Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions*

Daniele Micciancio
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0114, USA
daniele@cs.ucsd.edu

October 29, 2004

Abstract

We investigate the average case complexity of a generalization of the compact knapsack problem to arbitrary rings: given m (random) ring elements $a_1, \ldots, a_m \in R$ and a (random) target value $b \in R$, find coefficients $x_1, \ldots, x_m \in S$ (where S is an appropriately chosen subset of R) such that $\sum a_i \cdot x_i = b$. We consider compact versions of the generalized knapsack where the set S is large and the number of weights m is small. Most variants of this problem considered in the past (e.g., when $R = \mathbb{Z}$ is the ring of the integers) can be easily solved in polynomial time even in the worst case. We propose a new choice of the ring R and subset S that yields generalized compact knapsacks that are seemingly very hard to solve on the average, even for very small values of m. Namely, we prove that for any unbounded function $m = \omega(1)$ with arbitrarily slow growth rate, solving our generalized compact knapsack problems *on the average* is at least as hard as the *worst-case* instance of various approximation problems over cyclic lattices. Specific worst-case lattice problems considered in this paper are the shortest independent vector problem SIVP and the guaranteed distance decoding problem GDD (a variant of the closest vector problem, CVP) for approximation factors $n^{1+\epsilon}$ almost linear in the dimension of the lattice.

Our results yield very efficient and provably secure one-way functions (based on worst-case complexity assumptions) with key size and time complexity almost linear in the security parameter n. Previous constructions with similar security guarantees required quadratic key size and computation time. Our results can also be formulated as a connection between the worst-case and average-case complexity of various lattice problems over cyclic and quasi-cyclic lattices.

Keywords: Knapsack problem, cyclic lattices, average-case complexity, one-way functions.

1 Introduction

Few problems in the theory of computational complexity and its application to the foundations of cryptography have been as controversial as the knapsack problem and its many variants, including the notoriously NP-hard subset-sum problem [28]. The initial enthusiasm generated by the subset-sum based cryptosystem of Merkle and Hellman [35] in the late 70's, was immediately followed by intensive cryptanalytic efforts that culminated in the early 80's with the total break of the system in its basic [59] and iterated version [8]. Still, the possibility of building cryptographic functions based on NP-hard problems, and the relatively high speed at which numbers can be added up (compared to modular multiplication and exponentiation operations required by number theoretic functions), prompted many researchers to suggest variants, fixes, and improvements (e.g., [19, 10]) to the initial Merkle-Hellman proposal. These efforts, which lasted for

*A preliminary version of this paper appeared in Proceedings of the 43rd Annual Symposium on Foundations of Computer Science - FOCS 2002, IEEE. Research supported in part by NSF CAREER Award CCR-0093029 and a Sloan Research Fellowship. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

more than a decade, were invariably followed by attacks (e.g., [26, 58, 47, 51]) that seriously questioned the security of the systems either in theory or in practice. Recently, knapsack-like cryptographic functions have started attracting again considerable attention after Ajtai's discovery [1] that the generalized subset-sum problem (over the additive group $\mathbb{Z}_p^n$ of n-dimensional vectors modulo p) is provably hard to solve on the average based on a worst-case intractability assumption about certain lattice approximation problems for which no polynomial time solution is known. Following [1], Ajtai and Dwork [3] also proposed a cryptosystem with similar security properties. But, unfortunately, even this proposal with strong theoretical security guarantees has been subject to practical attacks [48].

Attacks to subset-sum (or more generally knapsack) problems can be classified into two broad categories:

1. attacks targeted to specific public key cryptosystems that try to exploit the special structure resulting from the embedding of a decryption trapdoor (e.g., [59]); and

2. attacks to generic subset-sum or knapsack instances that can be applied regardless of the existence of a trapdoor (e.g., [30, 11]).

The first class of attacks is usually stronger, meaning that it gives asymptotically good algorithms that succeed (with high probability) regardless of the value of the security parameter, but only applies to specific public key cryptosystems whose underlying knapsack problems are not as hard as the general case. The second class of attacks is more general but only heuristics: the asymptotic complexity of these attacks is usually exponential, or their success rate negligible as a function of the security parameter. These methods are evaluated experimentally by testing them on specific problem instances (e.g., challenges or randomly generated ciphertexts) for typical values of the security parameter, and attacks can be usually avoided setting the security parameter to a sufficiently large value. Still, the effectiveness of these attacks, even for moderately large values of the security parameter, is currently considered the main practical obstacle in the design of cryptographic functions based on variants of the knapsack problem.

It is important to realize that the second class of attacks dismisses most knapsack cryptographic functions as practical alternatives to number theory based functions, not on the grounds of their inherent insecurity, but simply because of the large key sizes required to avoid heuristics attacks. In fact (especially if one drops the more ambitious goal of designing a public key cryptosystem, and more modestly attempts to design cryptographic primitives with no trapdoors, like pseudo-random generators or one-way hash functions, etc.) there is theoretical evidence [24, 1, 3, 53] that subset-sum can indeed be a good source of computational hardness, at least from an asymptotic point of view. The main issue affecting the practical security of knapsack functions is efficiency. In a typical knapsack function, the key (corresponding to security parameter n) consists of $\Omega(n)$ numbers, each of which is n bits long. Therefore, the size of the resulting cryptographic key grows as $\Omega(n^2)$. Even if all known attacks to knapsack have exponential time complexity, one needs to set n to at least a few hundreds to make heuristics approaches (most notably lattice basis reduction [32, 57, 27, 49, 50]) ineffective or too costly. As a consequence, the resulting key can easily reach megabit sizes still without achieving a sufficient degree of security. Even if knapsack functions can be still competitive from a running time point of view, these huge key sizes are considered too big for most practical applications.

Generalized compact knapsacks. The impact of space efficiency on the practical security of knapsack based functions has long been recognized, even before the development of ingenious lattice based attacks. A simple improvement that comes to mind is to use a so called *compact* knapsack: instead of using 0–1 combinations of $\Omega(n)$ input weights (resulting in $\Omega(n^2)$ key size), consider a smaller (constant, or slowly increasing) number of weights $a_1, \ldots, a_m$ and combine them with coefficients from a larger set, e.g., $\{0, \ldots, 2^{\delta n}\}$ for some small constant $\delta > 0$. Notice that if $\delta = 0$, then we get the usual subset-sum problem, which can be solved (for $m = O(\log n)$) in polynomial time using exhaustive search. However, if $\delta = \Omega(1)$ then the search space becomes exponentially large, and exhaustive search is infeasible. Suggestions of this type appear already in Merkle and Hellman's original paper [35] and subsequent works as a method to increase the bandwidth of the scheme. These early attempts to reduce the key size of knapsack based functions were subject to attacks even more devastating than the general case: in [4] it is observed that the problem easily reduces to an integer programming instance with $O(m)$ variables, and therefore it can be solved in polynomial time for any constant value of $m(n) = O(1)$, or even any slowly growing function $m(n) = O(\log n / \log \log n)$. Attempts to use compact knapsacks to design efficient cryptographic functions persisted during the 90's [52, 33], but were always followed by cryptanalytic attacks [55, 12, 31].

In this paper we introduce and study a new class of compact knapsacks which are both very efficient and provably hard to solve in a strong sense similar to Ajtai's function [1]. The one-way function proposed in [1] can be described as a generalization of the integer knapsack problem to arbitrary rings. Specifically, for any ring R and subset $S \subset R$, consider the following problem: given ring elements $a_1, \ldots, a_m \in R$ and a target value $b \in R$, find coefficients $x_i \in S$ such that $\sum_{i=1}^{m} a_i \cdot x_i = b$, where all operations are performed in the ring. In Ajtai's work, R is the product ring[1] $\mathbb{Z}_p^n$ of n-dimensional vectors modulo p (for some polynomially bounded $p(n) = n^{O(1)}$) and $S = \{\mathbf{0}, \mathbf{1}\}$ consists of the additive and multiplicative identities of the ring. In particular, S has size 2, and the problem can be solved by exhaustive search in polynomial time when $m = O(\log n)$.

In this paper we study compact versions of the generalized knapsack problem, where the set S has size much larger than 2, so that exhaustive search is infeasible even for very small values of m. In the case of the ring $\mathbb{Z}_p^n$, the first idea that comes to mind is to use, as coefficients the set $S = \{0,1\}^n$ of all binary vectors, or, more generally, the set $S = \{0, \ldots, p^\delta\}^n$ of n-dimensional vectors with entries much smaller than p. Unfortunately, as for the case of the integer compact knapsack problem described above, this straightforward construction admits much faster solutions than exhaustive search: the resulting generalized compact knapsack is equivalent to n *independent* instances of the knapsack problem modulo p, which, for any polynomially bounded $p(n) = n^{O(1)}$, can be efficiently solved in the worst case by dynamic programming.

Our contribution. The main contribution of this paper is the study of a new class of compact knapsack functions $f_{\mathbf{a}}(\mathbf{x}) = \sum_i a_i \cdot x_i$ that are conceivably hard to invert in a very strong sense, even when the number m of weights is very small. In particular, we prove that, for appropriate choice of ring R and subset $S \subset R$, and for any unbounded function $m(n) = \omega(1)$ (with arbitrarily slow growth rate) the compact knapsack function is at least as hard to invert *on the average* (even with nonnegligible probability) as the *worst-case* instance of various lattice problems (for the special class of cyclic lattices) for which no polynomial time algorithm is known.

Our generalized knapsack problems are defined by the ring $R = \mathbb{Z}_p^n$ of n-dimensional vectors modulo a prime p with the componentwise addition and *convolution product* operations. As in the previously discussed compact variant of Ajtai's function, the set $S = \{0, \ldots, p^\delta\}^n$ consists of all n-dimensional vectors with small entries. Surprisingly, using the convolution product operation (as opposed to componentwise multiplication) makes the problem considerably harder: solving random instances of our generalized compact knapsacks with nonnegligible probability is as hard as approximating the shortest independent vector problem (as well as various other lattice problems) on cyclic lattices in the *worst case* within factors $n^{1+\epsilon}$ (for any $\epsilon > 0$) almost linear in the dimension of the lattice.

This results in strong one-way functions with average-case security guarantees based on a worst-case intractability assumption similar to Ajtai's function [1] (and subsequent improvements [9, 40, 42, 44],) but with a much smaller key size $O(m \log p^n) = \omega(n \log n)$, where $\omega(\cdot)$ is an unbounded function with arbitrarily slow growth rate. (For comparison, [1, 9, 40, 42, 44] require $m(n) = \Omega(n \log n)$, and key size $\Omega(n^2 \log^2 n)$.)

Our compact knapsack functions are also extremely fast, as, for appropriate choice of the parameters, they can be computed in almost linear time $O(n \log^c n)$ using the fast Fourier transform in the evaluation of the convolution products. Specifically, the cost of evaluating our functions is equivalent to computing an almost constant number $\omega(1)$ of FFT operations on n-dimensional vectors modulo a small prime $p = n^{O(1)}$. The almost linear time evaluation algorithm together with the substantially smaller key size, make our generalized compact knapsack function even much faster than the already attractive subset-sum function.

In the process of establishing our hardness result, we prove various properties of our knapsack functions that might be of independent interest. In particular, we prove that our compact knapsack function $f_{\mathbf{a}}(\mathbf{x})$ has very small collision probability. By a result of Impagliazzo and Zuckerman [25], this is enough to guarantee that the value $f_{\mathbf{a}}(\mathbf{x})$ (for randomly chosen $\mathbf{a}$ and $\mathbf{x}$) is almost uniformly distributed over $\mathbb{Z}_p^n$ and independent from $\mathbf{a} = (\mathbf{a}_1, \ldots, \mathbf{a}_m)$. Moreover, this is true for arbitrary small values of $m(n) = \omega(1)$. Previous results of this kind for the subset-sum function relied on the additive structure of $\mathbb{Z}_p^n$ alone, and required $m = \Omega(n \log p)$.

[1] The product ring R^n is the set of n-tuples with entries in R, with the componentwise addition and multiplication operations.

Our proof makes substantial use of the multiplicative structure of the ring $\mathbb{Z}_p^n$ (with the convolution product operation) and the characterization of its ideals as polynomial quotient rings.

Beside the technical contribution of a very efficient and provably secure one-way function based on a worst-case complexity assumption, we view the following as additional contributions of this papers: the introduction of the class of cyclic lattices as a source of interesting computational problems; casting a new light on the complexity of the compact knapsack problem showing that if the ring is appropriately chosen the problem can be substantially harder than the integer case; and demonstrating that the techniques initially developed in [1, 44] can be useful to study seemingly different problems, and still produce the same kind of strong worst-case/average-case security guarantees. In our view all these contributions are important steps toward the development of cryptographic functions that are both efficient and provably secure in a very strong sense.

Related work The first construction of one-way function that is provably secure based on a worst-case complexity assumption was given by Ajtai in [1]. Subsequent work [9, 40, 42, 44] focused on improving the required worst-case complexity assumption. In this paper, the goal is to improve the efficiency of the one-way function.

This paper is an almost complete rewriting and substantial improvement of an extended abstract [39] presented at FOCS 2002. In particular, in [39] the author proved that solving the generalized compact knapsack on the average when $m = O(\log n)$ is at least as hard as approximating various lattice problems in the worst case within a factor $n^{3+\epsilon}$. Here, we prove a new regularity theorem for compact knapsack functions (Theorem 4.2) and incorporate the recently developed Gaussian distribution techniques of [44], to present an improved result that holds for any function $m = \omega(1)$ with arbitrarily slow growth rate, and worst-case approximation factors $n^{1+\epsilon}$ almost linear in the dimension of the lattice.

For a description of other related works, see Section 5.

Organization The rest of the paper is organized as follows. In Section 2 we recall basic notation, definitions and results needed in this paper. In Section 3 we prove two preliminary lemmas about cyclic lattices that will be used in the proof of our main result. In Section 4 we present the main technical result of the paper: we formally define our generalized compact knapsack function, and prove that inverting the function on the average is at least as hard as the worst case instance of various lattice problems on cyclic lattices. In the process, we also establish various other properties of our compact knapsack functions that might be of independent interest, e.g., we bound the collision probability of the function, and prove that the function is almost regular. Section 5 concludes with a discussion of related work, the complexity of cyclic lattices, and open problems.

2 Preliminaries

In this section we introduce some notational conventions, and recall basic definitions and results about the statistical distance, hash functions, lattices and Gaussian probability distributions.

For any real $r \geq 0$, $\llbracket r \rrbracket$ denotes the set $\{0, \ldots, \lfloor r \rfloor\}$ of all positive integers not greater than r. The uniform probability distribution over a set S is denoted $U(S)$. We use the standard asymptotic notation $f = O(g)$ (or $g = \Omega(f)$) when $\limsup_{n\to\infty} |f(n)/g(n)| < \infty$, $f = o(g)$ (or $g = \omega(f)$) when $\lim_{n\to\infty} |f(n)/g(n)| = 0$, and $f = \Theta(g)$ when $f = O(g)$ and $f = \Omega(g)$.

A function $f(n)$ is negligible (denoted $f(n) = n^{-\omega(n)}$) if for every c there exists an n_0 such that $|f(n)| < 1/n^c$ for all $n > n_0$. Throughout the paper, we use column notation for all vectors, and use $(\cdot)^T$ to denote the matrix transposition operation.

2.1 Statistical distance

The statistical distance is a measure of how two probability distributions are far apart from each other, and it is a convenient tool in the analysis of randomized algorithms and reductions. In this subsection we define the statistical distance and state some simple facts that will be used in the analysis of the reductions in this paper. All the properties of the statistical distance stated in this subsection are easily verified. For more details the reader is referred to [43, Chapter 8].

Definition 2.1 *Let X and Y be two discrete random variables over a (countable) set A. The statistical distance between X and Y is the quantity*

$$\Delta(X,Y) = \frac{1}{2}\sum_{a\in A} \left|\Pr\{X=a\} - \Pr\{Y=a\}\right|.$$

In the case of continuous random variables, the statistical distance between X and Y is

$$\Delta(X,Y) = \frac{1}{2}\int_A |\delta_X(a) - \delta_Y(a)|da,$$

where δ_X and δ_Y are the probability density functions of X and Y respectively.

An easy calculation shows that the statistical distance $\Delta(X,Y)$ equals the maximum over all sets $S \subseteq A$ of $\Pr\{X \in S\} - \Pr\{Y \in S\}$. So, for example, there is always a set $S \subseteq A$ such that $\Pr\{X \in S\} = \Pr\{Y \in S\} + \Delta(X,Y)$.

We say that two random variables X, Y are identically distributed (written $X \equiv Y$) if and only if $\Pr\{X \in S\} = \Pr\{Y \in S\}$ for every $S \subseteq A$. The reader can easily check that the statistical distance satisfies the usual properties of distance functions, i.e., $\Delta(X,Y) \geq 0$ (with equality if and only if $X \equiv Y$), $\Delta(X,Y) = \Delta(Y,X)$, and $\Delta(X,Z) \leq \Delta(X,Y) + \Delta(Y,Z)$.

The following proposition shows that applying a (possibly randomized) function to two distributions does not increase the statistical distance.

Proposition 2.2 *Let X, Y be two random variables taking values in a common set A. For any (possibly randomized) function f with domain A, the statistical distance between $f(X)$ and $f(Y)$ is at most*

$$\Delta(f(X), f(Y)) \leq \Delta(X,Y) \tag{2.1}$$

As a corollary, we easily obtain the following.

Corollary 2.3 *If X and Y are random variables over set A and $p\colon A \to \{0,1\}$ is a predicate, then*

$$|\Pr\{p(X) = 1\} - \Pr\{p(Y) = 1\}| \leq \Delta(X,Y). \tag{2.2}$$

Another useful property of the statistical distance is the following.

Proposition 2.4 *Let $X_1, \ldots, X_k$ and $Y_1, \ldots, Y_k$ be two lists of totally independent random variables. Then*

$$\Delta((X_1,\ldots,X_k),(Y_1,\ldots,Y_k)) \leq \sum_{i=1}^{k} \Delta(X_i, Y_i). \tag{2.3}$$

2.2 One-way hash function families

A function family $\{f_a\colon X \to R\}_{a\in A}$ is a collection of functions (indexed by a set of keys A) with a common domain X and range R. A (polynomial) function ensemble is a sequence $\{f_a\colon X_n \to R_n\}_{a\in A_n}$ of function families (indexed by a security parameter $n \in \mathbb{N}$) such that $\log|A_n|, \log|X_n|$ and $\log|R_n|$ are all polynomial in n. We assume that the elements of the sets A_n, X_n and R_n can be efficiently represented with $\log_2|A_n|$, $\log_2|X_n|$ and $\log_2|R_n|$ bits respectively, membership in the sets can be decided in polynomial time, and there is a probabilistic polynomial time algorithm to sample from those sets with (almost) uniform distribution. It is also common to assume that the functions f_a are efficiently computable, in the sense that there is a polynomial time algorithm that on input $n, a \in A_n$ and $x \in X_n$, outputs $f_a(x)$. All function ensembles considered in this paper have these properties, namely the sets A_n, X_n, R_n have efficient representations and the functions f_a are efficiently computable.

A function (ensemble) is one-way if it is (easy to compute, but) computationally hard to invert, i.e., no algorithm can efficiently solve the following function inversion problem: given a pair $(a,r) \in A_n \times R_n$, find an $x \in X_n$ such that $f_a(x) = r$. One-wayness is an average-case complexity property, i.e., it requires that the function inversion problem is computationally hard when the input $(a,r) \in A_n \times R_n$ is selected at random. The exact definition, for the case of function ensembles, is given below.

Definition 2.5 *A function ensemble $\{f_a : X_n \to R_n\}_{a\in A_n}$ is* one-way *if for any probabilistic polynomial time algorithm $\mathcal{A}$, the probability that $f_a(\mathcal{A}(n,a,f_a(x))) = f_a(x)$ (when $a \in A_n$ and $x \in X_n$ are selected uniformly at random) is negligible in n.*

Notice that the input distribution underlying the definition of one-way function is not the uniform distribution over $A_n \times R_n$, but rather it corresponds to choosing the target value $r \in R_n$ as the image of a uniformly random solution $x \in X$. For any function ensemble $\mathcal{H} = \{f_a : X \to R\}_{a\in A}$, we write $\mathrm{OWF}(\mathcal{H})$ to denote the probability distribution $\{(a, f(x)) : a \in A_n, x \in X_n\}$ underlying the definition of one-way function, and $U(A \times R)$ to denote the uniform probability distribution over $A \times R$. We remark that Definition 2.5 corresponds to the notion of *strong* one-way function, i.e., it is required that the success probability of any probabilistic polynomial time algorithm in solving the function inversion problem (when the input is chosen according to distribution $\mathrm{OWF}(\mathcal{H})$) is negligible.

The function families $\mathcal{H} = \{f_a : X \to R\}_{a\in A}$ considered in this paper have the property that the input size $\log|X|$ is strictly bigger than the output size $\log|R|$, i.e., the functions "compress" the size of the input by a factor $\log|X|/\log|R|$. Such functions have many important applications in computer science and cryptography, and are generically called *hash* functions. In order to be useful, hash functions must satisfy some additional properties. A typical requirement is that if $a \in A$ and $x \in X$ are chosen uniformly at random, the distribution of $f_a(x) \in R$ is almost uniform and independent from a. In other words, $\mathrm{OWF}(\mathcal{H})$ is statistically close to the uniform distribution $U(A \times R)$.

Definition 2.6 *Let $\mathcal{H} = \{f_a : X \to R\}_{a\in A}$ be a hash function family. We say that $\mathcal{H}$ is ϵ-regular if the statistical distance between $\mathrm{OWF}(\mathcal{H})$ and the uniform distribution over $U(A \times R)$ is at most ϵ. A hash function ensemble $\{\mathcal{H}_n\}$ is called almost regular if $\mathcal{H}_n$ is $\epsilon(n)$-regular for every n, for some negligible function $\epsilon(n) = n^{-\omega(1)}$.*

We remark that if a function is ϵ-regular for $\epsilon = 0$, then the function maps the uniform input distribution to the uniform output distribution. So, definition 2.6 is a generalization of the standard notion of regular function.

2.3 Lattices

An n-dimensional *lattice*[2] is the set of all integer combinations $\{\sum_{i=1}^n x_i\mathbf{b}_i : x_i \in \mathbb{Z}\}$ of n linearly independent vectors $\mathbf{b}_1,\ldots,\mathbf{b}_n$ in $\mathbb{R}^n$. The set of vectors $\mathbf{b}_1,\ldots,\mathbf{b}_n$ is called a *basis* for the lattice, and can be compactly represented by the matrix $\mathbf{B} = [\mathbf{b}_1|\ldots|\mathbf{b}_n] \in \mathbb{R}^{n\times n}$ having the basis vectors as columns. The lattice generated by $\mathbf{B}$ is denoted $\mathcal{L}(\mathbf{B})$. Notice that $\mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^n\}$, where $\mathbf{Bx}$ is the usual matrix-vector multiplication. For any basis $\mathbf{B}$, we define the fundamental parallelepiped $\mathcal{P}(\mathbf{B}) = \{\mathbf{Bx} : \forall i. 0 \le x_i < 1\}$. The following lemma shows how to sample lattice points uniformly at random from the fundamental parallelepiped associated to a given sublattice.

Lemma 2.7 ([43, Proposition 8.2]) *There is a probabilistic polynomial time algorithm that on input a lattice basis $\mathbf{B}$ and a full rank sublattice $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$, outputs a lattice point $\mathbf{x} \in \mathcal{L}(\mathbf{B}) \cap \mathcal{P}(\mathbf{S})$ chosen uniformly at random.*

The dual of a lattice $\mathcal{L}(\mathbf{B})$ (denoted $\mathcal{L}(\mathbf{B})^*$) is the lattice generated by the matrix $\mathbf{B}^{-T}$, and consists of all vectors that have integer scalar product with all lattice vectors.

For any vector $\mathbf{x} = (x_1,\ldots,x_n)^T$, define the cyclic rotation $rot(\mathbf{x}) = (x_n, x_1, \ldots, x_{n-1})^T$, and the corresponding circulant matrix $Rot(\mathbf{x}) = [\mathbf{x}, rot(\mathbf{x}), rot^2(\mathbf{x}), \ldots, rot^{n-1}(\mathbf{x})]$. A lattice $\mathcal{L}(\mathbf{B})$ is cyclic if it is closed

[2]For simplicity, is this paper we restrict all definitions to full dimensional lattices.

under the rotation operation, i.e., if $\mathbf{x} \in \mathcal{L}(\mathbf{B})$ implies $rot(\mathbf{x}) \in \mathcal{L}(\mathbf{B})$. It is easy to see that a lattice is cyclic if and only if $\mathcal{L}(\mathbf{B}) = rot(\mathcal{L}(\mathbf{B}))$. The cyclic lattice generated by a vector $\mathbf{x}$ is the lattice $\mathcal{L}(Rot(\mathbf{x}))$ generated by the circulant matrix of $\mathbf{x}$, and it is the smallest cyclic lattice containing $\mathbf{x}$.

The convolution product of two vectors $\mathbf{x}$ and $\mathbf{y}$ is the vector

$$\mathbf{x} \otimes \mathbf{y} = Rot(\mathbf{x}) \cdot \mathbf{y}$$

with entries defined by the equation

$$(\mathbf{x} \otimes \mathbf{y})_k = \sum_{i+j=k \bmod n} x_i \cdot y_j.$$

It can be easily verified that the convolution product is associative and commutative, i.e., it satisfies the equational axioms $\mathbf{x} \otimes (\mathbf{y} \otimes \mathbf{z}) = (\mathbf{x} \otimes \mathbf{y}) \otimes \mathbf{z}$, and $\mathbf{x} \otimes \mathbf{y} = \mathbf{y} \otimes \mathbf{x}$. Moreover, it distributes over the vector addition operation: $(\mathbf{x} + \mathbf{y}) \otimes \mathbf{z} = \mathbf{x} \otimes \mathbf{z} + \mathbf{y} \otimes \mathbf{z}$. Therefore, $(R^n, +, \otimes)$ is a commutative ring with identity $\mathbf{e}_1 = (1, 0, \ldots, 0)^T$.

The Euclidean norm of a vector $\mathbf{x}$ is the quantity $\|\mathbf{x}\| = \sqrt{\sum_i x_i^2}$. Other norms used in this paper are the ℓ_1 norm $\|\mathbf{x}\|_1 = \sum_i |x_i|$ and the max norm $\|\mathbf{x}\|_\infty = \max_i |x_i|$. These norms and the convolution product are related by the following inequalities, valid for any n-dimensional vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$:

$$\begin{aligned}
\|\mathbf{x}\| \leq \|\mathbf{x}\|_1 &\leq \sqrt{n}\|\mathbf{x}\| \\
\|\mathbf{x}\|_\infty \leq \|\mathbf{x}\| &\leq \sqrt{n}\|\mathbf{x}\|_\infty \\
\|\mathbf{x} \otimes \mathbf{y}\|_\infty &\leq \|\mathbf{x}\| \cdot \|\mathbf{y}\| \\
\|\mathbf{x} \otimes \mathbf{y}\|_\infty &\leq \|\mathbf{x}\|_1 \cdot \|\mathbf{y}\|_\infty.
\end{aligned}$$

The *minimum distance* of a lattice $\mathcal{L}(\mathbf{B})$, denoted $\lambda_1(\mathcal{L}(\mathbf{B}))$, is the minimum distance between any two (distinct) lattice points and equals the length of the shortest nonzero lattice vector:

$$\lambda_1(\mathcal{L}(\mathbf{B})) = \min\{\mathrm{dist}(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y} \in \mathcal{L}(\mathbf{B})\} = \min\{\|\mathbf{x}\| : \mathbf{x} \in \mathcal{L}(\mathbf{B}) \setminus \{\mathbf{0}\}\}.$$

The notion of minimum distance can be generalized to define the ith successive minimum λ_i as the smallest radius r such that the closed sphere $\bar{\mathcal{B}}(r) = \{\mathbf{x} : \|\mathbf{x}\| \leq r\}$ contains i linearly independent lattice points:

$$\lambda_i(\mathcal{L}(\mathbf{B})) = \min\{r : \dim(\mathrm{span}(\mathcal{L}(\mathbf{B}) \cap \bar{\mathcal{B}}(r))) \geq i\}$$

Another important constant associated to a lattice is the covering radius. The covering radius $\rho(\mathcal{L}(\mathbf{B}))$ of a lattice is the maximum distance $\mathrm{dist}(\mathbf{x}, \mathcal{L}(\mathbf{B}))$ when $\mathbf{x}$ ranges over the linear span of $\mathbf{B}$:

$$\rho(\mathcal{L}(\mathbf{B})) = \max\{\mathrm{dist}(\mathbf{x}, \mathcal{L}(\mathbf{B})) : \mathbf{x} \in \mathbb{R}^n\}.$$

A sublattice of $\mathcal{L}(\mathbf{B})$ is a lattice $\mathcal{L}(\mathbf{S})$ such that $\mathcal{L}(\mathbf{S}) \subseteq \mathcal{L}(\mathbf{B})$. We always assume that sublattices have full rank, i.e., $\dim(\mathrm{span}(\mathbf{S})) = \dim(\mathrm{span}(\mathbf{B}))$.

In many algorithmic problems on point lattices the quality of a solution is measured with respect to some specific lattice parameter, e.g., the length λ_1 of the shortest nonzero vector, or the radius λ_n of the smallest sphere containing n linearly independent lattice vectors. For example, the $\gamma(n)$-approximate shortest vector problem asks to find a nonzero vector in a lattice $\mathcal{L}(\mathbf{B})$ of length at most $\gamma(n) \cdot \lambda_1(\mathcal{L}(\mathbf{B}))$, where n is the rank of the lattice. For technical reasons, in this paper we consider generalized versions of various lattice problems where the quality of the solution is measured with respect to an arbitrary function of the lattice $\phi(\mathcal{L}(\mathbf{B}))$. The first of these problems is the following generalization of the shortest independent vector problem introduced in [42].

Definition 2.8 *The* generalized independent vectors problem $\mathrm{GIVP}^\phi_\gamma$, *given an n-dimensional lattice* $\mathbf{B}$, *asks for a set of n linearly independent lattice vectors $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{S}\| \leq \gamma(n) \cdot \phi(\mathcal{L}(\mathbf{B}))$.*

The shortest independent vectors problem SIVP_γ (studied in [7] and used in [1, 9, 40, 42, 44] as a source of computational hardness) is a special case of $\mathrm{GIVP}^\phi_\gamma$ where $\phi = \lambda_n$. Another problem that will play a fundamental role in this paper is the following.

Definition 2.9 *The* guaranteed distance decoding *problem (GDD^ϕ_γ), given a lattice $\mathbf{B}$ and a target point $\mathbf{t} \in \mathrm{span}(\mathbf{B})$, asks for a lattice point $\mathbf{x} \in \mathcal{L}(\mathbf{B})$ such that $\mathrm{dist}(\mathbf{t}, \mathbf{x}) \leq \gamma(n) \cdot \phi(\mathcal{L}(\mathbf{B}))$, where n is the rank of the lattice.*

This time it is natural to set $\phi = \rho$ to the covering radius of the lattice, because for any lattice basis $\mathbf{B}$ and target $\mathbf{t} \in \mathbb{R}^n$, there is always a lattice point within distance $\rho(\mathcal{L}(\mathbf{B}))$ from $\mathbf{t}$. GDD^ρ_γ is an interesting variant of the closest vector problem CVP, where the quality of the solution is measured with respect to the worst possible distance $\max_{\mathbf{t}\in\mathbb{R}^n} \mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}))$ rather then the distance of the given target $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B}))$.

The GDD^ϕ_γ and $\mathrm{GIVP}^\phi_\gamma$ are easily related by the following theorem, whose proof is implicit in [43, Theorem 7.9].

Theorem 2.10 *For any $c > 2$, there is a polynomial time reduction from $\mathrm{GIVP}^\phi_{c\gamma}$ to GDD^ϕ_γ. Moreover, the reduction is lattice preserving, in the sense that all the calls made to the GDD oracle are of the form $(\mathbf{B}, \mathbf{t})$ where $\mathbf{B}$ is the input GIVP lattice.*

Proof: Let $\mathbf{B}$ an input $\mathrm{GIVP}^\phi_{c\gamma}$ instance. We build a set of $n = \dim(\mathbf{B})$ linearly independent vectors $\mathbf{s}_1, \ldots, \mathbf{s}_n \in \mathcal{L}(\mathbf{B})$ of length $\|\mathbf{s}_i\| \leq l = c\gamma(n) \cdot \phi(\mathcal{L}(\mathbf{B}))$ inductively as follows. For any $i = 1, \ldots, n$,

- let $\mathbf{t} \in \mathrm{span}(\mathbf{B})$ be a vector orthogonal to $\mathbf{s}_1, \ldots, \mathbf{s}_{i-1}$ of length $\|\mathbf{t}\| = l/2$,
- call the GDD^ϕ_γ oracle on input $(\mathbf{B}, \mathbf{t})$ to find a lattice vector $\mathbf{s}_i \in \mathcal{L}(\mathbf{B})$ within distance $\gamma(n) \cdot \phi(\mathcal{L}(\mathbf{B})) = l/c < l/2$ from $\mathbf{t}$.

Notice that each $\mathbf{s}_i$ is linearly independent from $\mathbf{s}_1, \ldots, \mathbf{s}_{i-1}$ because the distance of $\mathbf{s}_i$ from $\mathrm{span}(\mathbf{s}_1, \ldots, \mathbf{s}_{i-1})$ is at least $\|\mathbf{t}\| - \|\mathbf{s}_i - \mathbf{t}\| > 0$. Moreover, by triangle inequality, the length of $\mathbf{s}_i$ is at most $\|\mathbf{t}\| + \|\mathbf{s}_i - \mathbf{t}\| < l$. □

Most lattice problems can be meaningfully restricted to cyclic lattices, or other special classes of lattices. For example, the closest vector or GDD problem for cyclic lattices is: given a *cyclic lattice* $\mathcal{L}(\mathbf{B})$, a target vector $\mathbf{t}$, and a real parameter $r > 0$, find a lattice point $\mathbf{x} \in \mathcal{L}(\mathbf{B})$ within distance r from the target $\mathbf{t}$. Our generalized compact knapsack functions are at least as hard to invert on the average as the worst-case instance of approximating various lattice problems (e.g., SIVP or GDD) over cyclic lattices in the worst case within almost linear factors $n^{1+\epsilon}$, for arbitrarily small $\epsilon > 0$. Lattice preserving reductions, as the one given in Theorem 2.10, are particularly useful in the context of this paper because they allow to reduce a (worst-case) lattice problem over a given class of lattices (e.g., cyclic lattices) to another (worst-case) lattice problem over the same class of lattices. In particular, Theorem 2.10 implies that there is a reduction from GIVP over cyclic lattices to GDD over cyclic lattices.

2.4 Gaussian distributions

We use the Gaussian distribution techniques recently introduced in [44] to simplify and improve the results described in a preliminary version of this paper [39]. In this subsection we recall all the required definitions and results from [44]. For any vectors $\mathbf{c}, \mathbf{x}$ and any $s > 0$, let

$$\rho_{s,\mathbf{c}}(\mathbf{x}) = e^{-\pi\|(\mathbf{x}-\mathbf{c})/s\|^2}$$

be a Gaussian function centered in $\mathbf{c}$ scaled by a factor of s. The total measure associated to $\rho_{s,\mathbf{c}}$ is $\int_{\mathbf{x}\in\mathbb{R}^n} \rho_{s,\mathbf{c}}(\mathbf{x})d\mathbf{x} = s^n$. So, $\int_{\mathbf{x}\in\mathbb{R}^n} (\rho_{s,\mathbf{c}}(\mathbf{x})/s^n)d\mathbf{x} = 1$ and $\rho_{s,\mathbf{c}}/s^n$ is a probability density function. As noted in [44], $\rho_{s,\mathbf{c}}/s^n$ can be expressed as the sum of n orthogonal 1-dimensional Gaussian distributions, and each of them can be efficiently approximated with arbitrary precision using standard techniques. So, the distribution $\rho_{s,\mathbf{c}}/s^n$ can be efficiently approximated. For simplicity, in this paper we work with real numbers and assume we can sample from $\rho_{s,\mathbf{c}}/s^n$ exactly. In practice, when only finite precision is available, $\rho_{s,\mathbf{c}}/s^n$

can be approximated by picking a fine grid, and picking points from the grid with probability approximately proportional to $\rho_{s,\mathbf{c}}/s^n$. All our arguments can be made rigorous by selecting a sufficiently fine grid.

Functions are extended to sets in the usual way; e.g., $\rho_{s,\mathbf{c}}(A) = \sum_{\mathbf{x}\in A} \rho_{s,\mathbf{c}}(\mathbf{x})$ for any countable set A. For any $s, \mathbf{c}$ and lattice Λ, define the discrete probability distribution (over the lattice Λ)

$$D_{\Lambda,s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)},$$

where $\mathbf{x} \in \Lambda$. Intuitively, $D_{\Lambda,s,\mathbf{c}}$ is the conditional probability[3] that $(\rho_{s,\mathbf{c}}/s^n) = \mathbf{x}$ given $(\rho_{s,\mathbf{c}}/s^n) \in \Lambda$. For brevity, we sometimes omit s or $\mathbf{c}$ from the notation $\rho_{s,\mathbf{c}}$ and $D_{\Lambda,s,\mathbf{c}}$. When $\mathbf{c}$ or s are not specified, we assume that they are the origin and 1 respectively.

In [44] Gaussian distributions are used to define a new lattice invariant, called the *smoothing parameter*, defined as follows.

Definition 2.11 *For an n-dimensional lattice Λ, and positive real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\Lambda)$ is the smallest s such that $\rho_{1/s}(\Lambda^* \setminus \{\mathbf{0}\}) \le \epsilon$.*

In [44] many important properties of the smoothing parameter are established. Here we only need the following three bounds. The first one shows that the smoothing parameter is the amount of Gaussian noise that needs to be added to a lattice in order to get an almost uniform distribution.

Lemma 2.12 ([44, Lemma 4.1]) *Let $\rho_s/s^n \bmod \mathbf{B}$ be the distribution obtained by sampling a point according to the probability density function ρ_s/s^n and reducing the result modulo $\mathbf{B}$. For any lattice $\mathcal{L}(\mathbf{B})$, the statistical distance between $\rho_s/s^n \bmod \mathbf{B}$ and the uniform distribution over $\mathcal{P}(\mathbf{B})$ is at most $\frac{1}{2}\rho_{1/s}(\mathcal{L}(\mathbf{B})^* \setminus \{\mathbf{0}\})$. In particular, if $s \ge \eta_\epsilon(\mathcal{L}(\mathbf{B}))$, then the distance $\Delta(\rho_s/s^n \bmod \mathbf{B}, U(\mathcal{P}(\mathbf{B})))$ is at most $\epsilon/2$.*

The second property shows that if s is sufficiently large, then the second moment of the distribution $D_{\Lambda,s,\mathbf{c}}$ is essentially the same as the one of the continuous Gaussian distribution $\rho_{c,\mathbf{s}}/s^n$.

Lemma 2.13 ([44, Lemma 4.2, Equation (2)]) *For any n-dimensional lattice Λ, point $\mathbf{c} \in \mathbb{R}^n$, unit vector $\mathbf{u}$, and positive real $s > 0$ such that $\rho_{1/s}(\Lambda^* \setminus \{0\}) < 1$,*

$$\left| \operatorname*{Exp}_{\mathbf{x}\sim D_{\Lambda,s,\mathbf{c}}} \left[\langle \mathbf{x} - \mathbf{c}, \mathbf{u}\rangle^2\right] - \frac{s^2}{2\pi} \right| \quad \le \quad s^2 \cdot \frac{\rho_{2/s}(\Lambda^* \setminus \{\mathbf{0}\})}{1 - \rho_{1/s}(\Lambda^* \setminus \{\mathbf{0}\})}.$$

The last property bounds the smoothing parameter in terms of λ_n.

Lemma 2.14 ([44, Lemma 3.3]) *For any n-dimensional lattice Λ and positive real $\epsilon > 0$,*

$$\eta_\epsilon(\Lambda) \le \sqrt{\frac{\ln(2n(1+1/\epsilon))}{\pi}} \cdot \lambda_n(\Lambda).$$

In particular, for any super-logarithmic function $\omega(\log n)$ there is a negligible function $\epsilon(n)$ such that $\eta_\epsilon(\Lambda) \le \sqrt{\omega(\log n)} \cdot \lambda_n$.

3 Two lemmas about cyclic lattices

In this section we prove two preliminary lemmas about cyclic lattices that will be used in the proof of our main results in the next section. The results are presented here because their formulation is largely independent from the specific reduction in which they are used, and might be of independent interest.

The first lemma gives an efficient algorithm to select a full rank cyclic sublattice generated by a single short vector from an arbitrary cyclic input lattice.

[3] We are conditioning on an event that has probability 0; this can be made rigorous by standard techniques.

Lemma 3.1 *There exists a polynomial time algorithm that on input a full rank n-dimensional lattice $\mathbf{S}$, computes a vector $\mathbf{c} \in \mathcal{L}(\mathbf{S})$ such that $\|\mathbf{c}\|_1 \leq 2 \cdot n \cdot \|\mathbf{S}\|$ and $Rot(\mathbf{c})$ has full rank.*

Proof: Let $S = \|\mathbf{S}\|$. We use Babai's nearest plane algorithm [6] to find a vector $\mathbf{c} \in \mathcal{L}(\mathbf{S})$ within Euclidean distance $(\sqrt{n}/2) \cdot S$ from $nS\mathbf{e}_1$. Notice that the ℓ_1 norm of $\mathbf{c}$ is at most

$$\begin{aligned} \|\mathbf{c}\|_1 &\leq \|(nS \cdot \mathbf{e}_1)\|_1 + \|(\mathbf{c} - nS\mathbf{e}_1)\|_1 \\ &\leq nS + \sqrt{n}\|\mathbf{c} - nS\mathbf{e}_1\| \\ &\leq 1.5 \cdot nS. \end{aligned}$$

It remains to show that $Rot(\mathbf{c})$ is nonsingular, or equivalently, the n-dimensional volume of $\mathcal{P}(Rot(\mathbf{c}))$ is nonzero. Notice that $\mathcal{P}(Rot(\mathbf{c}))$ is an almost cubic parallelepiped obtained by perturbing the main vertices of a hypercube of size $l = nS$ by at most $\epsilon = (\sqrt{n}/2)S$. In [41] it is shown that, for all $\epsilon < \sqrt{1 - 1/n} \cdot l/\sqrt{n}$, the minimal volume of any such parallelepiped is $(1-\epsilon)^n l^n$. In particular the volume is nonzero.[4] Since

$$\epsilon = \frac{\sqrt{n}}{2} S < \sqrt{n} S \sqrt{1 - \frac{1}{n}} = \sqrt{1 - \frac{1}{n}} \cdot \frac{l}{\sqrt{n}},$$

the volume of $\mathcal{P}(Rot(\mathbf{c}))$ is nonzero, and the matrix $Rot(\mathbf{c})$ has full rank. □

In [44], Lemma 2.13 is used to prove that the expected squared norm $\|\mathbf{d} - \mathbf{c}\|^2$ (when $\mathbf{d}$ is chosen according to distribution $D_{\Lambda,\mathbf{s},\mathbf{c}}$) is at most $s^2 \cdot n$. In this paper we will need a bound on the expected value of the convolution product $\|(\mathbf{d} - \mathbf{c}) \otimes \mathbf{x}\|^2$. It immediately follows from the result in [44] and inequality $\|\mathbf{x} \otimes \mathbf{y}\| \leq \sqrt{n}\|\mathbf{x}\| \cdot \|\mathbf{y}\|$ that for any vector $\mathbf{x}$, the expectation of $\|(\mathbf{d} - \mathbf{c}) \otimes \mathbf{x}\|^2$ is at most $s^2 \cdot n^2 \cdot \|\mathbf{x}\|^2$. Below, we use Lemma 2.13 to directly prove a stronger bound.

Lemma 3.2 *For any n-dimensional lattice Λ, positive reals $\epsilon \leq 1/3$, $s \geq 2\eta_\epsilon(\Lambda)$ and vectors $\mathbf{c}, \mathbf{x} \in \mathbb{R}^n$,*

$$\underset{\mathbf{d} \sim D_{\Lambda,s,\mathbf{c}}}{\mathrm{Exp}} \left[\|(\mathbf{d} - \mathbf{c}) \otimes \mathbf{x}\|^2 \right] \leq s^2 \cdot n \cdot \|\mathbf{x}\|^2.$$

Proof: Let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be the standard basis of $\mathbb{R}^n$. Notice that $(\mathbf{d} - \mathbf{c}) \otimes \mathbf{x} = \mathbf{x} \otimes (\mathbf{d} - \mathbf{c}) = Rot(\mathbf{x}) \cdot (\mathbf{d} - \mathbf{c})$, and $\mathbf{e}_i^T \cdot Rot(\mathbf{x}) = (rot^i(\tilde{\mathbf{x}}))^T$, where $\tilde{\mathbf{x}} = (x_n, \ldots, x_1)^T$ is the reverse of $\mathbf{x}$. By linearity of expectation, we have

$$\underset{\mathbf{d} \sim D_{\Lambda,s,\mathbf{c}}}{\mathrm{Exp}} \left[\|(\mathbf{d} - \mathbf{c}) \otimes \mathbf{x}\|^2 \right] = \sum_{i=1}^{n} \underset{\mathbf{d} \sim D_{\Lambda,s,\mathbf{c}}}{\mathrm{Exp}} \left[\langle \mathbf{e}_i, (\mathbf{d} - \mathbf{c}) \otimes \mathbf{x} \rangle^2 \right].$$

For every $i = 1, \ldots, n$,

$$\begin{aligned} \langle \mathbf{e}_i, (\mathbf{d} - \mathbf{c}) \otimes \mathbf{x} \rangle &= \mathbf{e}_i^T \cdot Rot(\mathbf{x}) \cdot (\mathbf{d} - \mathbf{c}) \\ &= \langle rot^i(\tilde{\mathbf{x}}), \mathbf{d} - \mathbf{c} \rangle \\ &= \|\mathbf{x}\| \langle \mathbf{u}_i, \mathbf{d} - \mathbf{c} \rangle \end{aligned}$$

where $\mathbf{u}_i = rot^i(\tilde{\mathbf{x}})/\|\mathbf{x}\|$ is a unit vector. So,

$$\underset{\mathbf{d} \sim D_{\Lambda,s,\mathbf{c}}}{\mathrm{Exp}} \left[\|(\mathbf{d} - \mathbf{c}) \otimes \mathbf{x}\|^2 \right] = \|\mathbf{x}\|^2 \cdot \sum_{i=1}^{n} \underset{\mathbf{d} \sim D_{\Lambda,s,\mathbf{c}}}{\mathrm{Exp}} \left[\langle \mathbf{u}_i, \mathbf{d} - \mathbf{c} \rangle^2 \right].$$

Using the assumption $s \geq 2\eta_\epsilon(\Lambda)$ and applying Lemma 2.13, we get that for all $i = 1, \ldots, n$,

$$\underset{\mathbf{d} \sim D_{\Lambda,s,\mathbf{c}}}{\mathrm{Exp}} \left[\langle \mathbf{u}_i, \mathbf{d} - \mathbf{c} \rangle^2 \right] \leq s^2 \left(\frac{1}{2\pi} + \frac{\epsilon}{1 - \epsilon} \right) \leq s^2 \left(\frac{1}{2\pi} + \frac{1/3}{1 - 1/3} \right) \leq s^2.$$

Adding up for all i and substituting in the previous equation we get

$$\underset{\mathbf{d} \sim D_{\Lambda,s,\mathbf{c}}}{\mathrm{Exp}} \left[\|(\mathbf{d} - \mathbf{c}) \otimes \mathbf{x}\|^2 \right] \leq s^2 \|\mathbf{x}\|^2 n.$$

□

[4] The minimal volume $(1-\epsilon)^n l^n$ is achieved by the intuitive solution that shortens each edge by ϵ. Interestingly, as shown in [41], when $\epsilon = l/\sqrt{n}$ there are better ways to choose the perturbations that result in a singular parallelepiped with zero volume.

4 Generalized compact knapsacks

The hash function families considered in this paper, as well as previous works [1, 9, 40, 42, 44], are all special cases of the following general definition.

Definition 4.1 *For any ring R, subset $S \subset R$ and integer $m \geq 1$, the generalized knapsack function family $\mathcal{H}(R, S, m) = \{f_{\mathbf{a}} : S^m \to R\}_{\mathbf{a} \in R^m}$ is defined by*

$$f_{\mathbf{a}}(\mathbf{x}) = \sum_{i=1}^{m} x_i \cdot a_i,$$

for all $\mathbf{a} \in R^m$ and $\mathbf{x} \in S^m$, where $\sum_i x_i \cdot a_i$ is computed using the ring addition and multiplication operations.

In this paper we consider the ring $R = (\mathbb{F}^n_{p(n)}, +, \otimes)$ of n-dimensional vectors over the finite field $\mathbb{F}_{p(n)}$ with $p(n) = n^{O(1)}$ elements, with the usual vector addition operation and convolution product $\otimes$. For brevity, we will denote this ring simply as $\mathbb{F}^n_{p(n)}$. We remark that for any prime p, the field $\mathbb{F}_p$ is isomorphic to the ring $\mathbb{Z}_p$ of integers modulo p. Here we use notation $\mathbb{F}^n_p$ instead of $\mathbb{Z}^n_p$ both because some of our results are valid even when p is not a prime, and also to emphasize that $\mathbb{F}^n_p$ is the ring of vectors with the convolution product operation, rather than the componentwise multiplication of the product ring $\mathbb{Z}^n_p$.

As for S, we consider the set $S = D^n \subset \mathbb{F}^n_p$ of vectors with entries in an appropriately selected subset of $\mathbb{F}_p$. We want to study the hash function family $\mathcal{H}(\mathbb{F}^n_p, D^n, m)$, and prove that it is both almost regular and one-way.

The rest of the section is organized as follows. In Subsection 4.1 we prove that $\mathcal{H}(\mathbb{F}^n_p, D^n, m)$ is almost regular. In Subsection 4.2 we introduce and start studying a new worst-case lattice problem that will be instrumental to prove our main results. In Subsection 4.3 we give a reduction from solving this problem in the worst case to the problem of inverting functions $\mathcal{H}(\mathbb{F}^n_p, D^n, m)$ on the average. Finally, in Subsection 4.4 we establish relations between inverting $\mathcal{H}(\mathbb{F}^n_p, D^n, m)$ on the average, and solving various other worst-case problems on cyclic lattices, like SIVP and GDD$^\rho$.

4.1 Regularity lemma

For any ring R of size $|R| \geq 2^n$, a necessary condition for the hash function family $\mathcal{H}(R, \{0,1\}, m)$ to be almost regular is $m \geq \Omega(\log |R|) \geq \Omega(\log n)$, because when $m \leq o(\log |R|)$, almost a tiny fraction of the elements of R can be expressed as the sum of a subset of $\{a_1, \ldots, a_m\}$. In this subsection we prove that the hash function family $\mathcal{H}(\mathbb{F}^n_p, D^n, m)$ is almost regular already when $m = \omega(1)$ is an unbounded function with arbitrarily slow growth rate. Our proof is quite different from the standard proof for the subset-sum function $\mathcal{H}(R, \{0,1\}, m)$. In particular, while the proof for $\mathcal{H}(R, \{0,1\}, m)$ only relies on the additive structure of R, our proof makes full use of the ring properties of $\mathbb{F}^n_p$ and the characterization of its ideals as quotients of polynomial rings.

Theorem 4.2 *For any finite field $\mathbb{F}$, subset $D \subset \mathbb{F}$, and integers n, m, the hash function family $\mathcal{H}(\mathbb{F}^n, D^n, m)$ is ϵ-regular for*

$$\epsilon = \frac{1}{2}\sqrt{(1 + |\mathbb{F}|/|D|^m)^n - 1}.$$

In particular, for any $p(n) = n^{O(1)}$, $|D_n| = n^{\Omega(1)}$ and $m(n) = \omega(1)$, the function ensemble $\mathcal{H}(\mathbb{F}^n_{p(n)}, D^n_n, m(n))$ is almost regular.

The proof of the theorem is based on the following lemma of Impagliazzo and Zuckerman.

Lemma 4.3 ([25, Claim 2]) *Let V, V' be independent and identically distributed random variables taking values in a finite set S. If V, V' have collision probability $\Pr\{V = V'\} \leq (1 + 4\epsilon^2)/|S|$, then the statistical distance between V and the uniform distribution over S is at most ϵ.*

Proof: For completeness, we give a sketch of the proof. Let ϵ be the statistical distance between V and the uniform distribution. By definition of statistical distance, there is a set $X \subset S$ such that $\Pr\{V \in X\} = |X|/|S| + \epsilon$. Therefore the collision probability satisfies

$$\begin{aligned}
\Pr\{V = V'\} &= \Pr\{\ V = V' \mid V, V' \in X\ \} \Pr\{V \in X\}^2 + \Pr\{\ V = V' \mid V, V' \notin X\ \} \Pr\{V \notin X\}^2 \\
&\geq \frac{\Pr\{V \in X\}^2}{|X|} + \frac{\Pr\{V \notin X\}^2}{|S| - |X|} \\
&= \frac{1}{|S|} + \frac{\epsilon^2 |S|}{|X|(|S| - |X|)}
\end{aligned}$$

which is minimized when $|X| = |S|/2$. Substituting $|X| = |S|/2$, we get that the collision probability is at least $(1 + 4\epsilon^2)/|S|$. □

We also need the following simple lemma.

Lemma 4.4 *Let R be a finite ring, and $z_1, \ldots, z_m \in R$ a sequence of arbitrary ring elements. If $a_1, \ldots, a_m \in R$ are independently and uniformly distributed ring elements, then $\sum a_i \cdot z_i$ is uniformly distributed over the ideal $\langle z_1, \ldots, z_m \rangle$ generated by $z_1, \ldots, z_m$. In particular, for any $z_1, \ldots, z_m \in R$ and randomly chosen $a_1, \ldots, a_m \in R$, the probability that $\sum a_i \cdot z_i = 0$ is exactly $1/|\langle z_1, \ldots, z_m \rangle|$.*

Proof: Let $z_1, \ldots, z_m \in R$ be arbitrary ring elements, and, for any $b \in R$, define $A_b = \{(a_1, \ldots, a_m) \in R^m : \sum a_i \cdot z_i = b\}$. Notice that the probability that $\sum_i a_i \cdot z_i = b$ (over the random choice of $a_1, \ldots, a_m$) equals $|A_b|/|R|^m$. If $b \notin \langle z_1, \ldots, z_m \rangle$, then $A_b = \emptyset$ and $\Pr\{\sum a_i \cdot z_i = b\} = 0$. It remains to prove that all $b \in \langle z_1, \ldots, z_m \rangle$ have the same probability. Let $b = \sum a_i \cdot z_i$ an arbitrary element of $\langle z_1, \ldots, z_m \rangle$. We claim that $|A_b| = |A_0|$. It is easy to see that $\mathbf{a}' \in A_b$ if and only if $\mathbf{a}' - \mathbf{a} \in A_0$. Since $\mathbf{a}' \mapsto \mathbf{a}' - \mathbf{a}$ is a bijection between A_b and A_0, it follows that $|A_b| = |A_0|$. This proves that all $b \in R$ have the same probability $|A_b|/|R|^m = |A_0|/|R|^m$, and completes the proof of the lemma. □

We are now ready to prove the theorem.

Proof [of Theorem 4.2]: We want to prove that $\textsc{owf}(\mathcal{H}(\mathbb{F}^n, D^n, m))$ is very close to the uniform distribution over $(\mathbb{F}^n)^m \times \mathbb{F}^n$. We first bound the collision probability of two independent copies of $\textsc{owf}(\mathcal{H}(\mathbb{F}^n, D^n, m))$. Let $((\mathbf{a}_1, \ldots, \mathbf{a}_m), \sum_i \mathbf{a}_i \otimes \mathbf{x}_i)$ and $((\mathbf{a}'_1, \ldots, \mathbf{a}'_m), \sum_i \mathbf{a}'_i \otimes \mathbf{x}_i)$ be two independent samples chosen according to the distribution $\textsc{owf}(\mathcal{H}(\mathbb{F}^n, D^n, m))$. By definition, the elements $\mathbf{a}_i, \mathbf{a}'_i \in \mathbb{F}^n$ and $\mathbf{x}_i, \mathbf{x}'_i \in D^n$ are all chosen independently and uniformly at random from their respective sets. Therefore, the collision probability is

$$\begin{aligned}
\Pr\left\{\forall i.\mathbf{a}_i = \mathbf{a}'_i \wedge \sum_{i=1}^m \mathbf{a}_i \otimes \mathbf{x}_i = \sum_{i=1}^m \mathbf{a}'_i \otimes \mathbf{x}'_i\right\} &= \Pr\{\forall i.\mathbf{a}_i = \mathbf{a}'_i\} \\
&\quad \cdot \Pr\left\{\ \textstyle\sum_{i=1}^m \mathbf{a}_i \otimes \mathbf{x}_i = \sum_{i=1}^m \mathbf{a}'_i \otimes \mathbf{x}'_i \mid \forall i.\mathbf{a}_i = \mathbf{a}'_i\ \right\} \\
&= \frac{1}{|\mathbb{F}|^{mn}} \cdot \Pr\left\{\sum_{i=1}^m \mathbf{a}_i \cdot (\mathbf{x}_i - \mathbf{x}'_i) = \mathbf{0}\right\}.
\end{aligned}$$

By Lemma 4.4, the probability (over the random choice of $\mathbf{a}_1, \ldots, \mathbf{a}_m$) that $\sum_i \mathbf{a}_i \otimes (\mathbf{x}_i - \mathbf{x}'_i) = \mathbf{0}$ equals $1/|I|$ where $I = \langle \mathbf{x}_1 - \mathbf{x}'_1, \ldots, \mathbf{x}_m - \mathbf{x}'_m \rangle$ is the ideal generated by $\mathbf{x}_1 - \mathbf{x}'_1, \ldots, \mathbf{x}_m - \mathbf{x}'_m$. Let $\mathcal{I}$ be the set of all ideals of $(\mathbb{F}^n, +, \otimes)$. Conditioning on the value of I, the collision probability can be expressed as

$$\begin{aligned}
\frac{1}{|\mathbb{F}|^{mn}} \cdot \Pr\left\{\sum_{i=1}^m \mathbf{a}_i \cdot (\mathbf{x}_i - \mathbf{x}'_i) = \mathbf{0}\right\} &= \frac{1}{|\mathbb{F}|^{nm}} \cdot \sum_{I \in \mathcal{I}} \frac{\Pr\{\langle \mathbf{x}_1 - \mathbf{x}'_1, \ldots, \mathbf{x}_m - \mathbf{x}'_m \rangle = I\}}{|I|} \\
&\leq \frac{1}{|\mathbb{F}|^{nm}} \cdot \sum_{I \in \mathcal{I}} \frac{\Pr\{\langle \mathbf{x}_1 - \mathbf{x}'_1, \ldots, \mathbf{x}_m - \mathbf{x}'_m \rangle \subseteq I\}}{|I|} \\
&= \frac{1}{|\mathbb{F}|^{n(m+1)}} \cdot \sum_{I \in \mathcal{I}} \frac{|\mathbb{F}|^n}{|I|} \cdot \prod_{i=1}^m \Pr\{(\mathbf{x}_i - \mathbf{x}'_i) \in I\}.
\end{aligned}$$

In the rest of the proof, we regard $\mathbb{F}^n$ as the ring of univariate polynomials $\mathbb{F}[\alpha]$ modulo $\alpha^n - 1$. Since $\mathbb{F}$ is a field, $\mathbb{F}[\alpha]$ is a principal ideal domain, i.e., all ideals in $\mathbb{F}[\alpha]$ are of the form $\langle Q(\alpha)\rangle$ for some polynomial $Q(\alpha) \in \mathbb{F}[\alpha]$. It follows that all ideals $I \in \mathcal{I}$ of the quotient ring $\mathbb{F}[\alpha]/(\alpha^n - 1)$ are of the form $\langle Q(\alpha)\rangle$ where $Q(\alpha)$ is a factor of $\alpha^n - 1$. (To see this, given an ideal $I \in \mathcal{I}$, select a representative for each element of I, and let $Q(\alpha)$ be the greatest common divisor of all these representatives and the polynomial $\alpha^n - 1$.) Let $(\alpha^n - 1) = Q_1(\alpha) \cdot Q_2(\alpha) \cdot \cdots \cdot Q_r(\alpha)$ be the factorization of $(\alpha^n - 1)$ into irreducible polynomials over $\mathbb{F}$, and for any subset $S \subseteq \{1, \ldots, r\}$, let $Q_S(\alpha) = \Pi_{i\in S} Q_i(\alpha)$. The ideals of R are $\mathcal{I} = \{\langle Q_S\rangle : S \subseteq \{1, \ldots, r\}\}$. For any ideal $\langle Q_S\rangle \in \mathcal{I}$, we have $|\langle Q_S\rangle| = |\mathbb{F}|^{n-\deg Q_S}$ and

$$\Pr\{(\mathbf{x}_i - \mathbf{x}'_i) \in \langle Q_S\rangle\} = \Pr\{\mathbf{x}_i \equiv \mathbf{x}'_i \bmod Q_S\} \le \max_b \Pr\{\mathbf{x}_i \bmod Q_S = b\} \le \frac{1}{|D|^{\deg(Q_S)}}.$$

Therefore,

$$\frac{|\mathbb{F}|^n}{|\langle Q_S\rangle|} \prod_{i=1}^m \Pr\{(\mathbf{x}_i - \mathbf{x}'_i) \in \langle Q_S\rangle\} \le \frac{|\mathbb{F}|^n}{|\mathbb{F}|^{n-\deg Q_S}} \left(\frac{1}{|D|^{\deg Q_S}}\right)^m = \left(\frac{|\mathbb{F}|}{|D|^m}\right)^{\deg Q_S}$$

and, adding up over all ideals,

$$\begin{aligned}\sum_{\langle Q_S\rangle\in\mathcal{I}} \frac{|\mathbb{F}|^n}{|\langle Q_S\rangle|} \prod_{i=1}^m \Pr\{(\mathbf{x}_i - \mathbf{x}'_i) \in \langle Q_S\rangle\} &\le \sum_S \left(\frac{|\mathbb{F}|}{|D|^m}\right)^{\deg Q_S} \\ &= \prod_{i=1}^r \left(1 + \left(\frac{|\mathbb{F}|}{|D|^m}\right)^{\deg Q_i}\right) \\ &\le \left(1 + \frac{|\mathbb{F}|}{|D|^m}\right)^n.\end{aligned}$$

This proves that the collision probability is at most

$$\frac{(1 + |\mathbb{F}|/|D|^m)^n}{|\mathbb{F}|^{n(m+1)}}.$$

Now observe that random variable $\text{OWF}(\mathcal{H}(\mathbb{F}^n, D^n, m))$ takes values in the set $(\mathbb{F}^n)^m \times \mathbb{F}^n$, which has size $|\mathbb{F}|^{n(m+1)}$. Therefore, by Lemma 4.3, the statistical distance between $\text{OWF}(\mathcal{H}(\mathbb{F}^n, D^n, m))$ and the uniform distribution over $(\mathbb{F}^n)^m \times \mathbb{F}^n$ is at most

$$\epsilon = \frac{1}{2}\sqrt{\left(1 + \frac{|\mathbb{F}|}{|D|^m}\right)^n - 1}.$$

□

4.2 The worst case problems

We want to show that inverting our generalized compact knapsack function $\mathcal{H}(\mathbb{F}^n, D^n, m)$ (on the average and with nonnegligible probability) is at least as hard as solving GDD_γ^ρ (as well as various other related problems) over cyclic lattices in the worst case. Following [42], this is done in two steps. First, all relevant worst-case lattice problems are reduced to an intermediate worst-case problem, and then the intermediate problem is reduced to the problem of inverting functions in $\mathcal{H}(\mathbb{F}^n, D^n, m)$ on the average. In [42], the goal is to reduce the worst-case problem GIVP_γ to the problem of inverting[5] $\mathcal{H}(\mathbb{Z}_p^n, \{\mathbf{0}, \mathbf{1}\}, m)$ on the average, and the intermediate problem is an incremental version of GIVP, where given a lattice basis $\mathbf{B}$, a set of sufficiently long linearly independent lattice vectors $\mathbf{S}$, and a hyperplane H, the goal is to find a lattice vector not in H shorter than $\|\mathbf{S}\|$ by some constant factor.

[5]In fact, [42] only requires an algorithm that finds collisions $f_{\mathbf{a}}(\mathbf{x}) = f_{\mathbf{a}}(\mathbf{x}')$, an easier problem than inverting the function $f_{\mathbf{a}}$.

Definition 4.5 *The* incremental generalized shortest independent vector *problem* $\text{IncGIVP}^{\phi}_{\gamma,c}$ *is: given a lattice basis* $\mathbf{B}$*, a hyperplane* H*, and a set of linearly independent lattice vectors* $\mathbf{S}$ *such that* $\|\mathbf{S}\| > \gamma(n)\cdot\phi(\mathcal{L}(\mathbf{B}))$*, find a lattice vector* $\mathbf{s}\in\mathcal{L}(\mathbf{B})\setminus H$ *such that* $\|\mathbf{s}\|\leq\|\mathbf{S}\|/c$*.*

In [42] it is shown that $\text{GIVP}^{\phi}_{\gamma}$ is polynomial time reducible to $\text{IncGIVP}^{\phi}_{\gamma,2}$. The reduction given in [42] has also the additional property that all calls made by the reduction to the IncGIVP oracle are of the form $(\mathbf{B},\mathbf{S},H)$ where $\mathbf{B}$ is the GIVP input lattice basis. If a reduction between lattice problems has this property, then we say that the reduction is lattice preserving. Lattice preserving reductions are particularly useful in the context of our paper because they allow to reduce a (worst-case) lattice problem over a given class of lattices (e.g., cyclic lattices) to another (worst-case) lattice problem over the same class of lattices.

Theorem 4.6 ([42], Theorem 6.3) *There is a polynomial time lattice preserving reduction from* $\text{GIVP}^{\phi}_{\gamma}$ *to* $\text{IncGIVP}^{\phi}_{\gamma,2}$*.*

Here we consider a different intermediate problem, which is an incremental version of GDD, where one is given a GDD instance $(\mathbf{B},\mathbf{t})$, a set of n linearly independent vectors $\mathbf{S}\subset\mathcal{L}(\mathbf{B})$, and a sufficiently large real parameter r, and the goal is to find a lattice vector whose distance from the target is smaller than $\|\mathbf{S}\|+r$ by some constant factor.

Definition 4.7 *The* incremental guaranteed distance decoding *problem* ($\text{IncGDD}^{\phi}_{\gamma,c}$)*, given an* n*-dimensional lattice* $\mathbf{B}$*, a set of* n *linearly independent vectors* $\mathbf{S}\subset\mathcal{L}(\mathbf{B})$*, a target* $\mathbf{t}\in\mathbb{R}^n$*, and a real* $r>\gamma(n)\cdot\phi(\mathcal{L}(\mathbf{B}))$*, asks for a lattice vector* $\mathbf{s}\in\mathcal{L}(\mathbf{B})$ *such that* $\|\mathbf{s}-\mathbf{t}\|\leq(\|\mathbf{S}\|+r)/c$*.*

We want to prove a result similar to Theorem 4.6, but for the GDD problem and its incremental variant IncGDD.

Theorem 4.8 *For any* $c>8$*, there is a polynomial time lattice preserving reduction from* $\text{GDD}^{\phi}_{\gamma}$ *to* $\text{IncGDD}^{\phi}_{\gamma,c}$*.*

Proof: The reduction works in three stages. We first solve the GDD problem assuming we have oracles to solve both IncGDD and GIVP. Next, we use Theorem 4.6 to reduce GIVP to IncGIVP. Finally, we reduce IncGIVP to IncGDD, so that the original GDD problem can be solved using an oracle for IncGDD alone. All the reductions are lattice preserving, and therefore their combination is lattice preserving too.

Let $(\mathbf{B},\mathbf{t})$ be a $\text{GDD}^{\phi}_{\gamma}$ instance, and assume we have access to both an $\text{IncGDD}^{\phi}_{\gamma,c}$ oracle and a $\text{GIVP}^{\phi}_{\gamma,2}$ one. First we use the $\text{GIVP}^{\phi}_{\gamma,2}$ oracle on input $\mathbf{B}$ to find a set of linearly independent lattice vectors $\mathbf{S}\subset\mathcal{L}(\mathbf{B})$ such that $\|\mathbf{S}\|\leq\gamma(n)\cdot\phi(\mathcal{L}(\mathbf{B}))$. Then, we perform a binary search on the value of r until we find a value such that the IncGDD oracle successfully solves instance $(\mathbf{B},\mathbf{S},\mathbf{t},r)$, but fails on input $(\mathbf{B},\mathbf{S},\mathbf{t},r/2)$. Let $\mathbf{s}\in\mathcal{L}(\mathbf{B})$ be the solution returned by the oracle on input $(\mathbf{B},\mathbf{S},\mathbf{t},r)$. We know that $r/2\leq\gamma(n)\cdot\phi(\mathcal{L}(\mathbf{B}))$ because IncGDD failed on input $(\mathbf{B},\mathbf{S},\mathbf{t},r/2)$. Therefore

$$\operatorname{dist}(\mathbf{s},\mathbf{t})\leq\frac{\|\mathbf{S}\|+r}{c}\leq\frac{\gamma(n)\cdot\phi(\mathcal{L}(\mathbf{B}))+2\gamma(n)\cdot\phi(\mathcal{L}(\mathbf{B}))}{c}\leq\frac{3}{c}\gamma(n)\cdot\phi(\mathcal{L}(\mathbf{B})).$$

By Theorem 4.6, the $\text{GIVP}^{\phi}_{\gamma}$ oracle needed in the previous reduction, can be implemented given an $\text{IncGIVP}^{\phi}_{\gamma,2}$ oracle. It remains to show that there is a lattice preserving reduction from $\text{IncGIVP}^{\phi}_{\gamma,2}$ to $\text{IncGDD}^{\phi}_{\gamma,c}$ for any $c>8$. The reduction is very simple and works as follows. Let $(\mathbf{B},\mathbf{S},H)$ be the $\text{IncGIVP}^{\phi}_{\gamma,2}$ input instance. Let $\mathbf{t}$ be a vector orthogonal to H of length $\|\mathbf{S}\|/4$, and $r=\|\mathbf{S}\|$. Notice that, since $(\mathbf{B},\mathbf{S},H)$ is a valid $\text{IncGIVP}^{\phi}_{\gamma,2}$ instance, we have $r=\|\mathbf{S}\|>\gamma(n)\cdot\phi(\mathcal{L}(\mathbf{B}))$. This proves that $(\mathbf{B},\mathbf{S},\mathbf{t},r)$ is a valid instance of $\text{IncGDD}^{\phi}_{\gamma,c}$. Let $\mathbf{s}$ be the solution returned by the $\text{IncGDD}^{\phi}_{\gamma,c}$ oracle on input $(\mathbf{B},\mathbf{S},\mathbf{t},r)$. We know that $\mathbf{s}\in\mathcal{L}(\mathbf{B})$ and

$$\operatorname{dist}(\mathbf{s},\mathbf{t})\leq\frac{\|\mathbf{S}\|+r}{c}=\frac{2\|\mathbf{S}\|}{c}<\frac{\|\mathbf{S}\|}{4}.$$

Therefore, $\mathbf{s} \notin H$ because

$$\operatorname{dist}(\mathbf{s}, H) \geq \operatorname{dist}(\mathbf{t}, H) - \operatorname{dist}(\mathbf{s}, \mathbf{t}) > \|\mathbf{t}\| - \frac{\|\mathbf{S}\|}{4} \geq 0.$$

Moreover, by the triangle inequality,

$$\|\mathbf{s}\| \leq \|\mathbf{t}\| + \operatorname{dist}(\mathbf{s}, \mathbf{t}) < \frac{\|\mathbf{S}\|}{4} + \frac{\|\mathbf{S}\|}{4} = \frac{\|\mathbf{S}\|}{2}.$$

This proves that $\mathbf{s}$ is a solution to the original $\textsc{IncGIVP}^{\phi}_{\gamma,2}$ problem. □

4.3 The main reduction

In this section we reduce the worst-case problem $\textsc{IncGDD}^{\eta}_{\gamma,c}$ on cyclic lattices to the problem of inverting the compact knapsack functions $\textsc{owf}(\mathcal{H}(\mathbb{F}^n_{p(n)}, D_n, m(n)))$ on the average.

Theorem 4.9 *For any constants $c' > 2c$ and $\delta > 0$, negligible function $\epsilon(n) = n^{-\omega(1)}$, and polynomially bounded functions $m(n) = \omega(1)$ and $p(n) \geq (c' \cdot m(n) \cdot n^{2.5})^{1/(1-\delta)}$, there is a probabilistic polynomial time reduction from solving $\textsc{IncGDD}^{\eta_\epsilon}_{\gamma(n),c}$ within a factor $\gamma(n) = c' \cdot m(n) \cdot n \cdot p(n)^\delta$ in the worst case over cyclic lattices (with high probability), to solving random instances of $\textsc{owf}(\mathcal{H}(\mathbb{F}^n_{p(n)}, \llbracket p(n)^\delta \rrbracket^n, m(n)))$ on the average (with nonnegligible probability).*

Proof: For any equation $\mathbf{Q} = (\mathbf{q}_1, \ldots, \mathbf{q}_{m(n)}; \mathbf{q}_0) \in \mathbb{F}^{n \cdot m(m)}_{p(n)} \times \mathbb{F}^n_{p(n)}$, let

$$\Gamma(\mathbf{Q}) = \left\{ \mathbf{X} = (\mathbf{x}_1, \ldots, \mathbf{x}_{m(n)}) \colon \forall i. \mathbf{x}_i \in \llbracket p^\delta \rrbracket^n \wedge \sum_{i=1}^{m(n)} \mathbf{q}_i \otimes \mathbf{x}_i = \mathbf{q}_0 \bmod p(n) \right\}$$

be the corresponding set of solutions. Let $\mathcal{F}$ be an oracle that on input an instance $\mathbf{Q}$ of the knapsack function inversion problem selected at random according to distribution $\textsc{owf}(\mathcal{H}(\mathbb{F}^n_{p(n)}, \llbracket p(n)^\delta \rrbracket^n, m(n)))$, outputs a solution $\mathcal{F}(\mathbf{Q}) \in \Gamma(\mathbf{Q})$ with nonnegligible probability. Let $\lambda(n)$ be the probability that $\mathcal{F}(\tilde{\mathbf{Q}}) \in \Gamma(\tilde{\mathbf{Q}})$ when $\tilde{\mathbf{Q}}$ is selected uniformly at random from $\mathbb{F}^{n \cdot m(m)}_{p(n)} \times \mathbb{F}^n_{p(n)}$. Since $p(n) = n^{O(1)}$, $|\llbracket p(n)^\delta \rrbracket| \geq p(n)^\delta = n^{\Omega(1)}$ and $m(n) = \omega(1)$, by Theorem 4.2 the probability distribution $\textsc{owf}(\mathcal{H}(\mathbb{F}^n_{p(n)}, \llbracket p(n)^\delta \rrbracket^n, m(n)))$ is statistically close to the uniform one $U(\mathbb{F}^{n \cdot m(m)}_{p(n)} \times \mathbb{F}^n_{p(n)})$. Therefore, $\lambda(n)$ is nonnegligible too. We use $\mathcal{F}$ to solve problem $\textsc{IncGDD}^{\eta}_{\gamma,c}$ over cyclic lattices in the worst case, with nonnegligible probability $\Omega(\lambda(n))$. Since we are solving $\textsc{IncGDD}^{\eta}_{\gamma,c}$ in the worst case, the success probability of the reduction can be made exponentially close to 1 using standard repetition techniques.

Let $(\mathbf{B}, \mathbf{S}, \mathbf{t}, r)$ be a valid $\textsc{IncGDD}^{\eta}_{\gamma,c}$ instance such that the lattice $\mathcal{L}(\mathbf{B})$ is cyclic. We know that $\mathcal{L}(\mathbf{S})$ is a (not necessarily cyclic) full rank sublattice of $\mathcal{L}(\mathbf{B})$, and $r > \gamma(n) \cdot \eta_{\epsilon(n)}(\mathcal{L}(\mathbf{B}))$ for some negligible function $\epsilon(n) = n^{-\omega(1)}$. The goal of the reduction is to find a lattice vector $\mathbf{s} \in \mathcal{L}(\mathbf{B})$ within distance $(r + \|\mathbf{S}\|)/c$ from the target $\mathbf{t}$. The reduction works as follows:

1. Use Lemma 3.1 to find a vector $\mathbf{c} \in \mathcal{L}(\mathbf{S}) \subseteq \mathcal{L}(\mathbf{B})$ of length $\|\mathbf{c}\|_1 \leq 2 \cdot n \cdot \|\mathbf{S}\|$ such that $Rot(\mathbf{c})$ has full rank.
2. For $i = 0, \ldots, m(n)$, do the following
   (a) Use Lemma 2.7 to generate a uniformly random lattice vector $\mathbf{v}_i \in \mathcal{L}(\mathbf{B}) \cap \mathcal{P}(Rot(\mathbf{c}))$.
   (b) Generate a random noise vector $\mathbf{y}_i$ with probability density $\mathbf{y}_i \sim \rho_s / s^n$ for $s = 2r/\gamma(n)$, and let $\mathbf{y}'_i = \mathbf{y}_i \bmod \mathbf{B}$.
   (c) Compute $\mathbf{a}_i = \lfloor p(n) \cdot Rot^{-1}(\mathbf{c})(\mathbf{v}_i + \mathbf{y}'_i) \rceil$.
3. Compute $\mathbf{b} = \lfloor p(n) \cdot Rot^{-1}(\mathbf{c})\mathbf{t} \rceil$.

4. Define the equation

$$\mathbf{Q} = (\mathbf{a}_1 \bmod p(n), \ldots, \mathbf{a}_m \bmod p(n); \mathbf{a}_0 + \mathbf{b} \bmod p(n)) \tag{4.4}$$

and invoke $\mathcal{F}(\mathbf{Q})$ to find a potential solution $\mathbf{X} = (\mathbf{x}_1, \ldots, \mathbf{x}_{m(n)})$, where $\mathbf{x}_i \in \llbracket p(n)^\delta \rrbracket^n$ for all $i = 1, \ldots, m(n)$.

5. Let $\mathbf{x}_0 = -\mathbf{e}_1$, and return the vector

$$\mathbf{s} = \sum_{i=0}^{m(n)} \left(\mathbf{v}_i + \mathbf{y}'_i - \frac{\mathbf{c} \otimes \mathbf{a}_i}{p(n)} - \mathbf{y}_i \right) \otimes \mathbf{x}_i + \frac{\mathbf{c} \otimes \mathbf{b}}{p(n)}.$$

The correctness of the reduction is based on the following two lemmas. The first lemma shows that if the oracle $\mathcal{F}$ successfully outputs a solution to equation $\mathbf{Q}$, then the reduction outputs a lattice vector $\mathbf{s} \in \mathcal{L}(\mathbf{B})$.

Lemma 4.10 *If $(\mathbf{x}_1, \ldots, \mathbf{x}_{m(n)})$ is a valid solution to equation (4.4), then $\mathbf{s} \in \mathcal{L}(\mathbf{B})$ is a lattice vector.*

Proof: Assume $(\mathbf{x}_1, \ldots, \mathbf{x}_{m(n)})$ is a valid solution to equation (4.4), i.e.,

$$\sum_{i=1}^{m(n)} \mathbf{a}_i \otimes \mathbf{x}_i \equiv (\mathbf{a}_0 + \mathbf{b}) \bmod p(n).$$

Using the distributive and associative properties of $\otimes$, vector $\mathbf{s}$ can be rewritten as the sum

$$\mathbf{s} = \sum_{i=0}^{m(n)} (\mathbf{v}_i + \mathbf{y}'_i - \mathbf{y}_i) \otimes \mathbf{x}_i - \mathbf{c} \otimes \frac{\sum_{i=0}^{m(n)} \mathbf{a}_i \otimes \mathbf{x}_i - \mathbf{b}}{p(n)}.$$

We claim that all terms in the summation belong to the lattice $\mathcal{L}(\mathbf{B})$. First of all notice that for any $i \geq 0$, the vector $\mathbf{v}_i + \mathbf{y}'_i - \mathbf{y}_i$ belongs to the lattice $\mathcal{L}(\mathbf{B})$ because $\mathbf{v}_i \in \mathcal{L}(\mathbf{B})$ and $\mathbf{y}'_i \equiv \mathbf{y}_i$ modulo $\mathcal{L}(\mathbf{B})$. Using the cyclicity of $\mathcal{L}(\mathbf{B})$, we get that all columns of $\mathit{Rot}(\mathbf{v}_i + \mathbf{y}'_i - \mathbf{y}_i)$ belong to the lattice, and

$$(\mathbf{v}_i + \mathbf{y}'_i - \mathbf{y}_i) \otimes \mathbf{x}_i = \mathit{Rot}(\mathbf{v}_i + \mathbf{y}'_i - \mathbf{y}_i) \cdot \mathbf{x}_i \in \mathcal{L}(\mathbf{B})$$

because $\mathbf{x}_i$ has integer entries. For the last term, we use the fact that $(\mathbf{x}_1, \ldots, \mathbf{x}_{m(n)})$ is a solution to the linear equation (4.4) and $\mathbf{a}_0 \otimes \mathbf{x}_0 = -\mathbf{a}_0$, yielding

$$\sum_{i \geq 0} \mathbf{a}_i \otimes \mathbf{x}_i - \mathbf{b} = \sum_{i \geq 1} \mathbf{a}_i \otimes \mathbf{x}_i - (\mathbf{a}_0 + \mathbf{b}) \equiv \mathbf{0} \bmod p(n).$$

Therefore $(\sum_{i \geq 0} \mathbf{a}_i \otimes \mathbf{x}_i - \mathbf{b})/p(n)$ is an integer vector, and

$$\mathbf{c} \otimes \frac{\sum_{i \geq 0} \mathbf{a}_i \otimes \mathbf{x}_i - \mathbf{b}}{p(n)} = \mathit{Rot}(\mathbf{c}) \cdot \frac{\sum_{i \geq 0} \mathbf{a}_i \otimes \mathbf{x}_i - \mathbf{b}}{p(n)} \in \mathcal{L}(\mathit{Rot}(\mathbf{c})) \subseteq \mathcal{L}(\mathbf{B}).$$

□

The second lemma shows that the input $\mathbf{Q}$ to the oracle $\mathcal{F}$ is almost uniformly distributed, and therefore $\mathcal{F}(\mathbf{Q})$ is successful with probability very close to $\lambda(n)$.

Lemma 4.11 *For any $s \geq \eta_{\epsilon(n)}(\mathcal{L}(\mathbf{B}))$, the statistical distance of equation (4.4) from the uniform distribution is at most*

$$\frac{1}{2}(m(n) + 1) \cdot \epsilon(n).$$

In particular, for any polynomially bounded $m(n) = n^{O(1)}$, and negligible function $\epsilon(n) = n^{-\omega(1)}$, the distribution of equation (4.4) is within negligible distance from the uniform distribution $U(\mathbb{F}_{p(n)}^{n \cdot m(m)} \times \mathbb{F}_{p(n)}^n)$.

Proof: We first bound the distance of each $\mathbf{a}_i \bmod p(n)$ from the uniform distribution over $\mathbb{F}^n_{p(n)}$. Notice that

$$\begin{aligned} \mathbf{a}_i \bmod p(n) &= \lfloor p(n) \cdot \mathit{Rot}^{-1}(\mathbf{c})(\mathbf{v}_i + \mathbf{y}'_i) \rfloor \bmod p(n) \\ &= \lfloor p(n) \cdot \mathit{Rot}^{-1}(\mathbf{c})((\mathbf{v}_i + \mathbf{y}'_i) \bmod \mathit{Rot}(\mathbf{c})) \rfloor. \end{aligned}$$

So, if $\mathbf{y}'_i$ were distributed uniformly at random over $\mathcal{P}(\mathbf{B})$, then $(\mathbf{v}_i + \mathbf{y}'_i) \bmod \mathit{Rot}(\mathbf{c})$ would be uniform over $\mathcal{P}(\mathit{Rot}(\mathbf{c}))$, and $\mathbf{a}_i \bmod p(n)$ would also have perfectly uniform distribution over $\mathbb{F}^n_{p(n)}$. Therefore, by Proposition 2.2 the statistical distance between $\mathbf{a}_i \bmod p(n)$ and the uniform distribution over $\mathbb{F}^n_{p(n)}$ is at most as big as the statistical distance between $\mathbf{y}'_i$ and the uniform distribution over $\mathcal{P}(\mathbf{B})$. Notice that $\mathbf{y}'_i$ has distribution $\rho_s/s^n \bmod \mathcal{P}(\mathbf{B})$. Using the assumption $s \geq \eta_\epsilon(\mathcal{L}(\mathbf{B}))$ and Lemma 2.12, we get that

$$\Delta(\mathbf{a}_i \bmod p(n), U(\mathbb{F}^n_{p(n)})) \leq \Delta(\mathbf{y}'_i, U(\mathcal{P}(\mathbf{B}))) \leq \epsilon(n)/2.$$

Now consider equation $\mathbf{Q}$. Since the elements of $\mathbf{Q}$ are independently distributed, by Proposition 2.4 we have

$$\Delta(\mathbf{Q}, U(\mathbb{F}^{n \cdot m(m)}_{p(n)} \times \mathbb{F}^n_{p(n)})) \leq \sum_{i=1}^{m(n)} \Delta(\mathbf{a}_i \bmod p(n), U(\mathbb{F}^n_{p(n)})) + \Delta(\mathbf{a}_0 + \mathbf{b} \bmod p(n), U(\mathbb{F}^n_{p(n)})).$$

The last term satisfies

$$\Delta(\mathbf{a}_0 + \mathbf{b} \bmod p(n), U(\mathbb{F}^n_{p(n)})) = \Delta(\mathbf{a}_0 \bmod p(n), (U(\mathbb{F}^n_{p(n)}) - \mathbf{b}) \bmod p(n)) = \Delta(\mathbf{a}_0 \bmod p(n), U(\mathbb{F}^n_{p(n)})).$$

Therefore,

$$\Delta(\mathbf{Q}, U(\mathbb{F}^{n \cdot m(m)}_{p(n)} \times \mathbb{F}^n_{p(n)})) \leq \sum_{i=0}^{m(n)} \Delta(\mathbf{a}_i \bmod p(n), U(\mathbb{F}^n_{p(n)})) \leq (m(n) + 1) \cdot \epsilon(n)/2.$$

□

We are now ready to prove the correctness of the reduction. Namely, we want to prove that for any rank n lattice basis $\mathbf{B}$, full rank subset $\mathbf{S} \subset \mathcal{L}(\mathbf{B})$, target $\mathbf{t}$, and $r > \gamma(n) \cdot \eta_\epsilon(\mathcal{L}(\mathbf{B}))$, the reduction outputs a lattice vector $\mathbf{s} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{s} - \mathbf{t}\| \leq (r + \|\mathbf{S}\|)/c$ with nonnegligible probability $\Omega(\lambda(n))$. By Lemma 4.10, $\mathbf{s} \in \mathcal{L}(\mathbf{B})$ is satisfied whenever oracle $\mathcal{F}$ returns a valid solution $\mathbf{X} = \mathcal{F}(\mathbf{Q}) \in \Gamma(\mathbf{Q})$. Therefore, the success probability of the reduction is at least

$$\begin{aligned} \Pr\left\{\mathbf{s} \in \mathcal{L}(\mathbf{B}), \|\mathbf{s} - \mathbf{t}\| \leq \frac{r + \|\mathbf{S}\|}{c}\right\} &\geq \Pr\left\{\mathbf{X} \in \Gamma(\mathbf{Q}), \|\mathbf{s} - \mathbf{t}\| \leq \frac{r + \|\mathbf{S}\|}{c}\right\} \\ &= \Pr\{\mathbf{X} \in \Gamma(\mathbf{Q})\} \cdot \Pr\left\{ \ \|\mathbf{s} - \mathbf{t}\| \leq \tfrac{r + \|\mathbf{S}\|}{c} \ \middle| \ \mathbf{X} \in \Gamma(\mathbf{Q}) \ \right\}. \end{aligned} \tag{4.5}$$

Let $\tilde{\mathbf{Q}} \in U(\mathbb{F}^{n \times (m(n)+1)}_{p(n)})$ be an equation distributed uniformly at random. Notice that $s = 2r/\gamma(n) > 2\eta_{\epsilon(n)}(\mathcal{L}(\mathbf{B})) > \eta_{\epsilon(n)}(\mathcal{L}(\mathbf{B}))$. So, by Lemma 4.11, $\Delta(\mathbf{Q}, \tilde{\mathbf{Q}})$ is negligible. Therefore, the first probability in (4.5) satisfies

$$\begin{aligned} \Pr\{\mathbf{X} \in \Gamma(\mathbf{Q})\} &= \Pr\{\mathcal{F}(\mathbf{Q}) \in \Gamma(\mathbf{Q})\} \\ &\geq \Pr\left\{\mathcal{F}(\tilde{\mathbf{Q}}) \in \Gamma(\tilde{\mathbf{Q}})\right\} - \Delta(\mathbf{Q}, \tilde{\mathbf{Q}}) \\ &= \lambda(n) - n^{-\omega(1)} \geq \Omega(\lambda(n)). \end{aligned}$$

We bound the second probability in (4.5) using Markov's inequality:

$$\begin{aligned} \Pr\left\{ \ \|\mathbf{s} - \mathbf{t}\| \leq \tfrac{r + \|\mathbf{S}\|}{c} \ \middle| \ \mathbf{X} \in \Gamma(\mathbf{Q}) \ \right\} &= 1 - \Pr\left\{ \ \|\mathbf{s} - \mathbf{t}\| > \tfrac{r + \|\mathbf{S}\|}{c} \ \middle| \ \mathbf{X} \in \Gamma(\mathbf{Q}) \ \right\} \\ &\geq 1 - c \cdot \frac{\mathrm{Exp}\left[\ \|\mathbf{s} - \mathbf{t}\| \ \middle| \ \mathbf{X} \in \Gamma(\mathbf{Q}) \ \right]}{r + \|\mathbf{S}\|}. \end{aligned} \tag{4.6}$$

We will prove that the conditional expectation $\mathrm{Exp}\left[\ \|\mathbf{s}-\mathbf{t}\| \ \middle|\ \mathbf{X}\in\Gamma(\mathbf{Q})\ \right]$ is at most $2(1+1/m(n))\cdot(\|\mathbf{S}\|+r)/c'$, so that, for all sufficiently large $m(n)\geq 4c/(c'-2c)$, the conditional probability in (4.5) is at least

$$1-\frac{2c}{c'}\left(1+\frac{1}{m(n)}\right)\geq\frac{c'-2c}{2c'}=\Omega(1).$$

This proves that (4.5) (and therefore also the success probability of the reduction) is at least $\Omega(\lambda(n))\cdot\Omega(1)=\Omega(\lambda(n))$.

It remains to bound the expected length of $\mathbf{s}-\mathbf{t}$. By triangle inequality,

$$\|\mathbf{s}-\mathbf{t}\|\leq\sum_{i=0}^{m(n)}\left\|(\mathbf{v}_i+\mathbf{y}'_i-\frac{\mathbf{c}\otimes\mathbf{a}_i}{p(n)})\otimes\mathbf{x}_i\right\|+\sum_{i=0}^{m(n)}\|\mathbf{y}_i\otimes\mathbf{x}_i\|+\left\|\mathbf{t}-\frac{\mathbf{c}\otimes\mathbf{b}}{p(n)}\right\|. \tag{4.7}$$

Notice that

$$\mathbf{v}_i+\mathbf{y}'_i-\frac{\mathbf{c}\otimes\mathbf{a}_i}{p(n)}=\frac{\mathbf{c}\otimes(\mathbf{w}-\lfloor\mathbf{w}\rceil)}{p(n)}$$

where $\mathbf{w}=p(n)\,Rot^{-1}(\mathbf{c})(\mathbf{v}_i+\mathbf{y}'_i)$. Since $\|\mathbf{c}\|_1\leq 2n\|\mathbf{S}\|$ by construction and $\|\mathbf{w}-\lfloor\mathbf{w}\rceil\|_\infty\leq 1/2$ for any vector $\mathbf{w}$,

$$\|\mathbf{v}_i+\mathbf{y}'_i-\frac{\mathbf{c}\otimes\mathbf{a}_i}{p(n)}\|_\infty\leq\frac{\|\mathbf{c}\|_1\cdot\|\mathbf{w}-\lfloor\mathbf{w}\rceil\|_\infty}{p(n)}\leq\frac{n\|\mathbf{S}\|}{p(n)}. \tag{4.8}$$

Similarly, we have

$$\left\|\mathbf{t}-\frac{\mathbf{c}\otimes\mathbf{b}}{p(n)}\right\|_\infty\leq\frac{n\|\mathbf{S}\|}{p(n)}. \tag{4.9}$$

Multiplying (4.8) by $\mathbf{x}_i$ and using $\|\mathbf{x}_i\|_1\leq n\cdot p(n)^\delta$, we get

$$\left\|(\mathbf{v}_i+\mathbf{y}'_i-\frac{\mathbf{c}\otimes\mathbf{a}_i}{p(n)})\otimes\mathbf{x}_i\right\|_\infty\leq\left\|\mathbf{v}_i+\mathbf{y}'_i-\frac{\mathbf{c}\otimes\mathbf{a}_i}{p(n)}\right\|_\infty\cdot\|\mathbf{x}_i\|_1\leq\frac{n^2\|\mathbf{S}\|}{p(n)^{1-\delta}}.$$

Substituting these bounds in (4.7) and using the relation $\|\mathbf{z}\|\leq\sqrt{n}\|\mathbf{z}\|_\infty$ (valid for any n-dimensional vector $\mathbf{z}$) we obtain

$$\begin{aligned}\|\mathbf{s}-\mathbf{t}\| &\leq (m(n)+1)\cdot\frac{n^{2.5}\|\mathbf{S}\|}{p(n)^{1-\delta}}+\frac{n^{1.5}\|\mathbf{S}\|}{p(n)}+\sum_{i=0}^{m(n)}\|\mathbf{y}_i\otimes\mathbf{x}_i\|\\ &\leq (m(n)+2)\cdot\frac{n^{2.5}\|\mathbf{S}\|}{p(n)^{1-\delta}}+\sum_{i=0}^{m(n)}\|\mathbf{y}_i\otimes\mathbf{x}_i\|.\end{aligned}$$

Assuming $p(n)\geq(c'\cdot m(n)\cdot n^{2.5})^{1/(1-\delta)}$, the first term in the last expression is at most

$$\begin{aligned}(m(n)+2)\cdot\frac{n^{2.5}\|\mathbf{S}\|}{p(n)^{1-\delta}} &\leq \left(1+\frac{1}{m(n)}\right)\cdot\frac{2\|\mathbf{S}\|}{c'}.\\ \left(1+\frac{2}{m(n)}\right)\cdot\frac{\|\mathbf{S}\|}{c'}.\end{aligned}$$

We want to prove that the conditional expectation of the second term satisfies

$$\mathrm{Exp}\left[\ \textstyle\sum_{i=0}^{m(n)}\|\mathbf{y}_i\otimes\mathbf{x}_i\|\ \middle|\ \mathbf{X}\in\Gamma(\mathbf{Q})\ \right]\leq\left(1+\frac{1}{m(n)}\right)\cdot\frac{2r}{c'}.$$

We consider the conditional expectation, given $\mathbf{Q}$, $\mathbf{X}$ and $\mathbf{y}'_i$ (for $i=0,\ldots,m(n)$). The claim follows by averaging over all possible values of $\mathbf{Q}$, $\mathbf{X}$ and $\mathbf{y}'_i$ such that $\mathbf{X}\in\Gamma(\mathbf{Q})$.

Given $\mathbf{y}'_i$, vector $\mathbf{y}_i$ must necessarily belong to the set $\mathbf{y}'_i + \mathcal{L}(\mathbf{B})$, but it is otherwise random and independent from $\mathbf{Q}$ and $\mathbf{X}$. So, the conditional distribution of $\mathbf{y}_i$ is

$$\Pr\{\ \mathbf{y}_i \mid \mathbf{y}'_i, \mathbf{Q}, \mathbf{X}\ \} = \Pr\{\ \mathbf{y}_i \mid \mathbf{y}'_i\ \} = \frac{\rho_s(\mathbf{y}_i)}{\rho_s(\mathbf{y}'_i + \mathcal{L}(\mathbf{B}))} = \frac{\rho_{s,-\mathbf{y}'_i}(\mathbf{y}_i - \mathbf{y}'_i)}{\rho_{s,-\mathbf{y}'_i}(\mathcal{L}(\mathbf{B}))}.$$

In other words, the conditional distribution of $(\mathbf{y}_i - \mathbf{y}'_i) \in \mathcal{L}(\mathbf{B})$ is $D_{\mathcal{L}(\mathbf{B}),s,-\mathbf{y}'_i}$. Recall that $s = 2r/\gamma(n) > 2\eta_{\epsilon(n)}(\mathcal{L}(\mathbf{B}))$. So, by Lemma 3.2,

$$\begin{aligned} \operatorname{Exp}\left[\ \|\mathbf{y}_i \otimes \mathbf{x}_i\|^2 \mid \mathbf{y}'_i\ \right] &= \operatorname{Exp}_{(\mathbf{y}_i - \mathbf{y}'_i) \sim D_{\mathcal{L}(\mathbf{B}),s,-\mathbf{y}'_i}} \|((\mathbf{y}_i - \mathbf{y}'_i) - (-\mathbf{y}'_i)) \otimes \mathbf{x}_i\|^2 \\ &\le s^2 \|\mathbf{x}_i\|^2 n \\ &\le s^2 n^2 \cdot p(n)^{2\delta}. \end{aligned}$$

By convexity, we get

$$\operatorname{Exp}\left[\ \|\mathbf{y}_i \otimes \mathbf{x}_i\| \mid \mathbf{y}'_i\ \right] \le n \cdot s \cdot p(n)^{\delta}.$$

Finally, adding up for all values of i and using the definition of $s = 2r/\gamma(n)$ and $\gamma(n) = c' m(n) \cdot n \cdot p(n)^{\delta}$, we get

$$\begin{aligned} \sum_{i=0}^{m(n)} \operatorname{Exp}\left[\ \|\mathbf{y}_i \otimes \mathbf{x}_i\| \mid \mathbf{y}'_i\ \right] &\le (m(n)+1) \cdot n \cdot s \cdot p(n)^{\delta} \\ &= \frac{2r(m(n)+1) \cdot n \cdot p(n)^{\delta}}{\gamma(n)} \\ &= \left(1 + \frac{1}{m(n)}\right) \frac{2r}{c'}. \end{aligned}$$

This concludes the proof that the conditional expectation $\operatorname{Exp}\left[\ \|\mathbf{s} - \mathbf{t}\| \mid \mathbf{X} \in \Gamma(\mathbf{Q})\ \right]$ is at most $2(1 + 1/m(n))(\|\mathbf{S}\| + r)/c'$, and the reduction succeeds with nonnegligible probability $\Omega(\lambda(n))$. □

By choosing a small enough $\delta > 0$ in the previous theorem, we obtain the following corollary.

Corollary 4.12 *For any $c > 0$, $\epsilon > 0$, $p(n) = n^{2.5+\Theta(1)}$ and $m(n) = \omega(1) \le n^{o(1)}$, there exist a constant $\delta > 0$ such that there is a reduction from solving* $\textsc{IncGDD}^{\eta}_{\gamma,c}$ *in the worst case within a factor $\gamma(n) = n^{1+\epsilon}$ to inverting $\mathcal{H}(\mathbb{F}^n_{p(n)}, \llbracket p(n)^{\delta} \rrbracket, m(n))$ on the average with nonnegligible probability.*

Proof: Let $c' = 3c$ and δ be any constant strictly smaller than $\min\{\epsilon/\log_n p(n), 1 - 2.5/\log_n p(n)\}$. Notice that

$$p(n)^{1-\delta} = n^{(1-\delta)\log_n p(n)} \ge n^{2.5+\Omega(1)} > c' m(n) n^{2.5}.$$

Therefore, by Theorem 4.9, inverting $\mathcal{H}(\mathbb{F}^n_{p(n)}, \llbracket p(n)^{\delta} \rrbracket, m(n))$ on the average is at least as hard as solving $\textsc{IncGDD}^{\eta}_{\gamma,c}$ in the worst case, for

$$\gamma(n) = c' m(n) n p(n)^{\delta} \le n^{1+o(1)+\delta \log_n p(n)} \le n^{1+\epsilon}.$$

□

4.4 Other lattice problems

In Subsection 4.3 we have shown that inverting the generalized compact knapsack functions $\mathcal{H}(\mathbb{F}^n_p, \llbracket p^{\delta} \rrbracket, \omega(1))$ on the average is at least as hard as solving the IncGDD problem over cyclic lattices in the worst case. In this subsection we relate the complexity of inverting the compact knapsack functions to other standard worst-case lattice problems.

Corollary 4.13 *For any $\epsilon > 0$, $p(n) = n^{2.5+\Theta(1)}$ and $m(n) = \omega(1) \le n^{o(1)}$, there exist a constant $\delta > 0$ such that inverting $\mathcal{H}(\mathbb{F}^n_{p(n)}, \llbracket p(n)^{\delta} \rrbracket, m(n))$ on the average with nonnegligible probability is at least as hard as solving any of the following problems in the worst case within a factor $\gamma(n) = n^{1+\epsilon}$:*

- *the guaranteed distance decoding problem* GDD_γ^η *over cyclic lattices*
- *the generalized independent vector problem* $\mathrm{GIVP}_\gamma^\eta$ *over cyclic lattices.*

Proof: Both reductions easily follow by combining Corollary 4.12 with Theorem 4.8 and Theorem 2.10. □

Finally, using known relations between η and λ_n (see Lemma 2.14) and $\lambda_n \leq 2\rho$ (see [43, Theorem 7.9]), we can relate the hardness of breaking one-way function $\mathcal{H}(\mathbb{F}_p^n, \llbracket q^\delta \rrbracket, \omega(1))$ to the standard version of the lattice problems GDD^ρ and SIVP.

Corollary 4.14 *For any* $\epsilon > 0$, $p(n) = n^{2.5+\Theta(1)}$ *and* $m(n) = \omega(1) \leq n^{o(1)}$, *there exist* $\delta > 0$ *such that inverting* $\mathcal{H}(\mathbb{F}_{p(n)}^n, \llbracket p(n)^\delta \rrbracket, m(n))$ *on the average with nonnegligible probability is at least as hard as solving any of the following problems in the worst case for* $\gamma(n) = n^{1+\epsilon}$*:*

- *the guaranteed distance decoding problem* GDD_γ^ρ *over cyclic lattices*
- *the generalized independent vector problem* SIVP_γ *over cyclic lattices.*

5 Conclusions and open problems

We have introduced a new class of very efficient one-way functions with strong security guarantees. Namely, our functions are provably hard to invert (on the average), based on a worst-case intractability assumption. The assumption is that no polynomial time algorithm can approximate SIVP, GDD^ρ, or other related lattice problems, in the worst case over cyclic lattices within a factor $n^{1+\epsilon}$ almost linear in the dimension of the lattice.

This is similar to the result proved in [1, 44] and related works, but with the following differences. On the positive side,

- our function has almost linear (in the security parameter) key size $n^{1+\epsilon}$, much smaller than the quadratic key size $\Omega(n^2)$ required by [1, 44]
- our function can be evaluated in almost linear time $n^{1+\epsilon}$, much faster (for the same value of the security parameter) than the $\Omega(n^2)$ time (linear in the key size) required by [1, 44].

These major efficiency improvements do not come for free. The price of reducing the key size and computation time is that

- we need to assume that the lattice problems SIVP, GDD^ρ, etc., are hard to approximate in the worst case, even when the input lattice is *cyclic*,
- we assume that the lattice problems SIVP, GDD^ρ, etc., are hard to approximate in the worst case within factors $n^{1+\epsilon}$ slightly bigger than the factors $\omega(n \log n)$ required in [44],
- we prove that our compact knapsack function is one-way, a weaker security property than the collision resistance property proved in [44].

In this section we elaborate on all these issues: the complexity of lattice problems on cyclic lattices, the possibility of reducing the required inapproximability factor, and the construction of cryptographic primitives other than one-way functions.

Cyclic lattices From a theoretical point of view, the main difference between our one-way functions and those studied in [1, 44] and related papers, is that our functions are based on the worst-case intractability of lattice problems on a class of lattices with a special structure: namely, *cyclic lattices.*

Many lattice problems are known to be NP-hard even in their approximation versions for sufficiently small approximation factors. For example, the shortest vector problem SVP is NP-hard (under randomized reductions) to approximate within any constant factor [2, 38, 29], while the closest vector problem CVP is NP-hard to approximate even within quasi polynomial factors $n^{O(1/\log\log n)}$ [61, 5, 13]. These results support the conjecture that lattice problems are hard to solve in the worst case, at least for arbitrary lattices. It is natural to ask whether lattice problems remain hard even when the input lattice is cyclic.

Very little is known about the computational complexity of lattice problems on cyclic lattices. In fact, as far as we know cyclic lattices have received little or no attention so far. From an algorithmic point of view, it is not clear how to exploit the cyclic structure of the lattice in state of the art lattice algorithms, e.g., lattice basis reduction. The only algorithmic results related to cyclic lattices we are aware of are [34, 23, 60, 15]. The first paper [34] shows how the solution of certain lattice problems can be speeded up by a factor n when the lattice is cyclic. This is a quite modest improvement since the running time of the best algorithms to solve these problems over general lattices is exponential in the dimension n of the lattice. A more interesting algorithmic result is given in [23, 60, 15]. The problem considered in [23] (and solved building on previous algorithms from [60, 15]) is the following: given the autocorrelation $\mathbf{x} \otimes \mathbf{x}$ of a vector $\mathbf{x}$, retrieve $\mathbf{x}$. This problem (which arises from applications in n-dimensional crystallography) is related to cyclic lattices by the fact that the autocorrelation of $\mathbf{x}$ can be expressed as a vector in the cyclic lattice generated by $\mathbf{x}$. This problem is quite different from the worst-case computational problems on cyclic lattices considered in this paper, and it is not clear if the techniques of [23, 60, 15] can be used to speed up the solution of more general problems, like SIVP or GDD over cyclic lattices. Based on the current state of knowledge, it seems reasonable to conjecture that approximation problems on cyclic lattices are computationally hard, at least in the worst case and for small polynomial approximation factors. In order to further support this conjecture, it would be nice to prove NP-hardness results for lattice problems when restricted to cyclic lattices.

We remark that our definition of cyclic lattices is analogous to the definition of cyclic codes, one of the most useful and widely studied classes of codes in coding theory. Still, no polynomial time algorithm is known for many computational problems on cyclic codes (or lattices). A very recent result somehow suggesting that no such polynomial time algorithm may exist is the proof in [20] that the nearest codeword problem (the coding analogue of the closest vector problem for lattices) for appropriately shortened Reed-Solomon codes is NP-hard. Reed-Solomon codes are a well known class of cyclic codes, so the result in [20] seems to suggest that the nearest codeword problem is hard even when the code is cyclic. Unfortunately, shortening the Reed-Solomon code (as done in [20]) destroys the cyclic structure of the code, so, the results in [20] do no imply the NP-hardness of the nearest codeword problem over cyclic codes. We leave, as an open problem, to prove hardness results for any lattice or coding problem over cyclic lattices or codes. Is the shortest vector problem on cyclic lattices NP-hard? Is the shortest independent vector problem on cyclic lattices NP-hard? What about the closest vector problem on cyclic lattices? Is the closest vector problem NP-hard even for fixed families of cyclic lattices as shown (for arbitrary lattices) in [36, 14, 54]?

It is worth noting that finding shortest vectors and sets of linearly independent vectors seem much more closely related problems for cyclic lattices than for general lattices. The intuition is that each short vector $\mathbf{x}$, also gives short vectors $rot(\mathbf{x})$,$rot^2(\mathbf{x})$, etc. If these vectors are linearly independent, than we have found a set of short linearly independent vectors. Formalizing this intuition giving reductions between SVP and SIVP (in both directions) when restricted to cyclic lattices is left as an open problem.

Average-case/worst-case connection. As done in [1, 9, 16, 40, 42, 44] for the case of the shortest vector problem, our results too can be interpreted as a connection between the worst-case and average-case complexity of various lattice problems.

In [1, 9, 16, 40, 42, 44] it is shown that finding small nonzero integer solutions to a random linear equation $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod p$ on the average is at least as hard as solving SIVP and other lattice problems in the worst case. Since the integer solutions to the equation

$$\Lambda(\mathbf{A}) = \{\mathbf{x} \colon \mathbf{A}\mathbf{x} = \mathbf{0} \bmod p\}$$

form a lattice, the result in [1, 9, 16, 40, 42, 44] can be formulated as a reduction from solving SIVP in the worst case to solving SVP on the average.

In this paper we have shown that inverting our generalized compact knapsack functions on the average is at least as hard as the worst case instance of GDD, as well as other lattices problems, over cyclic lattices. We now show how inverting the compact knapsack function can also be formulated as a lattice problem. A compact knapsack function $\mathbf{a}_1, \ldots, \mathbf{a}_m$ implicitly defines a lattice in dimension $O(m \cdot n)$ given by the set of all $(\mathbf{y}_1, \ldots, \mathbf{y}_m)$ such that $\sum \mathbf{a}_i \otimes \mathbf{y}_i = \mathbf{0}$. In fact, using matrix notation, one can consider the weights $\mathbf{a}_1, \ldots, \mathbf{a}_m$ as a compact representation of an $n \times m \cdot n$ matrix

$$\mathbf{A} = [Rot(\mathbf{a}_1)| \ldots |Rot(\mathbf{a}_m)]$$

which defines a lattice $\Lambda(\mathbf{A}) = \{\mathbf{x}: \mathbf{A}\mathbf{x} = \mathbf{0} \bmod p\}$ in the usual way. Up to a permutation of the coordinates, it is immediate to see that the lattice associated to matrix $\mathbf{A}$ above is quasi-cyclic of order m, i.e., it is invariant under shifts rot^m by m positions. Inverting the subset-sum function can be formulated as a closest vector problem instance as follows. Given $\mathbf{a}_1, \ldots, \mathbf{a}_m$, and knapsack target $\mathbf{b}$, we first compute an arbitrary solution $\mathbf{z} = (\mathbf{z}_1, \ldots, \mathbf{z}_m)$ to the equation $\sum \mathbf{a}_i \otimes \mathbf{z}_i = \mathbf{b}$. (These vectors $\mathbf{z}_i$ are not required to belong to $S = D^n$, and can be efficiently found.) Then, finding small vectors $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_m)$ such that $\sum \mathbf{a}_i \otimes \mathbf{x}_i = \mathbf{b}$ is equivalent to finding lattice vectors $(\mathbf{x}_1 - \mathbf{z}_1, \ldots, \mathbf{x}_m - \mathbf{z}_m) \in \Lambda(\mathbf{A})$ close to $(\mathbf{z}_1, \ldots, \mathbf{z}_m)$.

So, our result can be interpreted as follows: if GDD on n-dimensional cyclic lattices is hard to approximate within $n^{1+\epsilon}$ factors in the *worst case*, then GDD on $\omega(n)$ dimensional $\omega(1)$-cyclic lattices is hard to solve on the *average*.

Cryptographic applications. From a practical point of view, it would be nice to prove that our function satisfies stronger security guarantees than one-wayness. In principle, one-way functions are known to be sufficient to build many other useful cryptographic primitives, like pseudo-random generators [18, 21], universal one-way hash functions [46], commitment schemes [45], digital signatures schemes [56], or private key encryption schemes [17]. However, these generic constructions are rather inefficient, so with their use most of the efficiency benefits of our compact knapsack function would be lost. We leave as an open problem the construction of provably secure pseudo-random generators, universal one-way hash functions, commitment schemes, digital signature schemes, or private key encryption schemes with efficiency comparable to our one-way function, and based on similar worst-case intractability assumptions. We remark that [24] showed that if the subset-sum function is one-way, then it is also a good pseudorandom generator or a universal one-way hash function (depending on whether it stretches or compresses the size of the input.) An interesting open problem is whether similar results can be proved for the generalized compact knapsack function.

Another interesting open problem is whether the generalized compact knapsack function is collision resistant. Collision resistant functions are a strong variant of one-way hash functions for which no construction based on arbitrary one-way functions is known. Still, [16, 40, 44] showed that under the assumption that SIVP is hard to approximate in the worst case within almost linear factors $\omega(n \log n)$, the generalized subset-sum function over $\mathbb{Z}_p^n$ is not only one-way, but also collision resistant. Unfortunately, technical differences between our proof and the one in [44] make it hard to establish the same result for the compact knapsack function. Proving or disproving that our generalized compact knapsack functions are collision resistant is left as an open problem.

Finally, and probably the hardest of the open problems concerning the cryptographic applicability of our techniques, is to build a public-key encryption scheme (or a trapdoor function) with efficiency and security guarantees similar to our compact knapsack function. Building *public-key* encryption schemes seems a much harder problem than building one-way functions or private key encryptions. Still, we believe that designing public-key encryption schemes with efficiency and security properties similar to our one-way function may not be so out of reach. We remark that the class of cyclic lattices used in this paper is related to (although different from) the class of "convolutional modular lattices" used by NTRU [22], commercial public-key cryptosystem based on lattices. Specifically, the lattices used by NTRU can be described as quasi-cyclic lattices of order 2, i.e., lattices that are invariant under cyclic shifts by 2 positions. Unfortunately, no proof of security is known for NTRU (even based on nontrivial *average-case* complexity assumptions). Still, based on the similarities between NTRU and other lattice based cryptosystems [37], we hope that, as Ajtai's one-way function [1] inspired the design of public-key cryptosystems [3, 53], our work will provide a starting point for the design of *efficient* and provably secure cryptosystems based on *cyclic* lattices. Proving the security of NTRU, or finding alternative ways to build public-key cryptosystems with efficiency and security properties similar to our one-way function is left as an open problem.

Improving the connection factor. The worst-case inapproximability factor for SIVP and GDD$^\rho$ required by our one-way function is $n^{1+\epsilon}$, for arbitrarily small $\epsilon > 0$. This is slightly worse than the

$\omega(n \log n) = n^{1+o(1)}$ factor required in [44] for the case of general lattices. An interesting open question is whether this $n^{1+\epsilon}$ factor can be improved. We remark that the worst-case problems solved by our reduction are somehow harder than SIVP and GDD^{ρ}. Our reduction allows to solve GIVP^{η} and GDD^{η} within almost linear factors, and then uses known relations between the smoothing parameter η and standard lattice parameters like λ_n and ρ. An interesting question is whether better relations between η, λ_n and ρ can be proved in the case of cyclic lattices.

For the case of GDD, we showed how to solve GDD^{λ_n} within almost linear factors $n^{1+\epsilon}$, and then used the inequality $\rho \geq \lambda_n/2$ to express our result in terms of GDD^{ρ}. Since ρ can be larger than λ_n by $\sqrt{n}/2$ (even for the case of cyclic lattices), our reduction may approximate GDD^{ρ} within factors much smaller than $n^{1+\epsilon}$, potentially as low as $n^{0.5+\epsilon}$, depending on the input lattice. We leave as an open problem to prove that the generalized compact knapsack function is as hard to invert as approximating GDD^{ρ} over cyclic lattices in the worst case within factors $\gamma(n) = n^{0.5+\epsilon}$.

References

[1] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the twenty-eighth annual ACM symposium on the theory of computing - STOC '96*, pages 99–108, Philadelphia, Pennsylvania, USA, May 1996. ACM.

[2] M. Ajtai. The shortest vector problem in l_2 is NP-hard for randomized reductions (extended abstract). In *Proceedings of the thirtieth annual ACM symposium on theory of computing - STOC '98*, pages 10–19, Dallas, Texas, USA, May 1998. ACM.

[3] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the twenty-ninth annual ACM symposium on theory of computing - STOC '97*, pages 284–293, El Paso, Texas, USA, May 1997. ACM.

[4] H. Amirazizi, E. Karnin, and J. Reyneri. Compact knapsacks are polynomially solvable. *ACM SIGACT News*, 15:20–22, 1983.

[5] S. Arora, L. Babai, J. Stern, and E. Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *Journal of Computer and System Sciences*, 54(2):317–331, Apr. 1997.

[6] L. Babai. On Lovasz' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.

[7] J. Blömer and J.-P. Seifert. On the complexity of computing short linearly independent vectors and short bases in a lattice. In *Proceedings of the thirty-first annual ACM symposium on theory of computing - STOC '99*, pages 711–720, Atlanta, Georgia, USA, May 1999. ACM.

[8] E. F. Brickell. Breaking iterated knapsacks. In G. R. Blakley and D. Chaum, editors, *Advances in cryptology - Proceedings of CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 342–358, Santa Barbara, California, USA, Aug. 1984. Springer-Verlag.

[9] J.-Y. Cai and A. P. Nerurkar. An improved worst-case to average-case connection for lattice problems (extended abstract). In *Proceedings of the 38th annual symposium on foundations of computer science - FOCS '97*, pages 468–477, Miami Beach, Florida, USA, Oct. 1997. IEEE.

[10] B. Chor and R. Rivest. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Transactions in Information Theory*, 34:901–909, 1988.

[11] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C.-P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. *Computational Complexity*, 2(2):111–128, 1992.

[12] T. W. Cusick. Cryptanalysis of a public key system based on Diophantine equations. *Information Processing Letters*, 56(2):73–75, Oct. 1995.

[13] I. Dinur, G. Kindler, R. Raz, and S. Safra. Approximating CVP to within almost-polynomial factors is NP-hard. *Combinatorica*, 23(2):205–243, 2003.

[14] U. Feige and D. Micciancio. The inapproximability of lattice and coding problems with preprocessing. *Journal of Computer and System Sciences*, 69(1):45–67, Aug. 2004.

[15] C. Gentry and M. Szydlo. Cryptanalysis of the revised NTRU signature scheme. In L. Knudsen, editor, *Advances in cryptology - EUROCRYPT 2002, Proceedings of the internarional conference on the theory and application of cryptographic techniques*, volume 2332 of *Lecture Notes in Computer Science*, pages 299–320, Amsterdam, The Netherlands, Apr. 2002. Springer-Verlag.

[16] O. Goldreich, S. Goldwasser, and S. Halevi. Collision-free hashing from lattice problems. Technical Report TR96-056, Electronic Colloquium on Computational Complexity (ECCC), 1996.

[17] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *Journal of the ACM*, 33:792–807, 1986.

[18] O. Goldreich and L. Levin. A hard predicate for all one-way functions. In *Proceedings of the twenty-first annual ACM symposium on the theory of computing - STOC '89*, Seattle, Washington, USA, May 1989. ACM.

[19] R. M. F. Goodman and A. J. McAuley. A new trapdoor knapsack public-key cryptosystem. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in cryptology - EUROCRYPT '84, Proceedings of a workshop on the theory and application of cryptographic techniques*, volume 209 of *Lecture Notes in Computer Science*, pages 150–158, Paris, France, Apr. 1984. Springer-Verlag.

[20] V. Guruswami and A. Vardy. Maximum-likelihood decoding of Reed-Solomon codes is NP-hard. In *Proceedings of the 16th annual ACM-SIAM symposium on discrete algorithms - SODA 2005*. ACM/SIAM, Jan. 2005. To appear.

[21] J. Hastad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[22] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: a ring based public key cryptosystem. In J. P. Buhler, editor, *Algorithmic number theory: Third international symposium - ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288, Portland, OR, USA, June 1998. Springer.

[23] N. Howgrave-Graham and M. Szydlo. A method to solve cyclotomic norm equations. In D. A. Buell, editor, *Algorithmic number theory: 6th international symposium - ANTS-VI*, volume 3076 of *Lecture Notes in Computer Science*, pages 272–279, Burlington, VT, USA, June 2004. Springer.

[24] R. Impagliazzo and M. Naor. Efficient cryptographic schemes provably as secure as subset sum. *Journal of Cryptology*, 9(4):199–216, 1996.

[25] R. Impagliazzo and D. Zuckerman. How to recycle random bits. In *Proceedings of the 30th annual symposium on foundations of computer science - FOCS '89*, pages 248–253, Reseach Triangle Park, NC, USA, Oct. 1989. IEEE.

[26] A. Joux and J. Stern. Cryptanalysis of another knapsack cryptosystem. In H. Imai, R.L. Rivest, and T. Matsumoto, editors, *Advances in cryptology – Proceedings Asiacrypt 1991*, volume 739 of *Lecture Notes in Computer Science*, pages 470–476. Springer-Verlag, 1993.

[27] A. Joux and J. Stern. Lattice reduction: A toolbox for the cryptanalyst. *Journal of Cryptology*, 11(3):161–185, 1998.

[28] R. M. Karp. Reducibility among combinatorial problems. In R. E. Miller and J. W. Thatcher, editors, *Complexity of computer computation*, pages 85–103. Plenum, 1972.

[29] S. Khot. Hardness of Approximating the Shortest Vector Problem in Lattices. In *Proceedings of the 45rd annual symposium on foundations of computer science - FOCS 2004*, pages 126–135, Rome, Italy, Oct. 2004. IEEE.

[30] J. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. *Journal of the ACM*, 32(1):229–246, Jan. 1985.

[31] M.-K. Lee and K. Park. Low-density attack of public-key cryptosystems based on compact knapsacks. *Journal of Electrical Engineering and Information Science*, 4(2):197–204, 1999.

[32] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:513–534, 1982.

[33] C. H. Lin, C. C. Chang, and R. C. T. Lee. A new public-key cipher system based upon the Diophantine equations. *IEEE Transactions on Computers*, 44(1):13–19, 1995.

[34] A. May and J. H. Silverman. Dimension reduction methods for convolution modular lattices. In J. Silverman, editor, *Cryptography and lattices conference – CaLC 2001*, volume 2146 of *Lecture Notes in Computer Science*, pages 110–125, Providence, RI, USA, Mar. 2001. Springer-Verlag.

[35] R. Merkle and M. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*, 24(5):525–530, Sept. 1978.

[36] D. Micciancio. The hardness of the closest vector problem with preprocessing. *IEEE Transactions on Information Theory*, 47(3):1212–1215, Mar. 2001.

[37] D. Micciancio. Improving lattice based cryptosystems using the Hermite normal form. In J. Silverman, editor, *Cryptography and lattices conference – CaLC 2001*, volume 2146 of *Lecture Notes in Computer Science*, pages 126–145, Providence, RI, USA, Mar. 2001. Springer-Verlag.

[38] D. Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. *SIAM Journal on Computing*, 30(6):2008–2035, Mar. 2001.

[39] D. Micciancio. Generalized compact knapsaks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In *Proceedings of the 43rd annual symposium on foundations of computer science - FOCS 2002*, pages 356–365, Vancouver, British Columbia, Canada, Nov. 2002. IEEE.

[40] D. Micciancio. Improved cryptographic hash functions with worst-case/average-case connection. In *Proceedings of the thirty-fourth annual ACM symposium on theory of computing - STOC 2002*, pages 609–618, Montréal, Québec, Canada, May 2002. ACM.

[41] D. Micciancio. A note on the minimal volume of almost cubic parallelepiped. *Discrete and Computational Geometry*, 29(1):133–138, Dec. 2002.

[42] D. Micciancio. Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor. *SIAM Journal on Computing*, 2004. To appear. Paper available from the author's web page http://www.cse.ucsd.edu/users/daniele. Preliminary version in STOC 2002.

[43] 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, Boston, Massachusetts, Mar. 2002.

[44] D. Micciancio and O. Regev. Worst-case to Average-case Reductions based on Gaussian Measure. In *Proceedings of the 45rd annual symposium on foundations of computer science - FOCS 2004*, pages 372–381, Rome, Italy, Nov. 2004. IEEE.

[45] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151–158, 1991.

[46] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the twenty-first annual ACM symposium on the theory of computing - STOC '89*, pages 33–43, Seattle, Washington, USA, May 1989. ACM.

[47] P. Nguyen and J. Stern. Merkle-Hellman revisited: A cryptanalysis of the Qu-Vanstone cryptosystem based on group factorizations. In B. S. Kaliski, Jr., editor, *Advances in cryptology - CRYPTO '97, Proceedings of the 17th annual international cryptology conference*, volume 1294 of *Lecture Notes in Computer Science*, pages 198–212, Santa Barbara, California, USA, Aug. 1997. Springer-Verlag.

[48] P. Nguyen and J. Stern. Cryptanalysis of the Ajtai-Dwork cryptosystem. In H. Krawczyk, editor, *Advances in cryptology - CRYPTO '98, Proceedings of the 18th annual international cryptology conference*, volume 1462 of *Lecture Notes in Computer Science*, pages 223–242, Santa Barbara, California, USA, Aug. 1998. Springer-Verlag.

[49] P. Nguyen and J. Stern. Lattice reduction in cryptology: an update. In W. Bosma, editor, *Algorithmic number theory: 4th international symposium - ANTS-IV*, volume 1838 of *Lecture Notes in Computer Science*, pages 85–112, Leiden, The Netherlands, July 2000. Springer.

[50] P. Nguyen and J. Stern. The two faces of lattices in cryptology. In J. Silverman, editor, *Cryptography and lattices conference – CaLC 2001*, volume 2146 of *Lecture Notes in Computer Science*, pages 146–180, Providence, RI, USA, Mar. 2001. Springer-Verlag.

[51] A. M. Odlyzko. The rise and fall of knapsack cryptosystems. In C. Pomerance, editor, *Cryptology and computational number theory*, volume 42 of *Procedings of Symposia in Applied Mathematics*, pages 75–88, Boulder, Colorado, 1989. AMS.

[52] G. Orton. A multiple-iterated trapdoor for dense compact knapsacks. In A. De Santis, editor, *Advances in cryptology - EUROCRYPT '94, Proceedings of a workshop on the theory and application of cryptographic techniques*, volume 950 of *Lecture Notes in Computer Science*, pages 112–130, Perugia, Italy, May 1994. Springer-Verlag.

[53] O. Regev. New lattice based cryptographic constructions. In *Proceedings of the thirty-fifth annual ACM symposium on theory of computing - STOC 2003*, pages 407–426, San Diego, CA, USA, June 2003. ACM.

[54] O. Regev. Improved inapproximability of lattice and coding problems with preprocessing. *IEEE Transactions on Information Theory*, 50(9):2031–2037, Sept. 2004.

[55] H. Ritter. Breaking knapsack cryptosystems by max-norm enumeration. In *First international conference of the theory and appications of cryptology - Pragocrypt 1996*, pages 480–492, 1996.

[56] J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of the twenty-second annual ACM symposium on the theory of computing - STOC '90*, pages 387–394, Baltimore, Maryland, USA, May 1990. ACM.

[57] C.-P. Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. In L. Budach, editor, *Proceedings of Fundamentals of Computation Theory*, volume 529 of *Lecture Notes in Computer Science*, pages 68–85. Springer-Verlag, 1991.

[58] C.-P. Schnorr and H. H. Hörner. Attacking the Chor–Rivest cryptosystem by improved lattice reduction. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in cryptology - EUROCRYPT '95, Proceedings of the international conference on the theory and application of cryptographic techniques*, volume 921 of *Lecture Notes in Computer Science*, pages 1–12, Saint-Malo, France, May 1995. Springer-Verlag.

[59] A. Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. *IEEE Transactions on Information Theory*, 30(5):699–704, Sept. 1984.

[60] M. Szydlo. Hypercubic lattice reduction and analysis of GGH and NTRU signatures. In E. Biham, editor, *Advances in cryptology - EUROCRYPT 2003, proceedings of the internarional conference on the theory and application of cryptographic techniques*, volume 2656 of *Lecture Notes in Computer Science*, pages 433–448, Warsaw, Poland, May 2003. Springer-Verlag.

[61] P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical Report 81-04, Mathematische Instituut, Universiry of Amsterdam, 1981. Available on-line at URL http://turing.wins.uva.nl/~peter/.