination of probability measures so that the coefficients are nonnegative and their sum is 1.

By (ii) there is a p so that $p = A_i$ for $i = 1,\ldots,n$. According to (i) $tp \ge 1$. On the other hand we claim that (iii) implies $tp \le 1+\sigma$. Indeed $1 = \mathtt{prob}(\bigcup A_i) \ge \sum_i \mathtt{prob}(A_i) - \sum_{i \ne j}\mathtt{prob}(A_i \cap A_j) \ge tp - \sigma$. Therefore we have

(15). $\frac{1}{t} \le p \le \frac{1}{t} + \frac{\sigma}{t}$.

Let $X = \bigcup\{A_i \cap A_j \mid i,j \in [1,t], i \ne j\}$. Property (iii) implies that $\mathtt{prob}(X) \le \sigma$. If Z is an event and there is an $i \in [1,n]$ so that $Z \subseteq A_i \backslash X$ then $\mathtt{prob}'(Z) = \frac{1}{t}\mathtt{prob}(Z|A_i) = \frac{1}{tp}\mathtt{prob}(Z)$. Therefore (15) implies that

(16). $\mathtt{prob}'(Z) \le \mathtt{prob}(Z) \le (1+\sigma)\mathtt{prob}'(Z)$.

Clearly these inequalities remain valid for any $Z \subseteq \bar{X}$ where $\bar{X}$ is the complement of X. Applying it to $Z = \bar{X}$ we get $\mathtt{prob}'(\bar{X}) \ge (1+\sigma)^{-1}\mathtt{prob}(\bar{X}) \ge (1+\sigma)^{-1}(1-\sigma) \ge 1-2\sigma$. Therefore $\mathtt{prob}'(X) \le 2\sigma$.

Assume now that W is an arbitrary event. $\mathtt{prob}(W) = \mathtt{prob}(W \cap X) + \mathtt{prob}(W \backslash X)$ and $\mathtt{prob}'(W) = \mathtt{prob}'(W \cap X) + \mathtt{prob}'(W \backslash X)$. Taking the difference of the two equations we get $|\mathtt{prob}(W) - \mathtt{prob}'(W)| = |\mathtt{prob}(W \cap X) - \mathtt{prob}'(W \cap X)| + |\mathtt{prob}(W \backslash X) - \mathtt{prob}'(W \backslash X)|$. Since $0 \le \mathtt{prob}(X) \le \sigma$ and $0 \le \mathtt{prob}'(X) \le 2\sigma$ we have $|\mathtt{prob}(W \cap X) - \mathtt{prob}'(W \cap X)| \le 2\sigma$. As we have noted (16) holds for any $Z \subseteq \bar{X}$ therefore $|\mathtt{prob}(W \backslash X) - \mathtt{prob}(W \backslash X)| \le \sigma\mathtt{prob}'(W \backslash X) \le \sigma$. The two upper bounds imply the conclusion of the lemma. (Lemma 5.4)■

We prove the statement of Lemma 4.2 applying Lemma 5.4 with the following choices of the parameters. $t = n^{cn}$, the probability space consists of the measurable subsets of B with the probability distribution

D_1, and $\sigma = \frac{1}{3}(\frac{1}{2}+\varepsilon)^n$. Condition (i) follows from the definition of the probability space. Condition (ii) is a consequence of the fact that the probability of the event "$[\![m\alpha_i]\!] \leq n^{-\beta}$ for all $i = 1,...,n$" is $(2n^{-\beta})^n$ independently of the choice of m. Lemma 5.3 implies that $\sum\{\mathtt{prob}(A_i \cap A_j)(\mathtt{prob}(B))^{-1} \mid i,j \in [1,n^c]\} \leq (\frac{1}{2}+\varepsilon')^n n^{cn} p_{1,1}$. This together with the lower bound (8) on $P(B)$ implies (iii). The conclusion of Lemma 5.4 gives the required upper bound on the distance of the two distributions. (Lemma 4.2)■

Proof of Lemma 4.3. The proof of this lemma is very similar to the proof of Lemma 5.1. Still there are a few differences which need additional attention. Let $d \in [1,n^{cn}]$. We estimate the probability q_d of the event that there are $k,l \in \Phi(n^{cn})$ with $(k,l) = d$ and with property (6). The distribution of $d\alpha_1,...,d\alpha_n$ is the same as the distribution of $\alpha_1,...,\alpha_n$, consequently q_d is the probability of the following event as well: there are $k,l \in \Phi(d^{-1}n^{cn})$ with $(k,l) = 1$ and with property (6).

For each pair of positive integers k,l and for each fixed $i = 1,...,n$, let $q^{(i)}_{k,l}$ be the probability of the event (6). Since the random variables α_i are independent, $q_{k,l} = \prod_{i=1}^n q^{(i)}_{k,l}$. Therefore according to Lemma the following two inequalities hold.

(17). $q_{k,l} \leq (2n^{-\beta}(2n^{-\rho}+\frac{1}{k}))^n$

(18). $q_{k,l} \leq ((2n^{-\beta}+\frac{1}{l})2n^{-\rho})^n$.

$q_d \leq \sum\{q_{k,l} \mid \langle k,l\rangle \in \Phi(d^{-1}n^{cn}), k \leq n^\beta, l \leq n^\beta\} + \sum\{q_{k,l} \mid \langle k,l\rangle \in \Phi(d^{-1}n^{cn}), k \leq n^\beta, l > n^\beta\} + \sum\{q_{k,l} \mid \langle k,l\rangle \in \Phi(d^{-1}n^{cn}), k > n^\beta\}$. We estimate the three terms separately. If $k > 1$ we use inequality (17) for each fixed pair in the first term and we get that this part of the first term is at most $(n^\beta)^2((2n^{-\beta}(2n^{-\rho}+\frac{1}{2}))^n$. If $k = 1$ then by the definition of Φ we have $l \geq \frac{1}{3}n^\beta$. We use inequality (18), and we get the upper bound $n^\beta((2n^{-\beta}+3n^{-\beta})2n^{-\rho})^n$ on the corresponding part of the first term. If n is sufficiently large then the sum of the two upper bounds is at most $(2n^{-\beta})^n(\frac{1}{2}+\frac{\varepsilon}{4})^n$.

We use inequality (18) for the second term for each fixed pair k,l. The number of choices for k is at most n^β, the number of choices for l is at most $\frac{1}{d}n^{cn}$, so we get the upper bound $n^\beta d^{-1}n^{cn}((2n^{-\beta}+\frac{1}{l})2n^{-\rho})^n \leq (2n^{-\beta})^n(\frac{1}{2}+\frac{\varepsilon}{4})^n$.

To get an upper bound on the third term we use inequality (17). We get $d^{-2}n^{2cn}(2n^{-\beta}(2n^{-\beta}+n^{-\beta}))^n \leq d^{-2}(2n^{-\beta})^n(\frac{1}{2}+\frac{\varepsilon}{4})^n$ if n is sufficiently large.

Adding these upper bounds for all $d \in [1,n^{cn}]$ and using that $\sum_{d=1}^\infty d^{-2} < \infty$ we get that $\sum\{q_{k,l} \mid \langle k,l\rangle \in \Phi(n^{cn})\} \leq (2n^{-\beta})^n(\frac{1}{2}+\varepsilon)^n$ as claimed in (7).

The upper bound in (7) gives an upper bound on the probability of the event described in the last statement of the lemma. The upper bound on the conditional probability follows from this and the lower bound on $P(B)$ given in Lemma 5.1. (Lemma 4.3)■

5.2 The proofs of Theorem 3.8 and Theorem 3.9

Proof of Theorem 3.8. Let $\langle\langle t_1,....,t_{n-1}\rangle,u\rangle$ be a random value of $\bar{\tau}_{Q,n}(\xi,\beta,\gamma)$ and $L = \mathcal{L}(t_1,...,t_{n-1},b_1,...,b_{n-1},\xi,\beta,\gamma)$. We will use the notation $u_L = u$ if we need the emphasize the dependency on L. We will show that with a probability of at least $1-2^{-n}$ we have $\|u_L\|_\infty \leq (n-1)^{-\beta}+n^{-\gamma+1}$. Then we show that with the probability indicated in the theorem the following holds. Assume that $w \in L$ and $\|w\|_\infty \leq (n-1)^{-\xi-\varepsilon/2}$. Then w and u_L are parallel. Therefore u_L is an $(n-1)^{-\xi+\beta-\varepsilon}$-unique nonzero shortest vector with respect to the ℓ_∞-norm and consequently it is an $(n-1)^{-\xi+\beta-\varepsilon-\frac{1}{2}}$-unique shortest

nonzero vector with respect to the Euclidean norm. (Since $(n-1)^{-\xi+\beta-\varepsilon-\frac{1}{2}} \geq n^{-\xi+\beta-\frac{\varepsilon}{2}-\frac{1}{2}}$ it does not matter whether the base is $n-1$ or n in this expression.)

We have defined L as the lattice generated by $e_1,...,e_{n-1}$ and v, where $v = (n-1)^{-\xi(n-1)-\beta}e_n + \sum_{i=1}^{n-1} \mathtt{fr}(\frac{q_i}{d}, kn^\gamma)e_i$. Therefore $dv = d(n-1)^{-\xi(n-1)-\beta}e_n + d\sum_{i=1}^{n-1} \mathtt{fr}(\frac{q_i}{d}, kn^\gamma)e_i \in L$. By the definition of $\mathtt{fr}(\frac{q_i}{n}d, kn^\gamma)$ we have $dv = v' + v_R$, where $v' = d(n-1)^{-\xi(n-1)-\beta}e_n + \sum_{i=1}^{n-1} q_i e_i$ and $v_R = \sum_{i=1}^{n-1} \delta_i e_i$, $|\delta_i| \leq d\frac{1}{kn^\gamma} \leq \frac{1}{n^{\gamma-1}}$. Let s_i be the closest integer to q_i and let $\tilde{u} = dv - \sum_{i=1}^{n-1} s_i e_i$. We claim that $\tilde{u} = u_L$, $\tilde{u} \neq 0$, and $\|\tilde{u}\|_\infty \leq (n-1)^{-\beta} + n^{-\gamma+1}$. $\tilde{u} \neq 0$ follows from the fact the the coefficient of e_n is not 0 if we write u as a linear combination of the unit vectors e_i.

$\tilde{u} = v' - \sum_{i=1}^{n-1} s_i e_i + v_R = d(n-1)^{-\xi(n-1)-\beta}e_n + \sum_{i=1}^{n-1}(q_i - s_i)e_i + v_R = d(n-1)^{-\xi(n-1)-\beta}e_n + \sum_{i=1}^{n-1} [\![q_i]\!]e_i + v_R$, where $\|v_R\|_\infty \leq n^{-\gamma+1}$. The definition of q_i implies that $[\![q_i]\!] \leq (n-1)^{-\beta}$, and $d \leq (n-1)^{\xi(n-1)}$ implies that the coefficient of e_n in absolute value is also at most $(n-1)^{-\beta}$, therefore $\|\tilde{u}\|_\infty \leq (n-1)^{-\beta} + n^{-\gamma+1} < (1+\frac{1}{10})(n-1)^{-\beta}$. This inequality and the definitions of u_L and $\tilde{u}$ imply that $\tilde{u} = u_L$.

The definition of u and the proof above also implies the following that we will use later.

Lemma 5.5. *Let $u_L = \langle u_1,...,u_n\rangle$. Then*
$u_n = d(n-1)^{-\xi(n-1)-\beta} \leq n^{-\beta}$ *and for all* $i = 1,...,n-1$
$u_i = [\![q_i]\!] + \delta_i$, *where* $|\delta_i| \leq n^{\gamma-1}$

To prove that u_L is indeed an $(n-1)^{\beta-\xi-\varepsilon}$-unique nonzero shortest vector with respect to the ℓ_∞ norm, as a first step, we show the following

Lemma 5.6. *Assume that $\xi,\beta,\gamma,\varepsilon$ are given as in Theorem 3.8, the integer n is sufficiently large, L is a value of the random variable $\kappa_{Q,n}(\xi,\beta,\gamma)$, and d is the integer and $q_1,...,q_n$ are the realnumbers from the definition of $\kappa_{Q,n}(\xi,\beta,\gamma)$ in the case when the value of κ is L. Then $\|u_L\|_\infty < (1+\frac{1}{10})(n-1)^{-\beta}$. Suppose further that there is a $w \in L$, $w \neq 0$ which is not parallel to u so that $\|w\|_\infty \leq (n-1)^{-\xi-\varepsilon}$. Then there is an integer h so that the pair d,h meets the following requirements: $[\![h\frac{q_i}{d}]\!] \leq (n-1)^{-\xi-\frac{\varepsilon}{2}}$, $h \in [1,(n-1)^{\xi(n-1)+\beta}]$, $[\![d\frac{q_i}{d}]\!] \leq (n-1)^{-\beta}$, $d \in [1,(n-1)^{\xi(n-1)}]$ and either $d \not| h$ or $\frac{h}{d} \geq \frac{1}{3}(n-1)^\beta$*

We have already proved the upper bound on $\|u_L\|_\infty$. Since $w \in L$ we have $w = hv + \sum_{i=1}^{n-1} g_i e_i$, where $hv = h(n-1)^{-\xi(n-1)-\beta}e_n + h\sum_{i=1}^{n-1} \mathtt{fr}(\frac{q_i}{d}, kn_\gamma)e_i$ and $g_1,...,g_{n-1}$ are integers. $\|w\| \leq 1$ implies that $|h(n-1)^{-\xi(n-1)-\beta}| \leq 1$ and so $h \leq (n-1)^{\xi(n-1)+\beta}$.

We have $\mathtt{fr}(\frac{q_i}{d}, kn^\gamma) = \frac{q_i}{d} + \frac{\tau_i}{kn^\gamma}$, where $0 \leq \tau_i < 1$. Therefore $hv = h(n-1)^{-\xi(n-1)-\beta}e_n + \sum_{i=1}^{n-1}(h\frac{q_i}{d} + \delta_i)e_i$ where $|\delta_i| \leq (n-1)^{\xi(n-1)+\beta}\frac{1}{(n-1)^{\xi(n-1)-1}n^\gamma} \leq (n-1)^{\beta+1-\gamma} \leq (n-1)^{-\xi-1}$.

Consequently the upper bound on $\|w\|_\infty$ implies that $[\![h\frac{q_i}{d} + \delta_i]\!] \leq (n-1)^{-\xi-\varepsilon}$. The upper bound on δ_i and the assumption $\beta > \xi$ of Theorem 3.8 imply that $[\![h\frac{q_i}{d}]\!] \leq (n-1)^{-\xi-\frac{\varepsilon}{2}}$ if n is sufficiently large.

Assume now that $d|h$. The definition of u_L and $w = hv + \sum_{i=1}^{n-1} g_i e_i$ imply, that $w = \frac{h}{d}u + \sum_{i=1}^{n-1} a_i e_i$, where $a_1,...,a_{n-1}$ are integers. Suppose now that contrary to the statement of Lemma 5.6 we have $\frac{h}{d} < \frac{1}{3}(n-1)^\beta$. Therefore $\|u_L\|_\infty \leq (1+\frac{1}{10})(n-1)^{-\beta}$ implies that $\|\frac{h}{d}u_L\|_\infty \leq (1+\frac{1}{10})(n-1)^{-\beta}\frac{1}{3}(n-1)^\beta < \frac{1}{2}$ if n is sufficiently large. This inequality, $\|w\|_\infty \leq (n-1)^{-\xi-\varepsilon} < \frac{1}{2}$, and the equation $w = \frac{h}{d}u_L + \sum_{i=1}^{n-1} a_i e_i$ imply that $a_1 = ... = a_{n-1} = 0$, and so u and w are parallel, in contradiction to our assumption. (Lemma 5.6)■

Definition 5.7. • We consider the process of choosing a random Q from $\mathtt{part}_{n-1}(k)$ with uniform distribution and then choosing a random L according to $\kappa_{Q,n}(\xi,\beta,\gamma)$, as a single randomization. During this randomization we pick an integer d from the interval $[\frac{1}{2}(n-1)^{\xi(n-1)},(n-1)^{\xi(n-1)}]$ with uniform distribution and a vector $q=\langle q_1,...,q_{n-1}\rangle$ form the set $\{\langle x_1,...,x_{n-1}\rangle \in dQ \mid [\![x_i]\!] \leq (n-1)^{-\beta}, i=1,...,n-1\}$ with uniform distribution with respect to the $n-1$-dimensional volume. Let $\mathcal{X}$ be the σ-algebra of all Borel subsets of $\mathbf{Z}\times\mathbf{R}^{n-1}$. We will denote by Θ the probability measure on $\mathcal{X}$ defined by $\Theta(X)=\mathtt{prob}(\langle d,\langle\frac{q_1}{d},...,\frac{q_n}{d}\rangle\rangle\in X)$ for all $X\in\mathcal{X}$, where $d,q_1,...,q_n$ are picked according to the randomization described above.

• We say that the pair $\langle d,\langle s_1,...,s_{n-1}\rangle\rangle$, $d\in\mathbf{Z}$, $\langle s_1,...,s_{n-1}\rangle\in\mathbf{R}^{n-1}$ is singular if the following condition is satisfied:

(19). Let $q_i=ds_i$ for $i=1,...,n-1$. Then there is an integer h so that $[\![h\frac{q_i}{d}]\!]\leq(n-1)^{-\xi-\frac{\varepsilon}{2}}$, $h\in[1,(n-1)^{\xi(n-1)+\beta}]$, $[\![d\frac{q_i}{d}]\!]\leq(n-1)^{-\beta}$, and either $d\not| h$ or $\frac{h}{d}\geq\frac{1}{3}(n-1)^{\beta}$

Remark 5.8. 9. We used the notation $s_i=\frac{q_i}{d}$ to indicate the connection of this definition to the definition of the lattice L.

Definition 5.9. • Assume that for each positive integer n, Γ_n is a probability measure on $\mathcal{X}$ and suppose that we chose the pair $\langle d,\langle s_1,...,s_{n-1}\rangle\rangle\in\mathbf{Z}\times\mathbf{R}^{n-1}$ according to distribution Γ_n. We say that the family of distributions Γ_n, $n=1,2,....$ is regular if for all $\vartheta>\frac{1}{2}$ and for all sufficiently large n the probability, with respect to Γ_n, that $\langle d,\langle s_1,...,s_n\rangle\rangle$ is singular is at most ϑ^n.

It is an immediate consequence of Lemma 5.6 that in order to complete the proof of Theorem 3.8 it is sufficient to show that the distribution Θ is regular. (Naturally, Θ depends on n so we can consider it as a family of distributions.) Indeed, this would show that a vector w with the properties described in Lemma 5.6 exists only with a probability of less than ϑ^n with respect to the randomization of Q and $\kappa_{Q,n}(\xi,\beta,\gamma)$ if n is sufficiently large. Therefore with a probability of at least $1-\vartheta^n$, with respect to the two randomizations together, there is an $(n-1)^{-\xi-\varepsilon}$-unique nonzero shortest vector, with respect to the ℓ_p norm, in the lattice L, as claimed by Theorem 3.8.

Our next goal is to show that Θ is regular. We will define a sequence of distributions Θ (already defined), Θ_1, Θ_2, Θ_3, Ψ' and show that the regularity of each of these distributions in the sequence follows from the regularity of the next one. Finally we will show that Ψ' is regular using Lemma 4.2.

First we define another probability measure Ψ on the σ-algebra $\mathcal{X}$. Ψ is defined by the following randomization. We pick the realnumbers $\alpha_1,...,\alpha_{n-1}$ independently and with uniform distribution from $(0,1)$, and with the condition "There exists an integer j in the interval $[1,(n-1)^{\xi(n-1)}]$ so that $[\![j\alpha_i]\!]\leq(n-1)^{-\beta}$ for all $i=1,...,n-1$", the integer d will be the smallest j with this property. For each $X\in\mathcal{X}$, $\Psi(X)=\mathtt{prob}(\langle d,\langle\alpha_1,...,\alpha_{n-1}\rangle\rangle\in X)$. (Lemma 5.1 implies that with a probability of at least $1-(\frac{1}{2}+\varepsilon')^n$ there is a unique j with the given property.) We will use the following lemma in the proof of Theorem 3.9, however some of the partial results will be useful for the proof of Theorem 3.8 as well.

Lemma 5.10. *There is a $c'>0$ so that for all $\varepsilon'>0$, if ξ,β,γ are given with the properties described in Theorem 3.8 and n is sufficiently large, then for all $A\in\mathcal{X}$ with $\Theta(A)>(\frac{1}{2}+\varepsilon')^n$ we have $\Psi(A)\geq c'\Theta(A)$.*

Proof. Let Θ_1 be the probability distribution that we get by modifying the randomization performed according to Θ in the following way. We leave the randomization of d unchanged. Suppose that d

have been already selected. Let $F = \{\langle r_1,...,r_n\rangle \in \mathbf{R}^{n-1} \mid [\![r_i]\!] \le (n-1)^{-\beta}, i = 1,...,n-1\}$. Instead of picking first Q and then q from $F \cap dQ$, (as we have done for the randomization of Θ), now we pick q from the set $F \cap \bigcup\{dQ \mid Q \in \mathtt{part}_{n-1}(k)\} = F \cap [0,d)^{n-1}$ with uniform distribution with respect to the $n-1$ dimensional volume. This creates a slightly different distribution on the set of possible vectors $q = \langle q_1,...,q_{n-1}\rangle$ since the various sets $dQ \cap F$ for different cubes $Q \in \mathtt{part}(k)$ may have different $n-1$-dimensional volumes. To estimate the ratio of probabilities according to the two distributions we give upper and lower bounds on the $n-1$ dimensional volume of the set $dQ \cap F$ where Q is an arbitrary element of $\mathtt{part}_{n-1}(k)$.

Suppose that $Q = \prod_{i=1}^{n-1}[\frac{b_i}{k}, \frac{b_i+1}{k})$. The definition of F implies that $\mathtt{vol}_{n-1}(dQ \cap F) = \prod_{i=1}^{n-1} \lambda(F_i \cap [\frac{d}{k}b_i, \frac{d}{k}(b_i+1)])$, where λ is the one dimensional Lebesgue measure and $F = \prod_{i=1}^{n} F_i$. Let $[a,b]$ be a maximal interval with integer endpoints so that $[a,b] \subseteq I$, where $I = [\frac{d}{k}b_i, \frac{d}{k}(b_i+1)]$. Clearly $\frac{d}{k} \ge b-a \ge \frac{d}{k}-2$. $\lambda(F \cap I) = \lambda(F_i \cap [a,b]) + \lambda(F_i \cap (I \backslash [a,b]))$. We have $\lambda(F_i \cap [a,b]) = 2(n-1)^{-\beta}(b-a)$ and $0 \le \lambda(F_i \cap (I \backslash [a,b]))) \le 4(n-1)^{-\beta}$. This implies that

(20). $(\frac{d}{k}-2)2(n-1)^{-\beta} \le \lambda(F_i \cap I) \le (\frac{d}{k}+2)2(n-1)^{-\beta}$.

Therefore $((\frac{d}{k}-2)2(n-1)^{-\beta})^{n-1} \le \mathtt{vol}_{n-1}(F \cap dQ) \le ((\frac{d}{k}+2)2(n-1)^{-\beta})^{n-1}$ and so $(\frac{d}{k})^{n-1}(1-\frac{2k}{d})^{n-1}2^{n-1}(n-1)^{-(n-1)\beta} \le \mathtt{vol}_{n-1}(F \cap dQ) \le (\frac{d}{k})^{n-1}(1+\frac{2k}{d})^{n-1}2^{n-1}(n-1)^{-(n-1)\beta}$. By the definition of d and k we have $0 \le \frac{2k}{d} \le \frac{4}{n-1}$, therefore $c_1(\frac{d}{k})^{n-1}2^{n-1}(n-1)^{-(n-1)\beta} \le \mathtt{vol}_{n-1}(F \cap dQ) \le c_2(\frac{d}{k})^{n-1}2^{n-1}(n-1)^{-(n-1)\beta}$, where $c_1 > 0, c_2 > 0$ are absolute constants. This shows that the probabilities defined by the two randomizations of q_i may differ at most by a constant factor, that is, $\Theta_1(A) \ge c_3\Theta(A)$ for all $A \in \mathcal{X}$ where $c_3 > 0$ is an absolute constant. Therefore the regularity of Θ_1 implies the regularity of Θ.

Let Θ_2, be the probability measure that we get from Θ_1 if we change only the randomization of d namely we pick d with uniform distribution from the interval $[1, n^{\xi(n-1)}]$. Clearly $\Theta_2(A) \ge \frac{1}{3}\Theta_1(A)$ for all $A \in \mathcal{X}$ and so the regularity of Θ_2 implies the regularity of Θ_1.

The remaining part of the proof of Lemma 5.10 is not needed for the proof of Theorem 3.8. The definition of the distribution Ψ and Lemma 4.2 implies that the distance of distributions Ψ and Θ_2 is at most $(\frac{1}{2}+\varepsilon)^n$, where we may assume that $\varepsilon > 0$. This fact and the inequalities between $\Theta(A)$, $\Theta_1(A)$, $\Theta_2(A)$ and $\Psi(A)$ imply the statement of the lemma. (Lemma 5.10)■

We continue the proof of Theorem 3.8. From the proof of Lemma 5.10 we know that the regularity of Θ_2 implies the regularity of Θ. Let Θ_3 be the distribution that we define the same way as Θ_2 with the only difference that we pick the integer d with uniform distribution from the integers of the interval $[1,(n-1)^{\xi(n-1)+\beta}]$ instead of the interval $[1,(n-1)^{\xi(n-1)}]$. Clearly for every $A \in \mathcal{X}$ we have $\Theta_2(A) \le \frac{1}{2}n^{-\beta}\Theta_3(A)$. Therefore the regularity of Θ_3 implies the regularity of Θ_2. Let Ψ' be the following distribution: we pick the realnumbers $\alpha_1,...,\alpha_{n-1}$ at random, independently and with uniform distribution from the interval $(0,1)$ with the condition that "$\exists j \in [1,(n-1)^{\xi(n-1)+\beta}]$ so that $[\![j\alpha_i]\!] \le (n-1)^{-\beta}$, $i = 1,...,n-1$". The smallest integer j with this property will be d and $\Psi'(X) = \mathtt{prob}(\langle d, \langle\alpha_1,...,\alpha_{n-1}\rangle\rangle \in X)$ for all $X \in \mathcal{X}$.

Remark 5.11. 10. The only difference between the distributions Ψ and Ψ' is that in Ψ' the integer j can be picked from the interval $[1,(n-1)^{\xi(n-1)+\beta}]$ while in Ψ it can be picked from the shorter interval $[1,(n-1)^{\xi(n-1)+\beta}]$.

According to Lemma 4.2 the distance of the distributions Θ_3 and Ψ' is at most $(\frac{1}{2}+\varepsilon')^n$ for all $\varepsilon'>0$ if n is sufficiently large. Therefore if Ψ' is regular then Θ_3 is also regular. To complete the proof of the regularity of Θ we have to show that Ψ' is regular.

Assume that a $\vartheta > \frac{1}{2}$ is fixed. We show that if n is sufficiently large and we randomize the pair $\langle d,q\rangle$ according to Ψ' then the probability that $\langle q,d\rangle$ is singular is at most ϑ^n. We apply Lemma 4.3 with $n\to n-1$, $\beta\to\beta$, $\rho\to\xi+\frac{\varepsilon}{2}$, $c\to\xi+\frac{\beta}{n-1}+\xi$, $\alpha_i\to\frac{q_i}{d}$. The choices $c_1=\beta$, $c_2=\frac{1}{2}\min\{\xi,\beta-\xi\}$ clearly meet the requirement of Lemma 4.3. The conclusion of the lemma implies that the probability that $\langle q,d\rangle$ is singular is at most ϑ^n.

Finally we prove inequality (2) of Theorem 1. The upper bound on u holds for every possible value of $u=\langle u_1,\dots,u_n\rangle$. Indeed by Lemma 5.5 each component of u is in the interval $[1,(n-1)^{-\beta}]$. We prove the lower bound by estimating ν, the number of components u_i of u with $|u_i|>\frac{1}{10}(n-1)^{-\beta}$. As we have seen already this inequality always holds for $i=n$. According to lemma 5.5 $|u_i|>[\![q_i]\!]+\frac{1}{10}(n-1)^{-\beta}$ therefore ν is not smaller then the number of integers $i\in[1,n-1]$ with $[\![q_i]\!]\geq\frac{1}{5}(n-1)^{-\beta}$. (20) implies that for each fixed i the probability of $[\![q_i]\!]\leq\frac{1}{2}(n-1)^{-\beta}$ is at least $\frac{3}{4}$. The random variables q_i, $i=1,\dots,n-1$ are mutually independent. Therefore the probability that $[\![q_i]\!]\geq\frac{1}{2}(n-1)^{-\beta}$ holds for less than $(n-1)^{1-\frac{1}{2}\varepsilon'}$ integers i in $[1,n-1]$ is at most $\binom{n-1}{(n-1)^{\frac{1}{2}\varepsilon'}}(\frac{1}{4})^{n-(n-1)^{1-\frac{1}{2}\varepsilon'}}<\vartheta^n$. Therefore with a probability of at least $1-\vartheta^n$ we have $\nu\geq(n-1)^{1-\frac{1}{2}\varepsilon'}$. Therefore $\|u\|\geq(n-1)^{\frac{1}{2}-\frac{1}{4}\varepsilon'}\frac{1}{10}(n-1)^{-\beta}$ which implies inequality (2) of Theorem 3.8. (Theorem 3.8)■

Proof of Theorem 3.9. Assume that contrary to our statement there is an algorithm $\mathcal{A}$ which solves problem **Q2** for some choice of ξ,β and γ with a probability of at least n^{-c_2} in time n^{c_1}. We show that using $\mathcal{A}$ as an oracle we can solve problem **Q1** (with parameters $c\to\xi$, $c'\to\beta-\xi$) in polynomial time with a polynomially large probability in contradiction to the Hardness Assumption.

Assume that the realnumbers $\alpha_1,..,\alpha_{n-1}$ are chosen at random independently and with uniform distribution from $(0,1)$ and with the condition that there is an integer $m\in[1,(n-1)^{\xi(n-1)}]$ so that $[\![m\alpha_i]\!]\leq(n-1)^{-\beta}$, $i=1,\dots,n-1$. We have to find such an m in polynomial time with a polynomially large probability. Let d be the smallest integer m with this property and let $q_i=d\alpha_i$, $q=\langle q_1,\dots,q_{n-1}\rangle$. The distribution of the pair $\langle d,\langle\frac{q_1}{d},\dots,\frac{q_{n-1}}{d}\rangle\rangle$ is Ψ. Assume now that a pair d,q, $d\in[1,n^{\xi(n-1)}]$, $q\in\prod_{i=1}^{n-1}(0,1)$ is fixed. For the moment we do *not* consider them as random variables. We may construct a lattice $L_{d,q}$ generated by the basis $e_1,\dots,e_{n-1},v$ described in the definition of random variable $\kappa_{Q,n}(\xi,\gamma,)$. Let A' be the set of all pairs $\langle d,\langle\frac{q_1}{d},\dots,\frac{q_{n-1}}{d}\rangle\rangle$ with the property that if $\mathcal{A}$ gets $L_{d,q}$ as an input ($q=\langle q_1,\dots,q_{n-1}\rangle$) then it returns a shortest nonzero vector with a probability of at least $\frac{1}{2}n^{-c_2}$ in time n^{c_1}, where the probability is taken for the random steps in $\mathcal{A}$. Our assumption about $\mathcal{A}$ implies that $\Theta(A')\geq\frac{1}{2}n^{-c_2}$. Let A be the set of all lattices in L which has a 2-unique shortest nonzero vector. Theorem 3.8 implies that $\Theta(A)\geq\Theta(A')-(\frac{3}{4})^n$ and so $\Theta(A)\geq\frac{1}{3}n^{-c^2}$. Therefore by Lemma 5.10 we have that $\Psi(A)\geq c'\Theta(A)\geq c''n^{-c_2}$, where $c''>0$ is an absolute constant.

This implies that if we pick $\langle d,\langle\frac{q_1}{d},\dots,\frac{q_{n-1}}{d}\rangle\rangle$ with distribution Ψ then with a polynomially large probability $\mathcal{A}$ finds a shortest nonzero vector in the lattice $L_{d,q}$ and this is $xv+\sum_{i=1}^n a_ie_i$, where $x,a_1,\dots,a_i$ are integers then $x=d$ and so we have found the solution of Problem **Q1**. (Theorem 3.9)■

6 The hardness of the n^c-unique SVP and the security of the cryptosystem

In this section we prove Theorem 3.13. The statement of the theorem differs only from the corresponding result about the second cryptosystem of [2] because the normal perturbations used in the definition of the system has different parameters. The improvement in the constant c (in n^c-uniqueness) is based on a result of Regev (Lemma 3.14 in [14]). Regev's proof is using a lemma of Banaszczyk given in [4].

We formulate our proof for System I, but based on this, in the same way as it is done in [5], the security of System II can be proved as well.

6.1 Notation, preliminaries

As we have already indicated earlier, in this section we will be interested algorithms whose inputs can be realnumbers.

In this section when realnumbers are inputs for algorithms we will consider them as oracles. For the formulation of the hardness assumption the binary form of realnumbers was satisfactory. Now we need a somewhat more sophisticated, treatment of the representations of reals. The reason is the following. In the hardness assumption the reals which served as inputs for algorithms were random realnumbers, chosen with uniform distribution from $(0,1)$ and therefore with probability 1 they had a unique representation. Moreover if the random real with this distribution was provided by another algorithm then this second algorithm was able to compute the bits of this unique binary representation of the realnumber α with the required precision in polynomial time for almost all α, where the set of exceptional numbers α is exponentially small. In this section we will deal with more complicated distributions, whose density function may be an arbitrary Borel measurable functions so these properties would be more difficult to check. However if we treat realnumbers as oracles then we avoid all of these problems.

The oracle representation of reals was introduced by Lovász in [10]. We will use this representation in our proofs. For the reader who is not familiar with this representation of the realnumbers we provide here a compact equivalent definition which has a more limited scope (e.g. we do not consider the issue of unifying the representation of integers, rational and reals). This simplified definition will be sufficient for our present purposes. The equivalence of the two oracle representation of the reals means, that they are equivalent from the point of view of polynomial time computation. In other words the times required by the same algorithm in the two different models can differ by only a polynomial factor.

Definition 6.1. • We assume that each realnumber is represented by an oracle. Suppose now that α is a fixed real and an algorithm has access to this oracle. The algorithm may get information about α in the following way. The algorithm gives a positive integer i as input to the oracle and the oracle returns a rational $\frac{t}{2^{i+1}}$, so that t is an integer and $|\alpha - \frac{t}{2^{i+1}}| \leq 2^{-i}$. We may think that the algorithm, by giving the integer i to the oracle, asks for an approximation of α with the described precision and in the described form. By definition the asking such a question and receiving the answer will count as $\lfloor \log_2(|\alpha|+1) \rfloor + i + 1$ additional time for the algorithm. (Roughly one time unit for each bit in the binary form of the number $\frac{t}{2^{i+1}}$.) The answer of the oracle is not uniquely determined. An answer meeting the listed requirements can be determined even by knowing only a rational approximation of α with a precision more than $\frac{1}{2^{i+1}}$ (and without knowing α itself). This is a crucial property if

another algorithm has to play the role of an oracle. When we say that an algorithm gives an output with property P at input α, we mean that the algorithm gives an output with property P for every possible choices of the answers provided by the oracle representing α.

The following definitions describe the normal perturbations that we use in our cryptosystem. Most of these definitions can be found in [14].

Definition 6.2. • Suppose that $L \subseteq \mathbf{R}^n$ is a lattice, $a_1, ..., a_n$ is a basis of L^* and $\mathcal{P} = \mathcal{P}(a_1, ..., a_n)$. Let D_{L^*} be a function on $\mathcal{P}$ defined by $D_{L^*}(x) = \sum_{y \in L^*} e^{-\pi \|x+y\|^2}$ for all $x \in \mathcal{P}$. It can be shown that D_{L^*} is a density function on $\mathcal{P}$ (see [14] and the next definition).

• We will denote by $\xi_{\mathtt{norm}}$ the random variable which takes its values in $\mathbf{R}^n$ and whose density function is $e^{-\pi \|x\|^2}$.

• If ξ is an arbitrary random variable with values in $\mathbf{R}^n$ then $(\xi)_{\mathcal{P}}$ will be the random variable defined in the following way: first we take a random value z of the random variable ξ. Let y be the unique element of $\mathcal{P}$ so that $z - y \in L^*$. y is the value of the random variable $(\xi)_{\mathcal{P}}$. For the special case $\xi = \xi_{\mathtt{norm}}$ we have that the density function of $(\xi_{\mathtt{norm}})_{\mathcal{P}}$ is D_{L^*}. (see [14]).

Remark 6.3. 11. We got a value of $(\xi_{\mathtt{norm}})_{\mathcal{P}}$ by perturbing 0 with a normal distribution and then reducing it modulo L^* to a point of $\mathcal{P}$. This is the way we encrypted the bit 1 in our cryptosystem.

Definition 6.4. • The random variable which takes its values from $\mathcal{P}$ with uniform distribution (with respect to the n-dimensional Lebesgue measure, that is, the n-dimensional volume) will be denoted by $U_{\mathcal{P}}$.

An encoding of the bit 0 in System I is a random value of $U_{\mathcal{P}}$ and encoding of the bit 1 is a random value of $(\xi_{\mathtt{norm}})_{\mathcal{P}}$, therefore the security of the system is equivalent to the following statement. First we define a random variable ζ. We take a random element δ with uniform distribution from the set $\{0,1\}$. Let $\zeta = U_{\mathcal{P}}$ if $\delta = 0$ and $\zeta = (\xi_{\mathtt{norm}})_{\mathcal{P}}$ if $\delta = 1$. The cryptosystem is secure if for any polynomial time probabilistic algorithm $\mathcal{B}$ and for all $c_1 > 0$, if n is sufficiently large and $\mathcal{B}$ gets n, b, t, and a random value of ζ as input and it gives a $0,1$ output Q, then we have $\mathtt{prob}((Q = 0 \wedge \zeta = U_{\xi}) \vee (Q = 1 \wedge \zeta = (\xi_{\mathtt{norm}})_{\mathcal{P}})) \leq \frac{1}{2} + n^{-c_1}$, where the probability is taken together for the randomization in ζ and the random steps of $\mathcal{B}$.

This means that if a polynomial time algorithm tries to guess whether a point in $\mathcal{P}$ has encoded a 1 or a 0 then the probability of success cannot be essentially larger than $\frac{1}{2}$.

In this section we will show that if the system is not secure in this sense then the vector u can be found in polynomial time.

Remark 6.5. 12. We have to add to the input of the algorithm $\mathcal{B}$ every information that is available from the lattice L. In System I this is the common random bits b and the public key t. Since these together determine the lattice L we do not have to add L to the input.

First we formulate the results from [14] that we will use in our proof. We have already defined the density function D_{L^*} on $\mathcal{P}$ which described a normal distribution reduced modulo L^* to $\mathcal{P}$.

Definition 6.6. • Suppose that $L, \mathcal{P}$ are the same as in the previous definition, $\det(L)$ is the determinant of L and u is a sh.n.v. in L. T_{L^*} will denote the function on $\mathcal{P}$ defined by

$$T_{L^*}(x) = \frac{\det(L)}{\|u\|} \sum_{k \in \mathbf{Z}} e^{-\pi (\frac{k+ux}{\|u\|})^2}$$

It can be shown that T_{L^*} is a density function on $\mathcal{P}$.

Remark 6.7. 13. From the point of view of the present paper the most important property of the function T_{L^*} is the following: there is function h defined on $\mathbf{R}$ with values in $\mathbf{R}$ so that for all $x \in \mathbf{R}^n$ we have $T_{L^*}(x) = h(ux)$.

Definition 6.8. • If f, g are density functions on $\mathcal{P}$ then by definition $\Delta(f,g) = \int_{\mathcal{P}} |f(x) - g(x)|dx$ where we integrate according to the n dimensional Lebesgue measure.

Lemma 6.9. (Regev) *Let $L \subseteq \mathbf{R}^n$ be a lattice with a sh.n.v. u so that each vector not parallel with u has length at least $n^{\frac{1}{2}}$. Then*

$$\Delta(D_{L^*}, T_{L^*}) < 2^{-\Omega(n)}(1 + \frac{1}{\|u\|})$$

In particular, if $\|u\| \geq \frac{1}{n^c}$ for some constant $c > 0$ then

$$\Delta(D_{L^*}, T_{L^*}) < 2^{-\Omega(n)}$$

Remark 6.10. 14. According to this lemma from the point of view of polynomial time computation the density function of $(\xi_{\mathtt{norm}})_{\mathcal{P}}$ at the point x depends only on the distance of x from the closest hyperplane of the type $\{x \in \mathbf{R}^n \mid xu = k\}$, $k \in \mathbf{Z}$.

We have already described the role of oracles representing realnumbers. We will use oracles in other roles as well. We will consider the situation e.g. when an algorithm has to decide whether two random variables has the same distribution. This is a reasonable question even if the random variables are not generated by the algorithm, but the algorithm gets their values from oracles.

Definition 6.11. • If ξ is a random variable then O_ξ will denote an oracle who provides a value of ξ upon a request of an algorithm. The various values of ξ provided to the same algorithm will be independent from each other. If the value of ξ is a finite sequence of realnumbers then these realnumbers will be available to the algorithm as oracles. We described here O_ξ with the assumption that it provides answers to an algorithm. Instead of an algorithm the answers may be given to another oracle, who needs the values of ξ as input.

• If ξ, η are random variables taking their values in $\mathbf{R}^n$ then the distance of ξ and η is defined as $\sup|\mathtt{prob}(\xi \in A) - \mathtt{prob}(\eta \in A)| + |\mathtt{prob}(\xi \in B) - \mathtt{prob}(\eta \in B)|$, where the supremum is taken for all disjoint pairs of Borel sets $\langle A, B\rangle$, with $A \subseteq \mathbf{R}^n$, $B \subseteq \mathbf{R}^n$, $A \cap B = \emptyset$.

Remark 6.12. 15. Suppose that for $i = 0, 1$ the random variables ξ_i, has density functions h_i on $\mathbf{R}^n$. Then

(21). $\text{distance}(\xi_0, \xi_1) = \int_{\mathbf{R}^n} |h_1(x) - h_0(x)|dx = \Delta(h_1, h_2)$.

A pair A, B where the supremum will be achieved in the definition of $\text{distance}(h_0, h_1)$ is $A = \{x \mid h_0(x) < h_1(x)\}$, $B = h_0(x) \geq h_1(x)$. The following observation will be used in our proofs:

Lemma 6.13. *Assume that ξ_i, $i = 0, 1$ are random variables with values in $\mathbf{R}^n$ and with Borel measurable density functions h_i, $i = 0, 1$ so that* $\text{distance}(\xi_0, \xi_1) < \varepsilon$. *Then there is a way to generate the random variables ξ_0, ξ_1 simultaneously so that* $\mathtt{prob}(\xi_0 - \xi_1 \neq 0) < \varepsilon$.

Proof. Let $X_i = \{\langle x,a\rangle \in \mathbf{R}^n \times \mathbf{R} \mid 0 \le a \le h_i(x)\}$ for $i = 0,1$. Since h_i is a density function, we have $\mathtt{vol}_{n+1}(X_i) = 1$, where $\mathtt{vol}_{n+1}$ is the $n+1$ dimensional Lebesgue measure. We may randomize ξ_i, $i = 0,1$ separately, by picking a random point $\langle x,a\rangle$ with uniform distribution with respect to $\mathtt{vol}_{n+1}$. x will be the value of ξ_i, for $i = 0,1$. Let $g = \min(h_0,h_1)$, and $\alpha = \int_{\mathbf{R}^n} g(x)dx$. distance$(\xi_0,\xi_1) < \varepsilon$ Clearly distance$(\xi_0,\xi_1) = 1-\alpha < \varepsilon$.

We generate ξ_i, for $i = 0,1$ simultaneously, by picking first a $0,1$ value δ so that $\delta = 1$ with probability α and $\delta = 0$ with probability $1-\alpha$. If $\delta = 0$, we pick a random point $\langle x,a\rangle$ from $X_0 \cap X_1$ with uniform distribution with respect to $\mathtt{vol}_{n+1}$. x is the value of both ξ_0 and ξ_1. If $\delta = 1$ then we pick random points $\langle x_i,a_i\rangle$ with uniform distribution form $X_i \backslash X_{1-i}$ (according to $\mathtt{vol}_{n+1}$) for both $i = 0$ and $i = 1$. x_i is the value of ξ_i for $i = 0,1$. $1-\alpha < \varepsilon$ implies the statement of the lemma. (Lemma 6.13)■

Definition 6.14. • Assume that $L \subseteq \mathbf{R}^n$ is a lattice, ξ is a random variable which takes its values in $\mathbf{R}^n$, and ξ has a Borel measurable density function g on $\mathbf{R}^n$. If $a_1,...,a_n$ is a basis of L and $\mathcal{P} = \mathcal{P}(a_1,...,a_n)$ then we define the random variable $\xi_{\mathcal{P}}$ by reducing each value of ξ to a point of $\mathcal{P}$ modulo the subgroup L in the group $\mathbf{R}^n$. (That is, if x is a value of ξ, then the corresponding value of $\xi_{\mathcal{P}}$ is the unique $y \in \mathcal{P}$ with $x-y \in L$.) It is easy to see that $\xi_{\mathcal{P}}$ has a density function $\bar{g}(x)$ and

(22). $\bar{g}(x) = \sum_{a\in L} g(x-a)$ for each $x \in \mathcal{P}$.

• Suppose that $a_1,...,a_n$ are linearly independent vectors in $\mathbf{R}^n$, $\mathcal{P} = \mathcal{P}(a_1,...,a_n)$, and $u \in \mathbf{R}^n$, $u \neq 0$. Assume further that η is a random variable taking its values in $\mathcal{P}$ with the density function h. We say that η is horizontal with respect to u, if for all $x,y \in \mathcal{P}$, $xu - yu \in \mathbf{Z}$ implies that $h(x) = h(y)$. Suppose that ζ is a random variable taking values on $\mathcal{P}$ and $\varepsilon > 0$. ζ is ε-horizontal with respect to u if there is an η so that η is horizontal with respect to u and the distance of η and ζ is at most ε.

• Assume that ξ,η are random variables. We take a random element δ with uniform distribution from the set $\{0,1\}$. Let $\zeta = \xi$ if $\delta = 0$ and $\zeta = \eta$ if $\delta = 1$. Suppose now that δ is fixed and T is an oracle which using O_ζ tries to decide whether $\zeta = \xi$ or $\zeta = \eta$. The oracle T provides a probabilistic $0,1$ answer $\bar{T}$ (with the intuitive meaning $\bar{T} = 1$ iff $\zeta = \xi$). Let $\alpha > 0$. Suppose that $\mathtt{prob}((\bar{T} = 1 \wedge \zeta = \xi) \vee (\bar{T} = 0 \wedge \zeta = \eta)) > \frac{1}{2} + \alpha$, where the probability is taken together for the choice of δ, for the randomization in O_ξ, and for the randomization in T. Then we say that T distinguishes ξ from η with a probability of $\frac{1}{2} + \alpha$.

• If $a \in \mathbf{Z}$ then size$(a) = \lceil \log_2(|a|+1) \rceil$. If $q \in \mathbf{Q}$ then size size$(q) = \min\{\text{size}(u) + \text{size}(v) \mid \frac{u}{v} = q, u,v, \in \mathbf{Z}\}$. Assume now that $x = \langle x_1,...,x_n\rangle \in \mathbf{Q}^n$. Then size$(x) = \sum_{i=1}^n \text{size}(x_i)$.

6.2 Finding the shortest vector by using oracles

In the following lemma an algorithm $\mathcal{A}$ will use an oracle T which distinguishes between random variables ξ and η with a given probability. The algorithm $\mathcal{A}$ will play the role of the oracle O_ζ and supplies the independent values of ζ to T. The algorithm will do this several times for different pairs ξ,η.

Definition 6.15. • Assume that L is a lattice and $u \in L$. u is called a primitive element of L, if $\alpha u \notin L$ for all realnumbers α with $0 < \alpha < 1$.

Lemma 6.16. *There is a probabilistic algorithm $\mathcal{A}$ so that for all $c_1 > 0$ and for all sufficiently large $c_2 > 0, c_3 > 0$ if n is a sufficiently large integer with respect to c_1,c_2,c_3 then the following holds. Suppose*

that $L \subseteq \mathbf{Q}^n$ is a lattice with determinant D, u is a 1-unique sh.n.v. of L, $a_1,...,a_n$ is a basis of L^*, $\mathrm{size}(u)+\sum_{i=1}^n \mathrm{size}(a_i) \le n^{c_1}$, $n^{-c_1} \le \|u\| \le n^{c_1}$, and $\mathcal{P} = \mathcal{P}(a_1,...,a_n)$. Assume further that ξ is a random variable with values in $\mathbf{R}^n$ and T is an oracle so that

(23). If g is the density function of ξ then for all $y \in \mathbf{R}^n$ with $\|y\| \le 1$ we have $\int_R |g(x)-g(x-y)|dx \le \frac{1}{2}n^{c_1}\|y\| + e^{-n}$, that is, the distance of the random variables ξ and $\xi + y$ is at most $\frac{1}{2}n^{c_1}\|y\| + e^{-n}$

(24). $\xi_{\mathcal{P}}$ is n^{-c_2}-horizontal with respect to u, and

(25). T distinguishes between the random variables $\xi_{\mathcal{P}}$ and $U_{\mathcal{P}}$ with a probability of at least $\frac{1}{2} + n^{-c_1}$.

Then $\mathcal{A}$, getting $n, a_1,...,a_n, c_1, c_2, c_3$ as input, and using the oracles O_ξ and T, finds u or $-u$ in time n^{c_3} with a probability of at least $1-n^{-c_1}$.

First we show that the lemma implies the security of System I (and so Theorem 3.13). Assume that the lattice L in Lemma 6.16 is $\tilde{L}(b,t)$, $\langle a_1,...,a_n\rangle = \langle f_1,...,f_n\rangle$, $\xi = \xi_{\mathtt{norm}}$ and also assume that contrary to our claim System I is not secure for this fixed L. As we have described earlier this means that there is a polynomial time test T which meets the requirements of (25). Lemma 6.17 below will imply that the requirements (23) and (24) are also met. Therefore Lemma 6.16 implies that the polynomial time algorithm, using the test T as an oracle can find a sh.n.v. in L with a probability close to one for this fixed value of L. Therefore if System I could be broken for a polynomially large fraction of the lattices $L = \tilde{L}(b,t)$ with the same polynomial time test T, (with respect to the randomization of both b and t) then algorithm $\mathcal{A}$ would find a sh.n.v. in a polynomially large fraction of the lattices, which, according to Theorem 3.9, contradicts our Hardness Assumption. (Theorem 3.13)■

Lemma 6.17. *For all $\varepsilon \in (0, \frac{1}{4})$, $c > \frac{1}{2}$, if $c_2 > 0, c_3 > 0$ are sufficiently large, n is a sufficiently large positive integer, $L \subseteq \mathbf{R}^n$, is a lattice and u is an n^c-unique sh.n.v. of L, $n^{-\frac{\varepsilon}{2}} \le \|u\| \le n^{-\frac{\varepsilon}{3}}$ and $\xi = \xi_{\mathtt{norm}}$, $\mathcal{P} = \mathcal{P}(a_1,...,a_n)$, where $a_1,...,a_n$ is a basis of L^* then conditions (23), (24) of Lemma 6.16 are satisfied.*

Proof of Lemma 6.17. According to the definition of $\xi_{\mathtt{norm}}$, its density function is $g(x) = e^{-\pi x^2}$. Let $B_n(R)$ be the closed ball in $\mathbf{R}^n$ with radius R around 0. $\int_R |g(x)-g(x-y)|dx = \int_{B_n(n^2)} |g(x)-g(x-y)|dx + \int_{R\setminus B_n(n^2)} |g(x)-g(x-y)|dx$. For the estimate of the first integral we use that the directional derivative of $g(x) = e^{-\pi x^2}$ in any direction in absolute value is a most $2\pi\|x\|e^{-\pi x^2}$ which, in $B_n(n^2+1)$, is at most $8(n+1)^2 g(x)$. Therefore $\int_{B_n(n^2)} |g(x)-g(x-y)|dx \le \int_{B_n(n^2)} |g(x)|8(n+1)^2\|y\|dx = 8(n+1)^2\|y\| \int_{B_n(n^2)} g(x)dx = 8(n+1)^2\|y\| \le \frac{1}{2}n^{c_1}\|y\|$.

For the estimate of $\int_{R\setminus B(n^2)} |g(x)-g(x-y)|dx$ and let $\gamma_n = \mathtt{vol}_n B_n(1)$. It is known that $\gamma_n = \pi^{\frac{n}{2}}(\Gamma(\frac{n}{2}+1))^{-1} \le e^{-\frac{1}{2}n\log n + 2n}$. Therefore if n is sufficiently large then $\gamma_n \le \frac{1}{2}e^{-n}$.

$\int_{\mathbf{R}^n\setminus B(n^2)} |g(x)-g(x-y)|dx \le 2\int_{\mathbf{R}^n\setminus B(n^2-1)} e^{-\pi x^2}dx \le 2\sum_{k=n^2}^{\infty} \gamma_n(k+1)^2 e^{-k^2} \le \gamma_n < e^{-n}$ if n is sufficiently large, which completes the proof of (23).

Condition (24) is an immediate consequence of Regev's lemma (Lemma 6.9). Indeed the density function of $(\xi_{\mathtt{norm}})_{\mathcal{P}}$ is D_{L^*}. T_{L^*} is a density function and its defining formula shows that it is horizontal with respect to u. Lemma 6.9 shows that the distance of the two density functions is exponentially small. (Lemma6.17)■

6.3 The proof of Lemma 6.16

Proof of Lemma 6.16. We describe the algorithm $\mathcal{A}$. Let ν be the smallest positive integer so that $L \subseteq \frac{1}{\nu}\mathbf{Z}^n$ and $L^* \subseteq \frac{1}{\nu}\mathbf{Z}^n$. Clearly size$(\nu) \leq n^{c_1'}$ where c_1' depends only on c_1. Let $d_1,...,d_n$ be the dual basis of $a_1,...,a_n$. $d_1,...,d_n$ is a basis of L. Let $M = n^2 + \|u\| + \sum_{i=1}^n \|d_i\| + \sum_{i=1}^n \|a_i\|$. Let H be the subspace of $\mathbf{R}^n$ orthogonal to u, let $d = \|u\|^{-1}$ and for all $\alpha \geq 0$ let $H(\alpha) = \{x \in \mathbf{R}^n \mid |dxu| \leq \alpha\}$, that is, $x \in H(\alpha)$ iff the distance of x from H is at most α. $\mathcal{A}$ will select a sequence $b_1,...,b_{n-1}$ of pairwise orthogonal vectors from $\mathbf{R}^n$ so that

(a) $b_i \in H(d)$ for all $i = 1,...,n-1$, and

(b) $\|b_i\| = N$ where $N = 8nM^4\nu^\chi$ and χ is a sufficiently large constant.

First we show that in the knowledge of such a sequence $b_1,...,b_{n-1}$ we can find the vector u (or $-u$). We will use the following lemma in the proof:

Lemma 6.18. *Assume that $f_1,...,f_n$ are vectors in an n-dimensional Euclidean space V and $\sigma > 0$, so that $\|f_i\| = 1$ and $|f_i f_j| < \sigma$ for all $i \neq j$, $i,j \in \{1,...,n\}$. Then, for all $v = \sum_{i=1}^n \alpha_i f_i$ we have*

(26). $\|v\|^2 = (1+R_1)\sum_{i=1}^n \alpha_i^2$, where $|R_1| \leq n^2\sigma$.

(27). $\alpha_i = (1+R_2)vf_i$, where $|R_2| \leq \sigma n^{\frac{1}{2}}(\sum_{i=1}^n \alpha_i^2)^{\frac{1}{2}}$. If $\sigma < n^{-2}$ then $|R_2| < 2\sigma n^{\frac{1}{2}}\|v\|^2$

(28). if $\sigma < \frac{1}{2}n^{-2}$ then the vectors $f_1,...,f_n$ are linearly independent.

Proof. $\|v\|^2 = \sum_{i=1}^n \alpha_i^2 + \sum_{i\neq j} \alpha_i\alpha_j f_i f_j$. $|R_1| = |\sum_{i\neq j} \alpha_i\alpha_j f_i f_j| \leq \sigma \sum_{i\neq j} |\alpha_i||\alpha_j| \leq \sigma n^2 \sum_{i=1}^n \alpha_i^2$ which completes the proof of (26).

$vf_i = (\sum_{j=1}^n \alpha_j f_j)f_i = \alpha_i + \sum_{j\neq i} \alpha_j f_j f_i$. $|R_2| = |\sum_{j\neq i} \alpha_j f_j f_i| \leq \sigma \sum_{j=1}^n |\alpha_j| \leq \sigma n^{\frac{1}{2}}(\sum_{j=1}^n \alpha_j^2)^{\frac{1}{2}}$. If $\sigma < n^{-2}$ then (26) implies that $\sum_{j=1}^n \alpha_j^2 \leq 2\|v\|^2$ and so $|R_2| \leq 2\sigma n^{\frac{1}{2}}\|v\|$ as claimed in (27).

To prove (28) we note that if $\sigma < \frac{1}{2}n^{-2}$ then (26) implies that $\|v\|^2 \geq \frac{1}{2}\sum_{i=1}^n \alpha_i^2$ provided that $v = \sum \alpha_i f_i$. Therefore if not all of the reals α_i, $i = 1,...,n$ are 0 then $\|v\| > 0$ and so $v \neq 0$, which implies the linear independence of the vectors $f_1,...,f_n$. (Lemma 6.18)■

Let v be one of the two vectors of length 1 which are orthogonal to $b_1,...,b_{n-1}$. Let $b_i = b_i' + b_i''$, $i = 1,...,n-1$ and let $v = v' + v''$ where $v', b_1', ..., b_{n-1}' \in H$ and $v'', b_1'', ..., b_{n-1}''$ are orthogonal to H and so parallel to u. For each $i = 1,...,n-1$ we have $vb_i = 0$ and so $v'b_i' + v'b_i'' + v''b_i' + v''b_i'' = 0$. Since $v' \perp b_i''$ and $v'' \perp b_i'$ while v'' and b_i'' are parallel this yields $v'b_i' \pm \|v''\|\|b_i''\| = 0$. Since $u \in \frac{1}{\nu}\mathbf{Z}^n$ we have $d = \|u\|^{-1} \leq \nu$ and so, by property (a), $\|b_i''\| \leq d \leq \nu$. This and $\|v'\| \leq \|v\| \leq 1$ implies that

(29). $|v'b_i'| \leq \nu$ for all $i = 1,...,n-1$.

Let $f_i = \|b_i'\|^{-1}b_i'$. For $i \neq j$ we have $|b_i'b_j'| = |(b_i - b_i'')(b_j - b_j'')| \leq |b_ib_j| + |b_ib_j''| + |b_i''b_j| + |b_in''b_j''| \leq Nd + dN + d^2$. Therefore $0 \leq d \leq \nu$ implies $|b_i'b_j'| = 2N\nu + \nu^2$. $\|b_i'\| \geq \|b_i\| - \|b_i''\| \geq \frac{3}{4}N$ consequently we have $|f_if_j| \leq (\frac{3}{4})^{-2}N^{-2}(2N + \nu^2) \leq 8N^{-1}\nu$.

We apply Lemma 6.18 with $n \to n-1$, f_i, $i = 1,...,n-1$, and with $\sigma \to 8N^{-1}\nu$. Let $v' = \sum_{i=1}^{n-1} \alpha_i f_i$. (29) implies that $|v'f_i| \leq \frac{2}{N}v'b_i' \leq \frac{2}{N}\nu$. Therefore by (27) we have $\alpha_i \leq 4N^{-1}\nu$ and so according to (26) $\|v'\|^2 \leq 8n\nu N^{-1} \leq M^{-4}\nu^{-(\chi-1)}$.

Let $w = \frac{u}{\|u\|} = \langle w_0,...,w_n\rangle$. We have $v = v' + v''$, $\|v\| = 1$, $\|v'\| \leq M^{-4}\nu^{-(\chi-1)}$, where u and v'' are parallel. $\|v''\| \geq \|v\| - \|v'\| \geq 1 - M^{-4}\nu^{-(\chi-1)}$, therefore $\|v-w\|_\infty \leq \|v-w\| \leq \|v-v''\| + \|v''-$

$w\| \leq M^{-4}\nu^{-(\chi-1)} + M^{-4}\nu^{-(\chi-1)} \leq 2M^{-4}\nu^{-(\chi-1)}$. Let $j \in \{1,...,n\}$ so that $|v_j|$ is maximal where $v = \langle v_1,...,v_n\rangle$. $\|v\| = 1$ implies $|v_j| \geq n^{-\frac{1}{2}}$ and $|w_j| \geq |v_j| - 2M^{-4}\nu^{-(\chi-1)} \geq \frac{1}{2}n^{-\frac{1}{2}}$. Let $\bar{v} = \langle \frac{v_1}{v_j},...., \frac{v_n}{v_j}\rangle$ and $\bar{w} = \langle \frac{w_1}{w_j},...., \frac{w_n}{w_j}\rangle$. We have $\|\bar{v} - \bar{w}\|_\infty = \|\frac{v}{v_j} - \frac{w}{w_j}\|_\infty \leq \|\frac{v}{v_j} - \frac{v}{w_j}\|_\infty + \|\frac{v}{w_j} - \frac{w}{w_j}\|_\infty \leq \frac{|w_j - v_j|}{|v_j||w_j|}\|v\|_\infty + \frac{1}{|w_j|}\|v - w\|_\infty \leq 2M^{-4}\nu^{-(\chi-1)}2n + 2n^{\frac{1}{2}}2M^{-4}\nu^{-(\chi-1)} \leq 5nM^{-4}\nu^{-(\chi-1)}$. Therefore $\|\bar{v} - \bar{w}\| \leq 5n^{\frac{3}{2}}M^{-4}\nu^{-(\chi-1)} \leq M^{-3}\nu^{-(\chi-1)}$.

Clearly $\bar{w} = \bar{u} = \frac{1}{u_j}\langle u_1,...,u_n\rangle$, where $u = \langle u_0,...,u_n\rangle$. The coefficients of $\bar{u}$ are rationals whose denominators are at most $M\nu$. Therefore we get $\bar{u}$ from $\bar{v}$ if we replace each coefficient r of $\bar{v}$ by the unique rationals with denominator at most $M\nu$ whose distance from r is at most $\frac{1}{3}(M\nu)^{-2}$. (These rationals are unique since the distance of two distinct rationals with denominators at most $M\nu$ is at least $\frac{1}{(M\nu)^2}$.) Once we have $\bar{u}$ we may get $\pm u$ by determining the smallest integer k so that $k\bar{u} \in U$, which can be done by e.g. considering the determinant of the lattice generated by L and $\bar{u}$.

Now we return to the selections of the vectors $b_1,...,b_{n-1}$. $\mathcal{H}$ will denote the set of all hyperplanes $H + i\|u\|^{-2}u$, where i is an integer. (These are the cosets of the subspace H which contain points from L^*.) We assume that the constant $c_1 > 0$ is fixed with the properties in Lemma 6.16 and constants $c_4 > 0, c_5 > 0, c_6 > 0$ are also fixed so that $c_1 \ll c_4 \ll c_5 \ll c_6$, where $a \ll b$ stands for "b is sufficiently large with respect to a".

In the selection of the vectors b_i, the algorithm $\mathcal{A}$ will use a test $T_1(x)$ which is a probabilistic algorithm with access to the oracles O_ξ, and T. Given an $x \in \mathbf{R}^n$ as input, in time n^{c_6}, the test computes a $0,1$ value $T_1(x)$ with the following properties:

(30). For any fixed $x \in \mathbf{R}^n$ with a probability of at least $1 - n^{-c_5}$ we have the following:

(31). if $x \in H(2d\sqrt{n})\backslash H(d)$ then $T_1(x) = 0$, and

(32). if $x \in H(n^{-c_4}d)$ then $T_1(x) = 1$.

Condition (30) determines the outcome of the test T_1 only in certain layers parallel to the subspace H in the n dimensional space. (See Figure 2). The behavior of the test at other places has no relevance for our proof.

Before we show that such a test T_1 exists we describe the selection of the vectors $b_1,...,b_{n-1}$ using test T_1. $\mathcal{A}$ determines the pairwise orthogonal vectors $b_1,...,b_{n-1}$ by recursion through the following steps. Assume that $b_1,...,b_i$ are already given so that they are pairwise orthogonal and satisfy (a) and (b). We pick a sequence of vectors $s_0, s_1,...$ so that their lengths grows exponentially and the first one longer than N will determine the direction of b_{i+1}.

(i) pick a vector $s_0 \in \mathbf{R}^n$, so that s_0 is orthogonal to $b_0,...,b_i$, $\|s_0\| \geq d$, and $T_1(s_0) = 1$ (and so with high probability $s_0 \in H(d)$).

(ii) suppose that a vector $s_j \in H(d)$ is given. Choose a vector $s_{j+1} \in \mathbf{R}^n$ so that s_{j+1} is orthogonal to, $b_1,...,b_i$, $\|s_{j+1}\| \geq 2\|s_j\|$, and $T_1(s_{j+1}) = 1$ (and so with high probability $s_{j+1} \in H(d)$).

(iii) If $\|s_j\| \geq N$ then let $b_{i+1} = N\|s_j\|^{-1}s_j$.

Since $\|s_0\| \geq d$ and $\|s_{j+1}\| \geq \|2s_j\|$ the definition of N implies that $b_{i+1} = N\|s_j\|^{-1}s_j$ for a $j \leq n^{c'}$, where c' depends only on c_1.

$\mathcal{A}$ can execute steps (i) and (ii) in the following way.

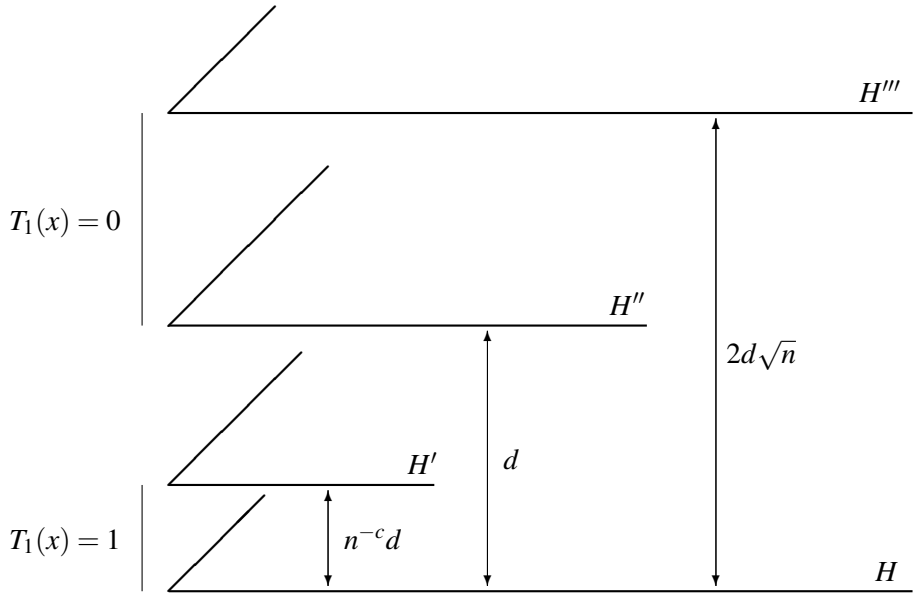

Figure 2: H', H'' resp. H''' are hyperplanes parallel to the subspace H at a distance $n^{-c}d, d$ resp. $2d\sqrt{n}$ from it. They are all on the same side of H. On that side of the subspace H there are two layers, as shown on the figure, where condition (30) uniquely determines the value of the test T_1. The behavior of T_1 is symmetric to H.

Step (i). We pick random vectors $x \in \mathbf{R}^n$ independently and with uniform distribution from the set of all vectors x orthogonal to $b_1,...,b_i$ with the property $\|x\| \leq 2d$. Since this set is an $n-i$ dimensional ball with radius $2d$ it is easy to see that if we took n^{c_4+1} random vectors x and perform the test T_1 for each of them then, with a probability exponentially close to one, at least one of them will meet the requirement $T_1(x) = 1$. s_0 is the first x with this property.

Step (ii). We pick now random points from an $n-i$-dimensional ball whose points are the vectors in $\mathbf{R}^n$ orthogonal to $b_1,...,b_i$ and whose distance from $2s_j$ is at most $2dn^{\frac{1}{2}}$. In a similar way as in step (i), it is easy to see that if we took n^{c_4+2} random points x independently, then with an exponentially high probability, for at least one of them we will have $T_1(x)$ and simultaneously $\|s_{j+1}\| \geq 2\|s_j\|$. s_{j+1} is the first x with this property.

The definition of the sequence s_j implies that the sequence $b_1,...,b_{n-1}$ will satisfy the conditions (a) and (b) with a probability of greater than n^{-c_1}. Since we have already shown how to find the vector u in the knowledge of such a sequence, to complete the proof of Lemma 6.16 it is sufficient to construct the test T_1 with the properties described in (30). First we construct a test T_2 with the similar properties that we want from T_1 namely we want T_2 to meet the following requirements, where c_6 is a constant with $c_5 \ll c_6$:

(33). For any fixed $x \in \mathbf{R}^n$ with a probability of at least $1-n^{-c_6}$ we have the following:

(34). if $|ux-1| \leq n^{-c_4}$ then $T_2(x) = 0$.

(35). if $x \in H(n^{-c_4}d)$ then $T_2(x) = 1$.

The test T_2 is the following. Suppose that a vector x is fixed. Let $\xi' = \xi + \mu x$, where μ is taken with uniform distribution from the interval $(0,1)$. We perform $l = n^{c_7}$ times the test T with $\xi'_{\mathcal{P}}$, where $c_7 > 0$ is a constant sufficiently large with respect to c_2 and c_6. If more than half of the times the test says that $\xi'_{\mathcal{P}}$ is not the uniform distribution then $T_2(x) = 1$, otherwise $T_2(x) = 0$.

To show that T_2 meets the requirements of (33) it is sufficient to prove the following two statements

(36). if $x \in H(n^{-c_4}d)$ then the distance of $\xi_{\mathcal{P}}$ and $\xi'_{\mathcal{P}}$ is smaller than n^{-c_1-1},

(37). if $|ux-1| \leq n^{-c_4}$ then the distance of $U_{\mathcal{P}}$ and $\xi'_{\mathcal{P}}$ is smaller than n^{-c_1-1}.

Indeed suppose that (36) and (37) hold. Lemma 6.13 implies that the T performed on random variables that are close to each other give similar results where the difference of the acceptance rate can be estimated from the distance of the random variables.

For the proof (36) and (37) we need the following two lemmata.

Definition 6.19. • If α is a realnumber then $\langle\langle\alpha\rangle\rangle$ will denote the number $\alpha - \lfloor\alpha\rfloor$. In other words $\langle\langle\alpha\rangle\rangle$ is the distance of α from the largest integer not exceeding α.

• Suppose that $L \subseteq \mathbf{R}^n$ is a lattice, u is a primitive element of L, $a_1,...,a_n$ is a basis of L^*, and $\mathcal{P} = \mathcal{P}(a_1,...,a_n)$. For each $\alpha \in [0,1)$ we will denote by $\mathcal{P}_{\alpha,u}$ the set $\{x \in \mathcal{P} \mid \langle\langle xu\rangle\rangle = \alpha\}$. For each realnumber β, $\mathcal{L}_{\beta,u}$ will denote the hyperplane $\{x \in \mathbf{R}^n \mid xu = \beta\}$.

• For each real α there is a finite number of reals $\beta_1,...,\beta_k$ so that $\mathcal{P}_{\alpha,u} = \bigcup_{i=1}^k \mathcal{P} \cap \mathcal{L}_{\beta_i,u}$. On each hyperplane $\mathcal{L}_{\gamma,u}$ we will consider the $n-1$-dimensional Lebesgue measure $\mathtt{vol}_{n-1}$. We may extend $\mathtt{vol}_{n-1}$ in a natural way to the union of a finite number of hyperplanes. With this definition we have $\mathtt{vol}_{n-1}(\mathcal{P}_{\alpha,u}) = \sum_{i=1}^k \mathtt{vol}_{n-1}(\mathcal{P} \cap \mathcal{L}_{\beta_i,u})$.

Lemma 6.20. *If $L \subseteq \mathbf{R}^n$ is a lattice, u is a primitive element of L, $a_1,...,a_n$ is a basis of L^*, and $\mathcal{P} = \mathcal{P}(a_1,...,a_n)$, then for all $\alpha \in [0,1)$ we have* $\mathtt{vol}_{n-1}(\mathcal{P}_{\alpha,u}) = \|u\|^{-1}\mathtt{vol}_n(\mathcal{P}) = \|u\|\det(L^*)$

Proof. First we show that $\mathtt{vol}_{n-1}(\mathcal{P}_{\alpha,u})$ does not depend on α. Let A_R be the set of all points in $\mathbf{R}^n$ whose orthogonal projection to the subspace $H = \mathcal{L}_{0,u}$ has a norm less than R and whose distance from H is also less than R. A_R is a cylinder of radius R and height $2R$. Let P be the set of all parallelepipeds $a+\mathcal{P}$ where $a \in L^*$, let P_R be the set of those elements of P which are contained in A_R and let P'_R be the set of those elements of P which has a nonempty intersection with A_R. If M is the diameter of $\mathcal{P}$ then clearly $A_{R-M} \subseteq \bigcup P_R \subseteq \bigcup P'_R \subseteq A_{R+M}$ and so $\mathtt{vol}_n(A_{R-M}) \leq |P_R|\mathtt{vol}_n(\mathcal{P}) \leq |P'_R|\mathtt{vol}_n(\mathcal{P}) \leq \mathtt{vol}_n(A_{R+M})$. This implies that

(38). $\lim_{R\to\infty} |P'_R - P_R||P_R| = 0$.

For $\gamma \in [0,1)$ let $Q_{\gamma,R}$ be the set of all realnumbers r with $\langle\langle r\rangle\rangle = \gamma$ and $\gamma \in (-R,R)$ and let T_γ be the set of all $x \in A_r$ with $\langle\langle xu\rangle\rangle = \gamma$. We have $2R\|u\|^{-1} - 2 \leq |Q_{\gamma,R}| \leq 2R\|u\|^{-1} + 2$

Let $S_{\gamma,R} = \mathtt{vol}_{n-1}(A_R \cap \bigcup_{r\in Q_{\gamma,R}} \mathcal{L}_{r,u})$. We have

(39). $S_{\gamma,R} = |Q_{\gamma,R}|\mathtt{vol}_{n-1}(B_{n-1}(r)) = (1 + R_0^{(R,\gamma)})2R\|u\|^{-1}\mathtt{vol}_{n-1}(B_{n-1}(R))$, where $B_{n-1}(R) =$ is an $n-1$-dimensional ball with radius R and for each fixed γ, $\lim_{R\to\infty} |R_0^{(R,\gamma)}|$.

$S_{\gamma,R} = \bigcup_{X\in P_R} X \cap S_{\gamma,R} \cup \bigcup_{Y\in P_R\setminus P'_R} S_{\gamma R}$. Therefore $\mathtt{vol}_{n-1}(S_{\gamma,R}) = |P_R|\mathtt{vol}_{n-1}(\mathcal{P}_{\alpha,u}) + R_1$, where $|R_1| \leq |P'_R - P_R|\mathtt{vol}_{n-1}(\mathcal{P}_{\gamma,u})|$. By (38) this yields $\mathtt{vol}_{n-1}(\mathcal{P}_{\alpha,u}) = |\mathcal{P}_R^{-1}|\mathtt{vol}_{n-1}(S_{\gamma,R}) + R_2$ where $\lim_{R\to\infty} |R_2| = 0$. Together with (39) this shows that $\mathtt{vol}_{n-1}(\mathcal{P}_{\gamma,u})$ does not depend on γ.

Let ν be the common value of $\mathcal{P}_{\gamma,u}$ for all $\gamma \in [0,1)$. We may get the value of ν if we compute the volume of the parallelepiped $\mathcal{P}$ by integrating the $n-1$-volumes of the sets $\mathcal{P}_{\alpha,u}$: $\mathtt{vol}_n(\mathcal{P}) = \int_0^1 \|u\|^{-1}\mathtt{vol}_{n-1}(\mathcal{P}_{\alpha,u})d\alpha = \int_0^1 \|u\|^{-1}\nu d\alpha$. That is $\mathtt{vol}_n(\mathcal{P}) = \nu\|u\|^{-1}$. (Lemma 6.20)■

Lemma 6.21. *Assume that ξ is a random variable whose values are in $\mathbf{R}^n$ and which has a Borel measurable density function. Then we have:*

(40). if ξ satisfies condition (24) of Lemma 6.16 then for all fixed $z \in \mathbf{R}^n$ the random variable $\xi + z$ also satisfies this condition. Moreover if $z \in H$ then distance$(\xi_\mathcal{P}, (\xi+z)_\mathcal{P}) \leq 2n^{-c_2}$.

(41). if ξ satisfies condition (23) of Lemma 6.16 and $y \in \mathbf{R}^n$, $\|y\| \leq 1$, then the distance of the random variables $\xi_\mathcal{P}$ and $(\xi+y)_\mathcal{P}$ is at most $\frac{1}{2}n^{c_1}\|y\| + e^{-n}$.

Proof. If $g(x)$, is the density function of ξ defined for $x \in \mathbf{R}^n$ then $g(x-z)$ is the density function of $\xi + z$. Moreover for the density functions $\bar{g}$ resp. $\bar{g}_z$ of $\xi_\mathcal{P}$ resp. $(\xi+z)_\mathcal{P}$ (defined only on $\mathcal{P}$) we have that $\bar{g}_z(x) = \bar{g}(x-z)$ if we reduce $x-z$ modulo L to an element of $\mathcal{P}$.

Assume that η is a random variable defined on $\mathcal{P}$ so that η is horizontal with respect to u and the distance of η and $\xi_\mathcal{P}$ is at most α for some realnumber $\alpha > 0$. If the density function of η is $f(x)$ then the density function of $\eta + z$ is $f(x-z)$, where we have to reduce $x-z$ modulo L the same way as above. Therefore distance of $(\eta+z)_\mathcal{P}$ and $(\xi+z)_\mathcal{P}$ is the same as the distance between η and ξ. Since $(\eta+z)_\mathcal{P}$ is clearly horizontal this completes the proof of the first part of (40)

If $z \in H$ then the horizontality of η implies that η and $(\eta+z)_{\mathcal{P}}$ has the same distribution, and therefore their distance is 0. As a consequence distance$(\xi_{\mathcal{P}},(\xi+z)_{\mathcal{P}}) \le$ distance$(\xi_{\mathcal{P}},\eta)+$ distance$(\eta,(\eta+z)_{\mathcal{P}})+$ distance$((\eta+z)_{\mathcal{P}},(\xi+z)_{\mathcal{P}}) \le 2n^{-c_2}$.

For the proof of the second statement of the lemma let $\bar{g}$ be the density function of $\xi_{\mathcal{P}}$. According to (22) we have $\bar{g}(x)=\sum_{\in L} g(x-a)$ for all $x \in \mathcal{P}$. The density function of $\xi+y$ is $\bar{g}(x-y)$, where we take a representative $x-y$ modulo L so that $x-y \in \mathcal{P}$. Therefore the distance of ξ and $\xi+y$ is $\int_{x\in\mathcal{P}} |\bar{g}(x)-\bar{g}(x-y)|dx \le \sum_{a\in L}\int_{a+\mathcal{P}} |g(x)-g(x-y)|dx = \int_{\mathbf{R}^n} |g(x)-g(x-y)|dx$. According to (23) the last integral is at most $\frac{1}{2}n^{c_1}\|y\|+e^{-n}$. (Lemma 6.21)■

We return now to the proof of the properties (36) and (37) of test T_2.

Proof of (36). Suppose $x \in H(n^{-c_4}d)$. For a fixed value of μ_0 of μ let h_{μ_0} be the density functions of $(\xi+\mu_0 x)_{\mathcal{P}}$. Clearly we have that if h is the density function of $(\xi+\mu x)_{\mathcal{P}}$ then

(42). $h(z)=\int_0^1 h_y(z)dy$.

Therefore (21) implies that it is sufficient to show that for each fixed $\mu_0 \in (0,1)$ the distance of $\xi_{\mathcal{P}}$ and $(\xi+\mu_0 x)_{\mathcal{P}}$ is at most n^{-c_1-1}. We may write $\mu_0 x$ in the form of $z+w$, where $z \in H$ and w is orthogonal to it and $\|w\|=n^{-c_4}d$. Using both parts of Lemma 6.21 and $d=\|u\|^{-1}$ we get:

distance$(\xi_{\mathcal{P}},(\xi+\mu_0 x)_{\mathcal{P}}) \le$ distance$(\xi_{\mathcal{P}},(\xi+z)_{\mathcal{P}})+$ distance$((\xi+z)_{\mathcal{P}},(\xi+z+w)_{\mathcal{P}}) \le n^{-c_2}+\frac{1}{2}n^{c_1}\|w\|+e^{-n} \le n^{-c_2}+\frac{1}{2}n^{c_1}n^{-c_4}d+e^{-n} \le n^{-c_2}+n^{2c_1-c_4} \le n^{-c_1-1}$. This completes the proof of (36).

Proof of (37). Assume now that an x is fixed with $|ux-1| \le n^{-c_4}$. Let h be the density function of $(\xi+\mu x)_{\mathcal{P}}$. We have to prove that

(43). $\int_{\mathcal{P}} |h(z)-\frac{1}{D}|dz \le n^{-c_1-1}$ or equivalently $\int_0^1 \int_{\mathcal{P}_{\gamma,u}} |h(z-\frac{1}{D})|dz\|u\|^{-1}d\gamma \le n^{-c_1-1}$.

Let $\gamma \in [0,1)$ so that $\xi+\mu x \in \mathcal{P}_{\gamma,u}$. The uniformity of μ implies that

(44). γ is uniform on the interval $X=(n^{-c_4},1-n^{-c_4})$ and the probability of $\gamma \in X$ is at most $4n^{-c_4}$.

Since $\xi+\mu_0 x$ is n^{-c_2} horizontal for each fixed value μ_0 of the random variable μ we have that for each $\gamma \in [0,1)$ there is a $q(\gamma)$ so that $\int_0^1 \int_{\mathcal{P}_{\mu_0,u}} |h(z)-q(\gamma)|d\mathtt{vol}_{n-1}\|u\|^{-1}d\gamma \le n^{-c^2}$. It is easy to see that the optimal choice for $q(\gamma)$ if we want to minimize the integral is the average value of $h(z)$ on the set $\mathcal{P}_{\gamma,u}$, that is, $q(\gamma)=(\mathtt{vol}_{n-1})^{-1}\int_{\mathcal{P}_{\gamma,u}} |h(z)-q(\gamma)|d\mathtt{vol}_{n-1}$. Therefore we have:

(45). $\int_0^1 \int_{\mathcal{P}_{\mu_0,u}} |h(z)-q(\gamma)|d\mathtt{vol}_{n-1}\|u\|^{-1}d\gamma \le n^{-c^2}$, where $q(\gamma)=(\mathtt{vol}_{n-1})^{-1}\int_{\mathcal{P}_{\gamma,u}} |h(z)-q(\gamma)|d\mathtt{vol}_{n-1}$.

We claim (44), (45) and the statement

(46). for all $\gamma \in [0,1)$ we have $\mathtt{vol}_{n-1}(\mathcal{P}_{\gamma,u})=\|u\|^{-1}\mathtt{vol}_n(\mathcal{P})=\|u\|\det(L^*)$

that follows from Lemma 6.20 already imply the inequality (43). To prove this first we show such an implication in a more abstract setting and then we apply it to the present situation.

Lemma 6.22. *Assume that μ is a measure defined on a σ-algebra consisting of subsets of the set M, and τ is a measure defined on a σ-algebra consisting of subsets of the set T, $Z \subseteq M\times T$ is a $\mu\times\tau$ measurable set, $f(x,y)$ is a $\mu\times\tau$-measurable function defined for $\langle x,y\rangle \in Z$, and ε,δ are realnumbers with $0<\varepsilon<\frac{1}{10}$, $\delta>0$. Suppose further that for all $x\in M$, $G_x=\int_{Z_x} f(x,y)d\tau_y$, $Z_x=Z\cap(\{x\}\times T)$, and the following conditions are satisfied:*

(47). $\mu(X) = 1$ and for all $x \in M$, $\tau(Z_x) = 1$

(48). $f(x,y) \geq 0$ for all $\langle x,y\rangle \in Z$

(49). $\int_M \int_{Z_x} f(x,y) d\tau_y d\mu_x = 1$

(50). there exists a μ-measurable $X \subseteq M$ and a realnumber g so that $\mu(X) < \varepsilon$, $\int_X \int_{Z_x} f(x,y) d\tau_y \mu_x < \varepsilon$ and for all $x \in M \backslash X$ we have $G_x = g$.

(51). for all $x \in M$, $\int_{Z_x} |f(x,y) - G_x| d\tau_y < \delta$.

Then $\int_M \int_{Z_x} |1 - f(x,y)| d\tau_y d\mu_x < 5\varepsilon + \delta$.

Proof. (49) and the definition of G_x imply that $\int_M G_x d\mu_x = 1$. Let X be the set whose existence is stated in (50). Then $1 = \int_X G_x d\mu_x + \int_{M\backslash X} G_x d\mu_x$. By (50) and (48) the value of the first integral is less than ε in absolute value. In the second integral we may replace G_x by g. Using that $1 \leq \mu(M\backslash X) < 1 - \varepsilon$ we get that $g = \frac{1-R_1}{1-R_2}$ where $|R_1| < \varepsilon$ and $|R_2| < \varepsilon$. This yields $|1-g| < 3\varepsilon$. Therefore $\int_M \int_{Z_x} |1 - f(x,y)| d\tau_y d\mu_x \leq \int_X \int_{Z_x} |1 - f(x,y)| d\tau_y d\mu_x \int_{M\backslash X} \int_{Z_x} |1-g| + |g - f(x,y)| d\tau_y d\mu_x$. By (50) the first integral is at most 2ε. Using that $|1-g| < 3\varepsilon$ and condition (51), we get that the second integral is at most $3\varepsilon + \delta$. (Lemma 6.22)■

We apply Lemma 6.22 for following values of its parameters. For the definition of T we note that each element of $z \in \mathbf{R}^n$ can be uniquely represented by pair $\langle \beta_z, \langle y_z, k_z\rangle\rangle$ where $\beta_z = \langle\langle uz\rangle\rangle$, y_z is the orthogonal projection of z to the subspace H orthogonal to H, $k_z = \lfloor zu \rfloor$. $M = [0,1)$ (containing the possible values of β), and μ is the Lebesgue measure restricted to the interval $[0,1)$. $T = H \times \mathbf{Z}$, τ is the product of the measure $D^{-1}\mathtt{vol}_{n-1}$ on H and the measure which assigns to each set its cardinality on $\mathbf{Z}$ (where D is the volume of $\mathcal{P}$). Since $z \leftrightarrow \langle \beta_z, \langle y_z, k_z\rangle\rangle$ is a one-to-one map between $\mathbf{R}^n$ and $M \times T$. We will denote this map by ι It is easy to see that for any Lebesgue measurable set $Y \subseteq \mathbf{R}^n$ we have $D^{-1}\mathtt{vol}_n(Y) = (\mu \times \tau)(\{\iota(y) \mid y \in Y\})$. For the sake of simplicity we identify the sets $\mathbf{R}^n$ and $M \times T$.

Z is the parallelepiped $\mathcal{P}$. $\varepsilon = 4n^{-c_4}$, $\delta = n^{-c_2}$ If $z \in \mathcal{P}$ and $\iota(z) = \langle x,y\rangle$ then $f(x,y) = D\|u\|^{-1}h(z)$ where h is he density function of $\xi + \mu x$. The factors D and $\|u\|^{-1}$ are needed since in the equation $\int_0^1 \int \mathcal{P}_{\gamma,u} h(z) dz \|u\|^{-1} d\gamma = 1$ which expresses that h is a density function the inner integral is taken by the measure $\mathtt{vol}_{n-1}$ and a factor $\|u\|^{-1}$ is present. Therefore this choice of f satisfies (49). The other conditions of the theorem follow from (44),(45), and (46).

The conclusion of Lemma 6.22 implies that $\int \mathcal{P} |h(z) - \frac{1}{D}| dz \leq n^{-c_1-1}$ or equivalently $\int_0^1 \int_{\mathcal{P}_{\gamma,u}} |h(z - \frac{1}{D})| dz \|u\|^{-1} d\gamma \leq 5n^{-c_4} + n^{-c_2} < n^{-c_1-1}$. Which completes the proof of (37) and so the test T_2 meets all of our requirements.

The test T_1 is the following. Let $x \in \mathbf{R}^n$. We perform the test T_2 for all of the vectors $w_i = \frac{i}{n^{c_4+1}} x$, $i = 1, \ldots, n^{c_4+1}$. If for at least one w_i the result is 0 then the output of T_1 is 0 otherwise it is 1. This test T_1 has all of the claimed properties since $x \in H(dn^{\frac{1}{2}}) \backslash H(d)$ implies that for at least one of the vectors w_i we have $|uw_i - 1| \leq n^{-c_4}$ and so $T_2(w_i) = 1$ with a probability of $1 - n^{-c_5}$ which implies $T_1(x) = 0$. On the other hand if $x \in n^{-c_4} H(d)$ then $w_i \in n^{-c_4} H(d)$ and so $T_2(w_i) = 1$ for all $i = 1, \ldots, n^{c_4+1}$ with a probability of at least $1 - n^{-c_5+c_4+1}$ and therefore $c_4 \ll c_5$ implies that $T_1(x) = 1$ with high probability. (Lemma 6.16)■

References

[1] M. AJTAI: Representing hard lattices with $o(n \log n)$ bits. In *Proc. of 37th ACM Symposium On the Theory of Computing*, 2001. 1

[2] M. AJTAI AND C. DWORK: A public-key cryptosystem with worst-case/average-case equivalence. In *Proc. of 29th ACM STOC*, 1997. (or Electronic Colloquium on Computational Complexity, 1996). 1, 2, 4, 14, 27

[3] M. AJTAI, R. KUMAR, AND D. SIVAKUMAR: A sieve algorithm for the shortest lattice vector problem. In *Proc. of 33rd ACM Symposium On the Theory of Computing*, 2001. 8

[4] W. BANASZCZYK: New bounds in some transference theorems in the geometry of numbers. *Matematische Annalen*, 296(4):625–635, 1993. 2, 27

[5] O. GOLDREICH, S. GOLDWASSER, AND S. HALEVI: Eliminating decryption errors in the Ajtai-Dwork cryptosystem. In *Advances in cryptology*, volume 1294 of *Lecture Notes in Computer Science*, pp. 112–131. Springer, 1997. 4, 5, 27

[6] P. M. GRUBER AND C. G. LEKKERKERKER: *Geometry of Numbers*. North Holland, 1987.

[7] P. R. HALMOS: *Measure Theory*. D. Van Nostrand Company, 1950. 20

[8] J. HOFFSTEIN, J. PIPER, AND J. H. SILVERMAN: Ntru: a ring based public key cryptosystem. In J. BUHLER, editor, *Algorithmic number theory (ANTS III)*, volume 1423 of *Lecture Notes in Computer Science*, pp. 267–288. Springer, 1988. 7

[9] A. K. LENSTRA, H. W. LENSTRA, AND L. LOVÁSZ: Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982. 8

[10] L. LOVÁSZ: *An algorithmic theory of numbers graphs and convexity*. Society for Industrial and Applied Mathematics, Philadelphia, 1986. 4, 27

[11] D. MICCIANCIO: Improving lattice based cryptosystems using the hermite normal form. In *Cryptography and Lattices Conference (CaLC)*, volume 2146 of *Lecture Notes in Computer Science*, pp. 126–145. Springer, 2001. 4

[12] D. MICCIANCIO: Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case assumptions. In *Proc. of 43rd IEEE Annual symposium on foundations of computer science- FOCS 2002*, pp. 356–365, 2002. 7

[13] D. MICCIANCIO AND S. GOLDWASSER: *Complexity of Lattice problems: A Cryptographic Perspective*. Volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, 2002. 3

[14] O. REGEV: New lattice based cryptographic constructions. In *Proceedings of the 35th ACM STOC*, 2003. 2, 4, 27, 28

[15] WOLFGANG M. SCHMIDT: *Diophantine approximation*. Springer Lecture Notes. Springer, 1970. 7

[16] C. P. SCHNORR: A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987. 8

AUTHOR

Miklós Ajtai
IBM Almaden Research Center