Generating Shorter Bases for Hard Random Lattices

Joël Alwen[*]
New York University

Chris Peikert [†]
Georgia Institute of Technology

June 25, 2009

Abstract

We revisit the problem of generating a 'hard' random lattice together with a basis of relatively short vectors. This problem has gained in importance lately due to new cryptographic schemes that use such a procedure to generate public/secret key pairs. In these applications, a shorter basis directly corresponds to milder underlying complexity assumptions and smaller key sizes.

The contributions of this work are twofold. First, we simplify and modularize an approach originally due to Ajtai (ICALP 1999). Second, we improve the construction and its analysis in several ways, most notably by making the output basis as short as possible (up to a small constant factor).

Keywords: Lattices, average-case hardness, cryptography, Hermite normal form

[*] Work performed while at SRI International.

[†] Much of this work was performed while at SRI International. This material is based upon work supported by the National Science Foundation under Grants CNS-0716786 and CNS-0749931. 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.

1 Introduction

A (point) *lattice* is a discrete additive subgroup of $\mathbb{R}^m$; alternatively, it is the set of all integer linear combinations of some linearly independent *basis* vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$. Lattices appear to be a rich source of computational hardness, and in recent years, *cryptographic* schemes based on lattices have emerged as a promising alternative to more traditional ones based on, e.g., the factoring and discrete logarithm problems. Among other reasons, this is because lattice-based schemes have yet to be broken by efficient quantum algorithms (cf. [Sho97]), and their security can often be based merely on *worst-case* computational assumptions (rather than *average-case* assumptions, which are the norm in cryptography).

In 1996, Ajtai's seminal work [Ajt04] in this area demonstrated a particular family of lattices for which (informally speaking) finding a short nonzero lattice vector in a randomly chosen lattice from the family is at least as hard as approximating some well-studied lattice problems in the *worst case*, i.e., for *any* lattice. This family of 'hard random lattices' has since been used as the foundation for several important cryptographic primitives, including one-way and collision-resistant hash functions, public-key encryption, digital signatures, and identity-based encryption (see, for example, [GGH96, MR07, Reg05, GPV08]).

Ajtai's initial work also showed how to generate a hard random lattice together with knowledge of one relatively short nonzero lattice vector. The short vector can be useful as secret information in cryptographic applications; examples include an identification scheme [MV03] and public-key cryptosystems [Reg05, GPV08]. Shortly after Ajtai's work, Goldreich, Goldwasser and Halevi [GGH97] proposed some public-key cryptographic schemes in which the secret key is an entire *short basis* of a public lattice, i.e., a basis in which all of the vectors are relatively short. Their method for generating a lattice along with a short basis is ad-hoc, and unfortunately does not produce lattices from the provably hard family defined in [Ajt04]. Although the algorithm and cryptosystem were later improved [Mic01] (following a cryptanalysis of the original scheme [Ngu99]), there is still no known proof that the induced random lattices are actually hard on the average. Therefore, the schemes from [GGH97] lack worst-case security proofs.[1]

Following the GGH proposal [GGH97], Ajtai demonstrated an entirely different method of generating a lattice together with a short basis [Ajt99]. His algorithm has the important property that the resulting lattice is drawn, under the appropriate distribution, from the hard family defined in [Ajt04]. Interestingly, the algorithm apparently went without application until recently, when Gentry, Peikert and Vaikuntanathan [GPV08] constructed several provably secure (under worst-case assumptions) cryptographic schemes that crucially use short bases as their secret keys; see also the subsequent works [PVW08, PV08, Pei09] for further applications. At this point we not that technically, the algorithm of [Ajt99] actually produces a *full-rank set* of short lattice vectors (not necessarily a basis), which nonetheless suffices for all the applications in question.

In the above applications, the 'quality' of the short basis directly affects the concrete security and efficiency of the schemes, both in theory and in practice. More precisely, the quality is measured by the maximal Euclidean length of the basis vectors, or alternatively of their *Gram-Schmidt orthogonalization* (shorter means higher quality). The quality determines the approximation factor in the underlying worst-case lattice assumptions, as well as the concrete dimensions and key sizes needed for security against real attacks (see Section 2.3 for details). Therefore, it is very desirable to generate a basis that is as short as possible. Unfortunately, the construction from [Ajt99] is far from optimal — the basis length is bounded by $m^{5/2}$, whereas the shortest possible basis has length about $\sqrt{m}$ (for commonly used parameters) — and the method seems not to have attracted much attention or improvement since its publication a decade ago (probably due to the lack of applications until recently).

[1] We should also mention that the digital signature scheme from [GGH97] has since been shown to be insecure *regardless* of the particular method used for generating lattices [NR06].

1.1 Our Contributions

Our first contribution is to elucidate and modularize Ajtai's basic approach for generating a hard random lattice along with a relatively short basis. We endeavor to give a 'top-down' exposition of the key aspects of the problem and the techniques used to address them (in the process, we also correct some minor errors in the original paper).

One novelty in our approach is to base the algorithm and its analysis around the concept of the *Hermite normal form* (HNF), which is an easily computable, unique canonical representation for (integer) lattices. Micciancio [Mic01] has proposed using the HNF in cryptographic applications to specify a lattice in its 'least revealing' representation; here we use the properties of the HNF to bound the dimension of the output lattice and the quality of the resulting basis.

Our second contribution is to refine the algorithm and its analysis, improving it in several ways. Most importantly, we improve the length of its output basis from $m^{5/2}$ to the asymptotically optimal $O(\sqrt{m})$, where m is the dimension of the output lattice (see Section 3 for precise statements of the new bounds). For the cryptographic schemes of, e.g., [GPV08], this immediately implies security under significantly milder worst-case assumptions: we need only that lattice problems are hard to approximate to within an $\tilde{O}(n^{3/2})$ factor, rather than $\tilde{O}(n^{7/2})$ as before.

We hasten to add that [GPV08, Section 5] briefly claims that Ajtai's algorithm can be improved to yield an $O(m^{1+\epsilon})$ bound on the basis length, but does not provide any further details. The focus of [GPV08] is on *applications* of a short basis, independent of the particular *generation* algorithm. The present work is a full exposition of an improved generation algorithm, and is meant to support and complement [GPV08] (and any other applications requiring a short basis).

1.2 Relation to Ajtai's Construction

Our construction is inspired by Ajtai's [Ajt99], but differs from it substantially in both the high-level structure and most of the details. The most significant similarity is a specially crafted unimodular matrix having small entries (called $\mathbf{B}$ in this work) that is used to generate vectors with 'exponentially large' entries.

Departing from the approach of [Ajt99], our construction is guided from the 'top down' by two main factors: the block structure of the short output basis, and the probability distribution of the output lattice. This approach illuminates the essential structure of the problem, and yields several technical simplifications. In particular, it lets us completely separate the *structural constraints* on the output lattice from its *randomization* (by contrast, in [Ajt99] the structure and randomization are tightly coupled).

2 Preliminaries

For a positive integer k, let $[k]$ denote the set $\{1, \ldots, k\}$; $[0]$ is the empty set. We denote the set of integers modulo an integer $q \geq 1$ by $\mathbb{Z}_q$, and identify it with the set of integer residues $\{0, \ldots, q-1\}$ in the natural way. Column vectors are named by lower-case bold letters (e.g., $\mathbf{x}$) and matrices by upper-case bold letters (e.g., $\mathbf{X}$). The ith entry of a vector $\mathbf{x}$ is denoted x_i, and the jth column of a matrix $\mathbf{X}$ is denoted $\mathbf{x}_j$. We identify a matrix $\mathbf{X}$ with the ordered set $\{\mathbf{x}_j\}$ of its column vectors, and define $\|\mathbf{X}\| = \max_j \|\mathbf{x}_j\|$. We let $\mathbf{e}_i$ denote the ith standard basis vector, where its dimension will be clear from context. The $d \times d$ identity matrix is denoted $\mathbf{I}_d$; we omit the dimension when it is clear from context.

For $\mathbf{X} \in \mathbb{R}^{n \times m}$ and $\mathbf{Y} \in \mathbb{R}^{n \times m'}$ having an equal number of rows, $[\mathbf{X}|\mathbf{Y}] \in \mathbb{R}^{n \times (m+m')}$ denotes the concatenation of the columns of $\mathbf{X}$ followed by the columns of $\mathbf{Y}$. Likewise, for $\mathbf{X} \in \mathbb{R}^{n \times m}$ and $\mathbf{Y} \in \mathbb{R}^{n' \times m}$

having an equal number of columns, $[\mathbf{X}; \mathbf{Y}] \in \mathbb{R}^{(n+n')\times m}$ is the concatenation of the rows of $\mathbf{X}$ and the rows of $\mathbf{Y}$.

We say that a function in n is *negligible*, written $\mathrm{negl}(n)$, if it vanishes faster than the inverse of any polynomial in n. We say that that a probability is *overwhelming* if it is $1 - \mathrm{negl}(n)$.

We denote the (Euclidean) unit ball in $\mathbb{R}^m$ by S^{m-1}, i.e., $S^{m-1} = \{\mathbf{x} \in \mathbb{R}^m \ : \ \|\mathbf{x}\| = 1\}$.

2.1 Matrix Decompositions

For an ordered set $\mathbf{S} = \{\mathbf{s}_1, \ldots, \mathbf{s}_m\} \subset \mathbb{R}^m$ of linearly independent vectors, the *Gram-Schmidt orthogonalization* $\widetilde{\mathbf{S}}$ of $\mathbf{S}$ is defined iteratively as follows: $\widetilde{\mathbf{s}_1} = \mathbf{s}_1$, and for $j = 2, \ldots, m$, $\widetilde{\mathbf{s}_j}$ is the component of $\mathbf{s}_j$ orthogonal to $\mathrm{span}(\mathbf{s}_1, \ldots, \mathbf{s}_{j-1})$, i.e., $\widetilde{\mathbf{s}_j} = \mathbf{s}_j - \sum_{i\in[j-1]} \widetilde{\mathbf{s}_i} \cdot \langle \mathbf{s}_j, \widetilde{\mathbf{s}_i}\rangle / \langle \widetilde{\mathbf{s}_i}, \widetilde{\mathbf{s}_i}\rangle$.

For a matrix $\mathbf{M} \in \mathbb{R}^{m\times n}$, a *singular value decomposition* is a factorization $\mathbf{M} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^{-1}$ where $\mathbf{U} \in \mathbb{R}^{m\times m}, \mathbf{V} \in \mathbb{R}^{n\times n}$ are orthogonal square matrices and $\mathbf{\Sigma} \in \mathbb{R}^{m\times n}$ is diagonal with nonnegative entries. The diagonal entries of $\mathbf{\Sigma}$ called the *singular values* of $\mathbf{M}$, and are unique up to order. By definition, it follows that the largest (respectively, smallest) singular value of $\mathbf{M}$ is the maximum (respectively, minimum) value of $\|\mathbf{M}\mathbf{x}\|$ over all $\mathbf{x} \in S^{n-1}$. Note also that the singular values of $\mathbf{M}$ and $\mathbf{M}^t$ are the same.

2.2 Probability

For two probability distributions D_1, D_2 (viewed as functions) over a finite set G, the statistical distance $\Delta(D_1, D_2)$ is defined to be $\frac{1}{2}\sum_{g\in G}|D_1(g) - D_2(g)|$. We say that a distribution D (or a random variable having distribution D) is ϵ-uniform if its statistical distance from the uniform distribution over G is at most ϵ.

Let $\mathcal{X}$ and $\mathcal{Y}$ be two finite domains. A family $\mathcal{H}$ of functions mapping $\mathcal{X}$ to $\mathcal{Y}$ is 2-*universal* if for all distinct $x, x' \in \mathcal{X}$, $\Pr_{h\leftarrow\mathcal{H}}[h(x) = h(x')] = 1/|\mathcal{Y}|$.

Lemma 2.1 (Simplified Leftover Hash Lemma [HILL99])**.** *Let $\mathcal{H}$ be a family of 2-universal hash functions from a domain $\mathcal{X}$ to range $\mathcal{Y}$. Then for $h \leftarrow \mathcal{H}$ and $X \leftarrow \mathcal{X}$ chosen uniformly and independently, $(h, h(X))$ is $\frac{1}{2}\sqrt{|\mathcal{Y}|/|\mathcal{X}|}$-uniform over $\mathcal{H} \times \mathcal{Y}$.*

We say that a random variable X is *subgaussian* of *parameter* $s > 0$ if $\Pr[|X| > t] \leq 2\exp(-t^2/s^2)$ for all $t \geq 0$. In particular, it is easy to check that a Bernoulli ± 1 random variable (or more generally, any bounded random variable) is subgaussian. Using the moment-generating function, it can also be shown that if $X_1, \ldots, X_k$ are independent subgaussian random variables of parameter s, and $\mathbf{a} \in \mathbb{R}^k$ is arbitrary, then $\sum_{i\in[k]} a_i X_i$ is subgaussian of parameter $s \cdot \|\mathbf{a}\|$.

The singular values of random matrices with independent entries are well-studied. We will use the following bound due to Litvak *et al.* [LPRTJ05] (somewhat tighter bounds are known, but this one is sufficient for our purposes).

Lemma 2.2 ([LPRTJ05])**.** *Let $\mathbf{X} \in \mathbb{R}^{m\times n}$ be a matrix whose entries are independent subgaussian random variables of parameter s. There exists a universal constant $C > 0$ such that the largest singular value of $\mathbf{X}$ is at most $C \cdot s \cdot (\sqrt{m} + \sqrt{n})$, except with probability $2^{-\Omega(m+n)}$.*

2.3 Lattices

Generally defined, a *lattice* Λ is a discrete additive subgroup of $\mathbb{R}^m$. In this work, we are concerned only with *full-rank integer* lattices, which are discrete additive subgroups of $\mathbb{Z}^m$ having finite index, i.e., the quotient group $\mathbb{Z}^m/\Lambda$ is finite. The determinant of Λ, denoted $\det(\Lambda)$, is the cardinality $|\mathbb{Z}^m/\Lambda|$ of this quotient group. Geometrically, the determinant is a measure of the 'sparsity' of the lattice.

A lattice $\Lambda \subseteq \mathbb{Z}^m$ can also be viewed as the set of all integer linear combinations of m linearly independent *basis* vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\} \subset \mathbb{Z}^m$:

$$\Lambda = \mathcal{L}(\mathbf{B}) = \left\{ \mathbf{Bc} = \sum_{i \in [m]} c_i \mathbf{b}_i \ : \ \mathbf{c} \in \mathbb{Z}^m \right\}.$$

A lattice has infinitely many bases (when $m \geq 2$), which are related to each other by unimodular transformations, i.e., $\mathbf{B}$ and $\mathbf{B}'$ generate the same lattice if and only if $\mathbf{B} = \mathbf{B}' \cdot \mathbf{U}$ for some unimodular $\mathbf{U} \in \mathbb{Z}^{m \times m}$. The determinant of any basis matrix $\mathbf{B}$ coincides with the determinant of the lattice it generates, up to sign: $|\det(\mathbf{B})| = \det(\mathcal{L}(\mathbf{B}))$.

Every lattice $\Lambda \subseteq \mathbb{Z}^m$ has a *unique* canonical basis $\mathbf{H} = \mathrm{HNF}(\Lambda) \in \mathbb{Z}^{m \times m}$ called its *Hermite normal form* (HNF). The matrix $\mathbf{H}$ is upper triangular and has non-negative entries (i.e., $h_{i,j} \geq 0$ with equality for $i > j$), has strictly positive diagonals (i.e., $h_{i,i} \geq 1$ for every i), and every entry above the diagonal is strictly smaller than the diagonal entry in its row (i.e., $h_{i,j} < h_{i,i}$ for $i < j$). Note that because $\mathbf{H}$ is upper triangular, its determinant is simply the product $\prod_{i \in [m]} h_{i,i} > 0$ of the diagonal entries. For a lattice basis $\mathbf{B}$, we write $\mathrm{HNF}(\mathbf{B})$ to denote $\mathrm{HNF}(\mathcal{L}(\mathbf{B}))$. Given an arbitrary basis $\mathbf{B}$, $\mathbf{H} = \mathrm{HNF}(\mathbf{B})$ can be computed in polynomial time (see [MW01] and references therein).

2.4 Hard Random Lattices

We will be especially concerned with a certain family of lattices in $\mathbb{Z}^m$ as defined by Ajtai [Ajt04]. A lattice from this family is most naturally specified not by a basis, but instead by a *parity check* matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ for some positive integer n and positive integer modulus q. (We discuss the parameters n, q, and m in detail below). The associated lattice is defined as

$$\Lambda^{\perp}(\mathbf{A}) = \left\{ \mathbf{x} \in \mathbb{Z}^m \ : \ \mathbf{Ax} = \sum_{j \in [m]} x_j \cdot \mathbf{a}_j = \mathbf{0} \in \mathbb{Z}_q^n \right\} \subseteq \mathbb{Z}^m.$$

It is routine to check that $\Lambda^{\perp}(\mathbf{A})$ contains the identity $\mathbf{0} \in \mathbb{Z}^m$ and is closed under addition, hence it is a subgroup of (and lattice in) $\mathbb{Z}^m$. Also observe that $\Lambda^{\perp}(\mathbf{A})$ is 'q-ary,' that is, $q \cdot \mathbb{Z}^m \subseteq \Lambda^{\perp}(\mathbf{A})$ for every $\mathbf{A}$, so membership in $\Lambda^{\perp}(\mathbf{A})$ is determined solely modulo q.

2.4.1 Hermite normal form

Let $\mathbf{H} \in \mathbb{Z}^{m \times m}$ be the Hermite normal form of a lattice $\Lambda = \Lambda^{\perp}(\mathbf{A})$ for some arbitrary parity check matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$. Given $\mathbf{A}$, the matrix $\mathbf{H}$ may be computed efficiently (e.g., by first computing a basis of Λ). In one of our constructions, we use the fact that every diagonal entry of $\mathbf{H}$ is at most q, which we now prove.

We can determine $\mathbf{H}$ as follows. Starting with the first column $\mathbf{h}_1 = h_{1,1} \cdot \mathbf{e}_1 \in \Lambda$, it must be the case that

$$\mathbf{A} \cdot \mathbf{h}_1 = h_{1,1} \cdot \mathbf{a}_1 = \mathbf{0} \in \mathbb{Z}_q^n.$$

Let $k \leq q$ be the smallest positive integer solution to $k \cdot \mathbf{a}_1 = \mathbf{0} \in \mathbb{Z}_q^n$. Then $k \cdot \mathbf{e}_1 \in \Lambda$, so we must be able to write $k \cdot \mathbf{e}_1 = \mathbf{Hz}$ for some $\mathbf{z} \in \mathbb{Z}^m$. Now because every diagonal $h_{i,i} > 0$ and $\mathbf{H}$ is upper triangular, it must be the case that $z_i = 0$ for all $i > 1$. This implies $z_1 \cdot h_{1,1} = k$, and because $0 < k \leq h_{1,1}$, we must have $z_1 = 1$ and thus $h_{1,1} = k \leq q$.

More generally, suppose that $\mathbf{h}_1, \ldots, \mathbf{h}_{j-1}$ are determined for some $j \in [m]$. Then by similar reasoning as above, $\mathbf{h}_j \in \mathbb{Z}^m$ is given by the unique solution to the equation

$$h_{j,j} \cdot \mathbf{a}_j + \sum_{i \in [j-1]} h_{i,j} \cdot \mathbf{a}_i = \mathbf{0} \in \mathbb{Z}_q^n$$

in which $h_{j,j} > 0$ is minimized and $0 \leq h_{i,j} < h_{i,i} \leq q$ for every $i < j$. In particular, $q \cdot \mathbf{e}_j$ is a solution to the above relation, hence $h_{j,j} \leq q$. We conclude by induction that every diagonal entry of $\mathbf{H}$ is at most q.

2.4.2 Geometric Facts

Let $\Lambda = \Lambda^{\perp}(\mathbf{A})$ for some arbitrary $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. First, we have $\det(\Lambda) \leq q^n$, by the following argument: let $\phi : (\mathbb{Z}^m/\Lambda) \to \mathbb{Z}_q^n$ be the homomorphism mapping the residue class $(\mathbf{x}+\Lambda)$ to $\mathbf{A}\mathbf{x} \in \mathbb{Z}_q^n$. Then ϕ is injective, because if $\phi(\mathbf{x} + \Lambda) = \phi(\mathbf{x}' + \Lambda)$ for some $\mathbf{x}, \mathbf{x}' \in \mathbb{Z}^m$, we have $\mathbf{A}(\mathbf{x} - \mathbf{x}') = \mathbf{0}$ which implies $\mathbf{x} - \mathbf{x}' \in \Lambda$, i.e., $\mathbf{x} = \mathbf{x}' \bmod \Lambda$. Therefore, there are at most $|\mathbb{Z}_q^n| = q^n$ residue classes in $\mathbb{Z}^m/\Lambda$. Minkowski's first inequality states that the minimum distance of Λ (i.e., the length of a shortest nonzero lattice vector) is at most

$$\sqrt{m} \cdot \det(\Lambda)^{1/m} \leq \sqrt{m} \cdot q^{n/m}. \tag{2.1}$$

For reasons motivated by Proposition 2.3 below, the family of lattices under discussion is most naturally parameterized by n (even though m is the lattice dimension), and the parameters $q = q(n)$ and $m = m(n)$ are viewed as functions of n. Given n and $q = q(n)$, a typical choice of the parameter m, which essentially minimizes the bound in (2.1), is $m = c \cdot n \lg q$ for some constant $c \geq 1$. Then by (2.1), the minimum distance of $\Lambda^{\perp}(\mathbf{A})$ for any $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ is at most

$$\sqrt{m} \cdot q^{n/m} = \sqrt{m} \cdot q^{1/(c \lg q)} = \sqrt{m} \cdot 2^{1/c} = \Theta(\sqrt{n \lg q}).$$

For a *uniformly random* $\mathbf{A}$, a counting argument reveals that with high probability, the above bound is tight up to a small constant factor. Note that for larger choices of m, the typical minimum distance of $\Lambda^{\perp}(\mathbf{A})$ remains $\Theta(\sqrt{n \lg q})$, because we can simply ignore the extra columns of $\mathbf{A}$. See [MR09] for further discussion of the key parameters.

2.4.3 Average-Case Hardness

The following proposition, proved first by Ajtai [Ajt04] (in a quantitatively weaker form) and in its current form in [MR07, GPV08], relates the average-case and worst-case complexity of certain lattice problems.

Proposition 2.3. *For any $m = m(n), \beta = \beta(n) = \text{poly}(n)$ and any $q = q(n) \geq \beta \cdot \omega(\sqrt{n \log n})$, finding a nonzero $\mathbf{x} \in \Lambda^{\perp}(\mathbf{A})$ having length at most β for* uniformly random $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ *(with nonnegligible probability over the choice of $\mathbf{A}$ and the randomness of the algorithm) is at least as hard as solving (with overwhelming probability) the approximate shortest vector problem GapSVP (and other problems) on n-dimensional lattices to within a $\gamma(n) = \beta \cdot \tilde{O}(\sqrt{n})$ factor in the* worst case.

Note that Proposition 2.3 is meaningful only when β is at least the typical minimum distance of $\Lambda^{\perp}(\mathbf{A})$ for uniformly random $\mathbf{A}$. For $m = c \cdot n \lg q$ as described above above, we can therefore take β to be as small as $O(\sqrt{n \lg n})$, which yields a hard-on-average problem assuming the worst-case hardness of approximating GapSVP (and other problems) to within an $\tilde{O}(n)$ factor.

In certain cryptographic applications, however, an adversary that breaks a cryptographic scheme is guaranteed only to produce a lattice vector whose length is substantially more than the minimum distance, so one needs average-case hardness for larger values of β. For example, the secret key in the digital signature schemes of [GPV08] is a basis of $\Lambda^{\perp}(\mathbf{A})$ having some length L, and signatures are vectors of length $\approx L\sqrt{m}$. It is shown that a signature forger is able to find a nonzero lattice vector of length $\beta \approx L\sqrt{m}$ in $\Lambda^{\perp}(\mathbf{A})$, which by Proposition 2.3 (for our choice of m) is as hard as approximating GapSVP in the worst case to within $L \cdot \tilde{O}(n)$ factors. Therefore, using a shorter secret basis in the signature scheme has the immediate advantage of a weaker underlying hardness assumption.

Note also that Proposition 2.3 requires the modulus q to exceed β (otherwise $q \cdot \mathbf{e}_1$ would trivially be a valid solution), and that m grows with $\lg q$. Therefore, a polynomial factor improvement in the length L also yields a constant factor improvement in the dimension m and modulus q, which translates to a constant factor improvement in the size of the public key $\mathbf{A}$ (all other variables remaining the same).

3 Constructions

We give two algorithms for constructing a hard random lattice together with a relatively short basis. Strictly speaking, our two constructions are incomparable. The first is relatively simple and gives a guaranteed bound on the basis quality, but is slightly suboptimal in either the lattice dimension or basis length (or both). Our second construction is more involved and its bounds on the basis quality hold only with overwhelming probability, but it is simultaneously optimal (up to constant factors) in both the lattice dimension and (another measure of) quality. For technical reasons relating to the distribution of the output lattice, our second construction also needs an *odd* modulus q.[2]

Theorem 3.1. *Let $\delta > 0$ be any fixed constant. There is a probabilistic polynomial-time algorithm that, on input positive integers n (in unary), $q, r \geq 2$ (in binary), and $m \geq (1+\delta)(1+\lceil \lg_r q \rceil) \cdot n \lg q$ (in unary), outputs $(\mathbf{A} \in \mathbb{Z}_q^{n \times m}, \mathbf{S} \in \mathbb{Z}^{m \times m})$ such that:*

- *$\mathbf{A}$ is $(m \cdot q^{-\delta n/2})$-uniform over $\mathbb{Z}_q^{n \times m}$,*
- *$\mathbf{S}$ is a basis of $\Lambda^{\perp}(\mathbf{A})$, and*
- *$\|\mathbf{S}\| \leq 2r\sqrt{m}$.*

Setting $r = 2$ in the above theorem, the algorithm generates a basis of length $O(\sqrt{m}) = O(\sqrt{n \lg^2 q})$ for a random lattice having dimension $m = O(n \lg^2 q)$. These quantities are larger than our ultimate goal by $O(\sqrt{\lg q})$ and $O(\lg q)$ factors, respectively. Alternatively, if $q = \text{poly}(n)$, we may set $r = n^{\epsilon}$ for some small constant $\epsilon > 0$, which implies $\lg_r q = O(1)$. In this case, the algorithm generates a basis of only slightly suboptimal length $O(\sqrt{n^{1+2\epsilon} \lg q})$ for a random lattice having dimension $m = O(n \lg q)$.

Our next construction *simultaneously* optimizes the lattice dimension *and* basis quality, when the quality is measured according to the *Gram-Schmidt orthogonalization* of the basis. As explained in the introduction, this measure of quality is appropriate for all known applications.

Theorem 3.2. *Let $\delta > 0$ be any fixed constant. There is a probabilistic polynomial-time algorithm that, on input positive integers n (in unary),* odd *$q \geq 3$ (in binary), and $m \geq (5+3\delta) \cdot n \lg q$ (in unary), outputs $(\mathbf{A} \in \mathbb{Z}_q^{n \times m}, \mathbf{S} \in \mathbb{Z}^{m \times m})$ such that:*

- *$\mathbf{A}$ is $(m \cdot q^{-\delta n/2})$-uniform over $\mathbb{Z}_q^{n \times m}$,*

[2] This condition can be lifted by using a more sophisticated probability distribution in the randomization step, but the analysis becomes significantly more complicated.

$$n\left\{\left[\begin{array}{c:c} \mathbf{A}_1 & \mathbf{A}_2 \end{array}\right]\right. \times \begin{array}{c:cl} \mathbf{D} & \mathbf{V} & \}\, m_1 \\ \hdashline \mathbf{B} & \mathbf{P} & \}\, m_2 \\ \underbrace{\qquad}_{m_2} & \underbrace{\qquad}_{m_1} & \end{array} = \mathbf{0} \in \mathbb{Z}_q^{n\times m}, \qquad \begin{array}{cc} \underbrace{\qquad}_{m_1} & \underbrace{\qquad}_{m_2} \end{array}$$

Figure 1: Block structure of the equation $\mathbf{AS} = \mathbf{0} \in \mathbb{Z}_q^{n\times m}$.

- $\|\mathbf{S}\| \leq O(n \lg q)$ *with overwhelming probability, and*
- $\|\widetilde{\mathbf{S}}\| \leq O(\sqrt{n \lg q})$ *with overwhelming probability.*

3.1 Common Approach

Here we describe the common framework that underlies the two constructions from Theorems 3.1 and 3.2. (The particular details of each construction are given below in Sections 3.2 and 3.3, respectively.)

Let $m = m_1 + m_2$ for some sufficiently large dimensions m_1, m_2. Our algorithms start off with a uniformly random matrix $\mathbf{A}_1 \in \mathbb{Z}_q^{n\times m_1}$, then extend $\mathbf{A}_1$ into $\mathbf{A} = [\mathbf{A}_1|\mathbf{A}_2] \in \mathbb{Z}_q^{n\times m}$ by together generating $\mathbf{A}_2 \in \mathbb{Z}_q^{n\times m_2}$ with some short basis $\mathbf{S} \in \mathbb{Z}^{m\times m}$ of $\Lambda^\perp(\mathbf{A})$.

First consider the requirement that $\mathbf{S} \subset \Lambda^\perp(\mathbf{A})$, i.e., $\mathbf{AS} = \mathbf{0} \in \mathbb{Z}_q^{n\times m}$. We decompose $\mathbf{S}$ as a block matrix in the natural way, as depicted in Figure 1. We then need to construct integer matrices $\mathbf{D}, \mathbf{B}, \mathbf{V}, \mathbf{P}$ to satisfy the constraints

$$\mathbf{A}_1\mathbf{D} + \mathbf{A}_2\mathbf{B} = \mathbf{0} \in \mathbb{Z}_q^{n\times m_2} \qquad (3.1)$$
$$\mathbf{A}_1\mathbf{V} + \mathbf{A}_2\mathbf{P} = \mathbf{0} \in \mathbb{Z}_q^{n\times m_1}. \qquad (3.2)$$

For convenience, we additionally require that $\mathbf{B} \in \mathbb{Z}^{m_2\times m_2}$ be *unimodular*, so that $\mathbf{B}^{-1} \in \mathbb{Z}^{m_2\times m_2}$ exists. Rearranging Equation (3.1) and substituting for $\mathbf{A}_2$ in Equation (3.2), we may rewrite the constraints equivalently as

$$\mathbf{A}_2 = -\mathbf{A}_1 \cdot (\mathbf{DB}^{-1}) \in \mathbb{Z}_q^{n\times m_2} \qquad (3.3)$$
$$\mathbf{A}_1 \cdot (\mathbf{V} - \mathbf{DB}^{-1}\mathbf{P}) = \mathbf{0} \in \mathbb{Z}_q^{n\times m_1}. \qquad (3.4)$$

Put another way, Equation (3.4) asks that $\mathbf{V} - \mathbf{DB}^{-1}\mathbf{P} \subset \Lambda^\perp(\mathbf{A}_1)$. Looking forward, we will see that $\mathbf{S}$ is a *basis* of $\Lambda^\perp(\mathbf{A})$ if and only if $\mathbf{V} - \mathbf{DB}^{-1}\mathbf{P}$ is a basis of $\Lambda^\perp(\mathbf{A}_1)$, so we aim to satisfy that stronger condition as well.

Note the common term $\mathbf{DB}^{-1}$ appearing in both Equation (3.3) and (3.4). For Equation (3.3), our primary goal is to ensure that $\mathbf{A}_2$ is nearly uniform (even given $\mathbf{A}_1$); this means that $\mathbf{DB}^{-1}$ should be 'sufficiently random.' For Equation (3.4), our task is to construct short $\mathbf{V}$ and $\mathbf{P}$ so that $\mathbf{V} - (\mathbf{DB}^{-1})\mathbf{P}$ is a basis of the given lattice $\Lambda^\perp(\mathbf{A}_1)$; for this we somehow need $\mathbf{DB}^{-1}$ to be 'sufficiently structured.' To resolve these conflicting goals, we write $\mathbf{DB}^{-1}$ as the sum of two components:

$$\mathbf{DB}^{-1} = \mathbf{R} + \mathbf{G} \quad \iff \quad \mathbf{D} = (\mathbf{R} + \mathbf{G})\mathbf{B},$$

where $\mathbf{R}$ is a short 'random' matrix that should induce a suitable distribution of $\mathbf{A}_2$ via Equation (3.3), and $\mathbf{G}$ is a deterministic 'structured' matrix (having large entries) that should make it easy to satisfy Equation (3.4). Of course, we also need $\mathbf{D}$ to be short because it is a component of $\mathbf{S}$, so we want $\mathbf{GB}$ to be short as well. (Note that $\mathbf{RB}$ is automatically short, because both $\mathbf{R}$ and $\mathbf{B}$ are.)

The bulk of the effort in our constructions is devoted to satisfying Equation (3.4). Let $\mathbf{H} \in \mathbb{Z}^{m_1 \times m_1}$ be an easily computable basis of $\Lambda^{\perp}(\mathbf{A}_1)$; the Hermite normal form will be convenient in our particular constructions. We design the structured matrix $\mathbf{G}$ together with a short matrix $\mathbf{P}$ so that $\mathbf{GP} = \mathbf{H} - \mathbf{I}$, and let $\mathbf{V} = \mathbf{RP} - \mathbf{I}$. Then

$$\mathbf{V} - \mathbf{D}\mathbf{B}^{-1}\mathbf{P} = (\mathbf{RP} - \mathbf{I}) - (\mathbf{R} + \mathbf{G})\mathbf{P} = -(\mathbf{GP} + \mathbf{I}) = -\mathbf{H},$$

which is a basis of $\Lambda^{\perp}(\mathbf{A}_1)$, as desired.[3] Note also that $\mathbf{V} = \mathbf{RP} - \mathbf{I}$ is short, because $\mathbf{R}$ and $\mathbf{P}$ are.

Finally, let us verify that $\mathbf{S}$ is indeed a *basis* of $\Lambda^{\perp}(\mathbf{A})$. Using the formula for the determinant of a block matrix, we have

$$|\det(\mathbf{S})| = |\det(\mathbf{V} - \mathbf{D}\mathbf{B}^{-1}\mathbf{P})| = |\det(\mathbf{H})|.$$

Observe that the additive subgroup $\mathbb{G} \subseteq \mathbb{Z}_q^n$ generated by the columns of $\mathbf{A}_1$ is exactly the subgroup generated by the columns of $\mathbf{A}$, because the columns of $\mathbf{A}_2$ are in $\mathbb{G}$ by construction. Therefore,

$$\det(\Lambda^{\perp}(\mathbf{A})) = |\mathbb{G}| = \det(\Lambda^{\perp}(\mathbf{A}_1)) = |\det(\mathbf{H})| = |\det(\mathbf{V} - \mathbf{D}\mathbf{B}^{-1}\mathbf{P})| = |\det(\mathbf{S})|,$$

which means that $\mathbf{S}$ is a basis of $\Lambda^{\perp}(\mathbf{A})$, as desired. (Note that if $\mathbf{H}$ is *not* a basis of $\Lambda^{\perp}(\mathbf{A}_1)$, then the middle equality above becomes an inequality, and $\mathbf{S}$ is no longer a basis of $\Lambda^{\perp}(\mathbf{A})$.)

Our general framework is represented in Algorithm 1. By the above discussion, the reader may verify that for any input $\mathbf{A}_1$ and any Step 2 fulfilling the stated hypotheses, the output condition is satisfied, namely, that $\mathbf{S}$ is a basis of $\Lambda^{\perp}(\mathbf{A})$. The remainder of the paper is dedicated to implementing Step 2, and to analyzing the distribution of $\mathbf{A}$ and the quality of $\mathbf{S}$ for the particular constructions.

Algorithm 1 Framework for constructing $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and basis $\mathbf{S}$ of $\Lambda^{\perp}(\mathbf{A})$.

```
Input: $\mathbf{A}_1 \in \mathbb{Z}_q^{n \times m_1}$ and dimension $m_2$ (in unary).
Output: $\mathbf{A}_2 \in \mathbb{Z}_q^{n \times m_2}$ and basis $\mathbf{S}$ of $\Lambda^{\perp}(\mathbf{A})$, where $\mathbf{A} = [\mathbf{A}_1 | \mathbf{A}_2] \in \mathbb{Z}_q^{n \times m}$ for $m = m_1 + m_2$.
 1: compute the Hermite normal form $\mathbf{H} \in \mathbb{Z}^{m_1 \times m_1}$ of $\Lambda^{\perp}(\mathbf{A}_1)$.
 2: generate $\mathbf{B} \in \mathbb{Z}^{m_2 \times m_2}$; $\mathbf{R}, \mathbf{G} \in \mathbb{Z}^{m_1 \times m_2}$; $\mathbf{P} \in \mathbb{Z}^{m_2 \times m_1}$ (e.g., as described in Section 3.2 or 3.3) so that
    $\mathbf{B}$ is unimodular and $\mathbf{GP} = \mathbf{H}' = \mathbf{H} - \mathbf{I}$.
 3: let $\mathbf{D} = (\mathbf{R} + \mathbf{G}) \cdot \mathbf{B} \in \mathbb{Z}^{m_1 \times m_2}$.
 4: let $\mathbf{V} = \mathbf{RP} - \mathbf{I} \in \mathbb{Z}^{m_1 \times m_1}$.
 5: let $\mathbf{A}_2 = -\mathbf{A}_1 \cdot (\mathbf{R} + \mathbf{G}) \in \mathbb{Z}_q^{n \times m_2}$.
 6: return $\mathbf{A}_2$ and block matrix $\mathbf{S} = [\mathbf{D} | \mathbf{V}; \mathbf{B} | \mathbf{P}] \in \mathbb{Z}^{m \times m}$ as depicted in Figure 1.
```

3.2 First Construction

We begin with a relatively simple instantiation of Step 2 in Algorithm 1. Its properties are summarized in the following lemma, of which Theorem 3.1 is an immediate corollary.

[3] The $-\mathbf{I}$ terms in the expressions of $\mathbf{GP}$ and $\mathbf{V}$ is not strictly necessary, but it will be convenient for the particular constructions.

Lemma 3.3. *Let $\delta > 0$ be any fixed constant. There is a probabilistic polynomial-time algorithm that, given uniformly random $\mathbf{A}_1 \in \mathbb{Z}_q^{n \times m_1}$ for any $m_1 \geq d = (1+\delta) n \lg q$, an integer $r \geq 2$, and any integer $m_2 \geq m_1 \cdot \ell$ (in unary) where $\ell = \lceil \log_r q \rceil$, outputs matrices $\mathbf{B}, \mathbf{R}, \mathbf{G}, \mathbf{P}$ as required by Step 2 of Algorithm 1 such that:*

- $\mathbf{A} = [\mathbf{A}_1 | \mathbf{A}_2]$ *is $(m_2 \cdot q^{-\delta n/2})$-uniform, where $\mathbf{A}_2$ is as in Step 5 of Algorithm 1.*
- $\|\mathbf{S}\| \leq 2r\sqrt{m_1 + 1}$*, where $\mathbf{S}$ is as in Step 6 of Algorithm 1.*

The remainder of this subsection consists of the proof of Lemma 3.3.

3.2.1 Construction

Given $\mathbf{A}_1$, let $\mathbf{H} \in \mathbb{Z}^{m_1 \times m_1}$ be the Hermite normal form of $\Lambda^\perp(\mathbf{A}_1)$. The basic idea of the construction is that $\mathbf{G}$ itself contains the m_1 columns of $\mathbf{H}' = \mathbf{H} - \mathbf{I}$ (among many others), and $\mathbf{P}$ simply selects those columns to yield $\mathbf{GP} = \mathbf{H}'$. To ensure a short unimodular $\mathbf{B}$ such that $\mathbf{GB}$ is also short, we include additional columns in $\mathbf{G}$ that increase geometrically (with base r) to the desired columns of $\mathbf{H}'$; this is the reason for the extra $\ell = \log_r q$ factor in the dimension m_2.

Definition of G. Write

$$\mathbf{G} = \left[\mathbf{G}^{(1)} | \cdots | \mathbf{G}^{(m_1)} | \mathbf{0} \right] \in \mathbb{Z}^{m_1 \times m_2}$$

as a block matrix consisting of m_1 blocks $\mathbf{G}^{(i)}$ having ℓ columns each, and a final zero block consisting of the remaining $m_2 - m_1 \cdot \ell$ columns (if any). As per our usual notation, $\mathbf{g}_j^{(i)}$ and $\mathbf{h}'_j$ denote the jth columns of $\mathbf{G}^{(i)}$ and $\mathbf{H}'$, respectively. For each $i \in [m_1]$, $\mathbf{G}^{(i)}$ is defined as follows: let $\mathbf{g}_\ell^{(i)} = \mathbf{h}'_i$, and for each $j = \ell - 1, \ldots, 1$, let

$$\mathbf{g}_j^{(i)} = \lfloor \mathbf{g}_{j+1}^{(i)} / r \rfloor = \lfloor \mathbf{h}'_i / r^{\ell - j} \rfloor,$$

where the division and floor operations are coordinate-wise.

Note that because all the entries of $\mathbf{h}'_i$ are less than $q \leq r^\ell$, all the entries of $\mathbf{g}_1^{(i)}$ are in the range $[0, r-1]$.

Definition of P. For each $j \in [m_1]$, let $\mathbf{p}_j = \mathbf{e}_{j\ell} \in \mathbb{Z}^{m_2}$, the $(j\ell)$th standard basis vector. Observe that the ith column of $\mathbf{P}$ simply selects the rightmost column of $\mathbf{G}^{(i)}$, yielding $\mathbf{GP} = \mathbf{H}'$, as desired. Clearly, $\|\mathbf{p}_j\|^2 = 1$ for all $j \in [m_1]$.

Definition of B. Define the unimodular upper-triangular matrix $\mathbf{T}_\ell \in \mathbb{Z}^{\ell \times \ell}$ to have diagonal entries equal to 1 (i.e., $t_{i,i} = 1$ for every $i \in [\ell]$), upper diagonal entries equal to $-r$ (i.e, $t_{i,i+1} = -r$ for every $i \in [\ell - 1]$), and zero entries elsewhere. Define $\mathbf{B} \in \mathbb{Z}^{m_2 \times m_2}$ to be the block-diagonal matrix

$$\mathbf{B} = \text{diag}(\mathbf{T}_\ell, \ldots, \mathbf{T}_\ell, \mathbf{0})$$

consisting of m_1 blocks $\mathbf{T}_\ell$, followed by the square zero matrix of dimension $m_2 - m_1 \cdot \ell$.

Note that $\mathbf{B}$ is unimodular and that $\|\mathbf{b}_j\|^2 \leq r^2 + 1$ for all j. Also observe that

$$\mathbf{GB} = \left[\mathbf{G}^{(1)} \cdot \mathbf{T}_\ell | \cdots | \mathbf{G}^{(m_1)} \cdot \mathbf{T}_\ell | \mathbf{0} \right].$$

We claim that all the entries of each block $\mathbf{F}^{(i)} = \mathbf{G}^{(i)} \cdot \mathbf{T}_\ell$ are integers in the range $[0, r-1]$, and thus $\|\mathbf{f}_j^{(i)}\|^2 \leq m_1 \cdot (r-1)^2$. First observe that the claim is true for $\mathbf{f}_1^{(i)} = \mathbf{g}_1^{(i)}$, as explained above. Moreover, for each $j \in [\ell - 1]$ we have

$$\mathbf{f}_{j+1}^{(i)} = \mathbf{g}_{j+1}^{(i)} - r \cdot \mathbf{g}_j^{(i)} = \mathbf{g}_{j+1}^{(i)} - r \cdot \lfloor \mathbf{g}_{j+1}^{(i)}/r \rfloor,$$

which establishes the claim.

Definition of R. Let $\mathbb{D} = \{0,1\}^d \times \{0\}^{m_1 - d}$ (recall that $d = (1+\delta)n \lg q$). Each column $\mathbf{r}_j$ of $\mathbf{R}$ is chosen uniformly and independently from $\mathbb{D}$. In other words, all but the first d rows of $\mathbf{R}$ are zero, and the remaining entries are independent unbiased 0-1 random variables. Observe that $\|\mathbf{r}_j\|^2 \leq d$ for all j.

3.2.2 Distribution of A

We now show that for uniformly random $\mathbf{A}_1 \in \mathbb{Z}_q^{n \times m_1}$, the distribution of $\mathbf{R}$ ensures that $\mathbf{A} = [\mathbf{A}_1 | \mathbf{A}_2]$ is close to uniformly distributed over $\mathbb{Z}_q^{n \times m}$. We first claim that $\{h_{\mathbf{A}_1} : h_{\mathbf{A}_1}(\mathbf{r}) = \mathbf{A}_1 \mathbf{r} \in \mathbb{Z}_q^n\}$ is a family of 2-universal hash functions from domain $\mathbb{D}$ to range $\mathbb{Z}_q^n$. To see this, note that for any fixed distinct $\mathbf{r}, \mathbf{r}' \in \mathbb{D}$, we have $\mathbf{A}_1\mathbf{r} = \mathbf{A}_1\mathbf{r}'$ if and only if $\mathbf{A}_1(\mathbf{r} - \mathbf{r}') = \mathbf{0} \in \mathbb{Z}_q^n$. Furthermore, $\mathbf{0} \neq \mathbf{r} - \mathbf{r}' \in \{0, \pm 1\}^d \times \{0\}^{m_1 - d}$. Suppose that $\mathbf{r}$ and $\mathbf{r}'$ differ in entry $i \in [d]$. Then we have

$$\Pr_{\mathbf{A}_1}[\mathbf{A}_1(\mathbf{r} - \mathbf{r}') = \mathbf{0}] = 1/|\mathbb{Z}_q^n| = q^{-n},$$

by averaging over each fixed choice of all but the ith column of $\mathbf{A}_1$.

Now because $d = (1+\delta)n \log q$, Lemma 2.1 and the triangle inequality imply that $[\mathbf{A}_1 | \mathbf{A}_1 \cdot \mathbf{R}]$ is $(m_2 \cdot q^{-\delta n/2})$-uniform over $\mathbb{Z}_q^{n \times m}$. It follows that $\mathbf{A} = [\mathbf{A}_1 | -\mathbf{A}_1 \cdot (\mathbf{R} + \mathbf{G})]$ is as well.

3.2.3 Quality of S

We now analyze the length of the basis matrix $\mathbf{S}$. By the triangle inequality and Pythagorean theorem,

$$\|\mathbf{S}\| \leq \max\{\|\mathbf{D}\| + \|\mathbf{B}\|, \sqrt{\|\mathbf{V}\|^2 + \|\mathbf{P}\|^2}\}.$$

We have $\|\mathbf{P}\|^2 = 1$ and $\|\mathbf{V}\|^2 \leq m_1$, because each entry of $\mathbf{V} = \mathbf{RP} - \mathbf{I}$ has magnitude at most 1. Next, we have $\|\mathbf{B}\| \leq \sqrt{r^2 + 1} \leq r + 1$. For $\mathbf{D} = \mathbf{RB} + \mathbf{GB}$, we have

$$\|\mathbf{RB}\| \leq (r+1)\sqrt{d} \leq (r+1)\sqrt{m_1 + 1} \quad \text{and} \quad \|\mathbf{GB}\| \leq (r-1)\sqrt{m_1 + 1}.$$

Combining everything together, we have $\|\mathbf{S}\| \leq 2r\sqrt{m_1 + 1}$, as claimed.

3.3 Second Construction

Theorem 3.2 is an immediate corollary of the following lemma.

Lemma 3.4. *Let $\delta > 0$ be any fixed constant. There is a universal constant $C > 0$ and a probabilistic polynomial-time algorithm that, given uniformly random $\mathbf{A}_1 \in \mathbb{Z}_q^{n \times m_1}$ for any $m_1 \geq d = (1+\delta)n \lg q$, and any integer $m_2 \geq (4 + 2\delta)n \lg q$ (in unary), outputs matrices $\mathbf{B}, \mathbf{R}, \mathbf{G}, \mathbf{P}$ as required by Step 2 of Algorithm 1 such that:*

- $\mathbf{A} = [\mathbf{A}_1 | \mathbf{A}_2]$ *is $(m_2 \cdot q^{-\delta n/2})$-uniform, where $\mathbf{A}_2$ is as in Step 5 of Algorithm 1.*

- $\|\mathbf{S}\| \leq Cn \lg q$ *with probability* $1 - 2^{-\Omega(n)}$ *over the choice of* $\mathbf{R}$*, where* $\mathbf{S}$ *is as in Step 6 of Algorithm 1.*
- $\|\widetilde{\mathbf{S}}\| \leq 1 + C\sqrt{d} = O(\sqrt{n \lg q})$ *with probability* $1 - 2^{-\Omega(n)}$ *over the choice of* $\mathbf{R}$.

We have not attempted to optimize the exact constant C appearing in the above bounds, but it is not exceedingly large; certainly $C = 20$ is a valid choice. The remainder of this subsection is devoted to proving the lemma.

3.3.1 Construction

The basic idea behind the construction is to ensure that the columns of $\mathbf{G}$ include sufficiently many power-of-2 multiples of each standard basis vector $\mathbf{e}_i \in \mathbb{Z}^{m_1}$. This allows us to express each vector in the (modified) Hermite normal form $\mathbf{H}'$ as a simple binary combination of such vectors. To obtain a good bound on the length of the Gram-Schmidt orthogonalization $\widetilde{\mathbf{S}}$, we additionally ensure that certain rows of $\mathbf{G}$ are mutually orthogonal and sufficiently long. This ensures that adding the random matrix $\mathbf{R}$ to $\mathbf{G}$ does not 'distort the shape' of $\mathbf{G}$ by much, which turns out to be an important property in the analysis.

Given $\mathbf{A}_1$, let $\mathbf{H} \in \mathbb{Z}^{m_1 \times m_1}$ be the Hermite normal form of $\Lambda^{\perp}(\mathbf{A}_1)$. Recall that every diagonal entry $h_{i,i}$ is at least 1, that

$$\prod_{i \in [m_1]} h_{i,i} = \det(\mathbf{H}) = \det(\Lambda^{\perp}(\mathbf{A}_1)) \leq q^n,$$

and that $0 \leq h_{i,j} < h_{i,i}$ for every $j \neq i$. Therefore, every column $\mathbf{h}'_j$ of $\mathbf{H}' = \mathbf{H} - \mathbf{I}$ belongs to the Cartesian product

$$C = \prod_{i \in [m_1]} [0, \ldots, h_{i,i} - 1] \subset \mathbb{Z}^{m_1},$$

which has size $\prod_{i \in [m_1]} h_{i,i} \leq q^n$.

Definition of G. Write

$$\mathbf{G} = \left[\mathbf{G}^{(1)} | \cdots | \mathbf{G}^{(m_1)} | \mathbf{M} | \mathbf{0}\right] \in \mathbb{Z}^{m_1 \times m_2}$$

as a block matrix of m_1 blocks $\mathbf{G}^{(i)}$ having various widths, followed by a special block $\mathbf{M}$, followed by a zero block of any remaining columns. For each $i \in [m_1]$, block $\mathbf{G}^{(i)}$ has width $w_i = \lceil \lg h_{i,i} \rceil < 1 + \lg h_{i,i}$, and its jth column is $\mathbf{g}_j^{(i)} = 2^{k-1} \cdot \mathbf{e}_i \in \mathbb{Z}^{m_1}$. Note that if $h_{i,i} = 1$, block $\mathbf{G}^{(i)}$ actually has width 0, and that there are at most $n \lg q$ values of i for which $h_{i,i} > 1$. Taking all blocks $\mathbf{G}^{(i)}$ together, the total number of columns is therefore

$$\sum_{i \in [m_1]} w_i \leq n \lg q + \sum_{i \in [m_1]} \lg h_{i,i} \leq 2n \lg q.$$

The block $\mathbf{M}$ is a special component needed only for the analysis of $\|\widetilde{\mathbf{S}}\|$ (the bound on the length $\|\mathbf{S}\|$ from Lemma 3.4 holds even if $\mathbf{M}$ is not included). It has width w, where w is the largest power of 2 in the range $[d, m_2 - 2n \lg q]$. Note that $m_2 - 2n \lg q \geq 2d$, so a power of 2 always exists in the given range, and that $w \geq m_2/2 - n \lg q \geq m_2/4$. Block $\mathbf{M}$ is zero in all but its first d rows, which are a C' multiple (for some suitably large constant $C' > 0$) of d distinct rows taken from a square *Hadamard* matrix of dimension w. (Recall that a Hadamard matrix is a square ± 1 matrix whose rows are mutually orthogonal. Moreover, a Hadamard matrix in any power-of-2 dimension may be constructed efficiently using a simple recursive procedure originally due to Sylvester.)

Definition of $\mathbf{P}$. Mirroring the structure of $\mathbf{G}$, we write

$$\mathbf{P} = \left[\mathbf{P}^{(1)}; \cdots; \mathbf{P}^{(m_1)}; \mathbf{0}; \mathbf{0}\right] \in \mathbb{Z}^{m_2 \times m_1}$$

as a vertical block matrix where each block $\mathbf{P}^{(i)}$ has m_1 columns and w_i rows.

For each $i, j \in [m_1]$, the jth column of $\mathbf{P}^{(i)}$ contains the binary representation of $h'_{i,j} \in [0, \ldots, h_{i,i} - 1]$, which has length at most w_i. Specifically, $\mathbf{P}^{(i)}$ contains entries $p^{(i)}_{k,j} \in \{0, 1\}$ such that

$$h'_{i,j} = \sum_{k \in [w_i]} p^{(i)}_{k,j} \cdot 2^{k-1}.$$

Note that $\|\mathbf{p}_j\|^2 \leq \sum_{i \in [m_1]} w_i \leq 2n \lg q$.

By definition of $\mathbf{G}^{(i)}$, we have $\mathbf{G}^{(i)} \mathbf{p}^{(i)}_j = \mathbf{e}_i \cdot \sum_{k \in [m_1]} p^{(i)}_{k,j} \cdot 2^{k-1} = \mathbf{e}_i \cdot h'_{i,j}$, hence

$$\mathbf{GP} = \sum_{i \in [m_1]} \mathbf{G}^{(i)} \mathbf{P}^{(i)} = \mathbf{H}',$$

as desired.

Definition of $\mathbf{B}$. Let $\mathbf{T}_w \in \mathbb{Z}^{w \times w}$ be the upper-triangular unimodular matrix with 1s along the diagonal and -2s along the upper diagonal, i.e., $t_{i,i} = 1$ for $i \in [w]$ and $t_{i,i+1} = -2$ for $i \in [w-1]$ (all other entries are zero). By definition of $\mathbf{G}^{(i)}$, observe that $\mathbf{F}^{(i)} = \mathbf{G}^{(i)} \cdot \mathbf{T}_{w_i} \in \mathbb{Z}^{m_1 \times w_i}$ is simply $\mathbf{e}_i$ in its first column and zero elsewhere. Then letting $\mathbf{B}$ be the block diagonal matrix

$$\mathbf{B} = \mathrm{diag}(\mathbf{T}_{w_1}, \ldots, \mathbf{T}_{w_{m_1}}, \mathbf{I}) \in \mathbb{Z}^{m_2 \times m_2},$$

we see that $\mathbf{B}$ is unimodular and very short, i.e., $\|\mathbf{B}\|^2 \leq 5$, and that

$$\mathbf{GB} = \left[\mathbf{F}^{(1)} | \cdots | \mathbf{F}^{(m_1)} | \mathbf{M} | \mathbf{0}\right]$$

is also short, i.e., $\|\mathbf{GB}\| \leq C' \sqrt{d}$.

Definition of $\mathbf{R}$. Let $\mathbb{D} = \{\pm 1\}^d \times \{0\}^{m_1 - d}$ (recall that $d = (1 + \delta) n \lg q$). Each column $\mathbf{r}_j$ of $\mathbf{R}$ is chosen uniformly and independently from $\mathbb{D}$. In other words, all but the first d rows of $\mathbf{R}$ are zero, and the remaining entries are independent unbiased ± 1 random variables. By construction, $\|\mathbf{r}_i\|^2 = d$.

3.3.2 Distribution of $\mathbf{A}$

We now show that the distribution of $\mathbf{R}$ implies that $[\mathbf{A}_1 | \mathbf{A}_2]$ is close to uniformly distributed over $\mathbb{Z}_q^{n \times m}$. We first claim that for *odd* modulus q, $\{h_{\mathbf{A}_1} : h_{\mathbf{A}_1}(\mathbf{r}) = \mathbf{A}_1 \mathbf{r} \in \mathbb{Z}_q^n\}$ is a family of 2-universal hash functions from domain $\mathbb{D}$ to range $\mathbb{Z}_q^n$. To see this, note that for any fixed distinct $\mathbf{r}, \mathbf{r}' \in \mathbb{D}$, we have $\mathbf{A}_1 \mathbf{r} = \mathbf{A}_1 \mathbf{r}'$ if and only if $\mathbf{A}_1(\mathbf{r} - \mathbf{r}') = \mathbf{0} \in \mathbb{Z}_q^n$. Furthermore, $\mathbf{0} \neq \mathbf{r} - \mathbf{r}' \in \{0, \pm 2\}^d \times \{0\}^{m_1 - d}$. Suppose that $\mathbf{r}$ and $\mathbf{r}'$ differ in entry $i \in [d]$. Then because $\gcd(\pm 2, q) = 1$, we have

$$\Pr_{\mathbf{A}_1}[\mathbf{A}_1(\mathbf{r} - \mathbf{r}') = \mathbf{0}] = 1/|\mathbb{Z}_q^n| = q^{-n},$$

by averaging over any fixed choice of all but the ith column of $\mathbf{A}_1$.

Now because $d = (1 + \delta) n \log q$, Lemma 2.1 and the triangle inequality imply that $[\mathbf{A}_1 | \mathbf{A}_1 \cdot \mathbf{R}]$ is $(m_2 \cdot q^{-\delta n/2})$-uniform over $\mathbb{Z}_q^{n \times m}$. It follows that $\mathbf{A} = [\mathbf{A}_1 | -\mathbf{A}_1 \cdot (\mathbf{R} + \mathbf{G})]$ is as well.

3.3.3 Quality of S

We now analyze $\|\mathbf{S}\|$ and $\|\widetilde{\mathbf{S}}\|$. For both analyses, we partition $\mathbf{S}$ into two sets of vectors,

$$\mathbf{S}_1 = \{\mathbf{s}_j\}_{j \in [m_2]} = [\mathbf{D}; \mathbf{B}] = [(\mathbf{G} + \mathbf{R})\mathbf{B}; \mathbf{B}] \quad \text{and} \quad \mathbf{S}_2 = \{\mathbf{s}_j\}_{j > m_2} = [\mathbf{V}; \mathbf{P}] = [\mathbf{R}\mathbf{P} - \mathbf{I}; \mathbf{P}].$$

Length of basis vectors. We have

$$\|\mathbf{S}\| \leq \max\{\|\mathbf{S}_1\|, \|\mathbf{S}_2\|\}.$$

By the Pythagorean theorem and the triangle inequality,

$$\|\mathbf{S}_1\|^2 \leq \|\mathbf{G}\mathbf{B} + \mathbf{R}\mathbf{B}\|^2 + \|\mathbf{B}\|^2 \leq (C'\sqrt{d} + 3\sqrt{d})^2 + 5 \leq (C\sqrt{d} + 1)^2, \tag{3.5}$$

for some large enough constant $C > 0$.

For $\|\mathbf{S}_2\|$, observe that $\mathbf{R}$ is zero on all but a $d \times m_2$ submatrix whose entries are independent subgaussian random variables of some constant parameter $C'' > 0$. Therefore, for every fixed $\mathbf{p}_j$, the first d entries of $\mathbf{R}\mathbf{p}_j \in \mathbb{R}^{m_1}$ are independent subgaussian variables of parameter $C'' \cdot \|\mathbf{p}_j\| = O(\sqrt{n \lg q})$. By Lemma 2.2, the largest singular value of $\mathbf{R}\mathbf{p}_j$, and hence the length $\|\mathbf{R}\mathbf{p}_j\|$, is at most $O(\sqrt{dn \lg q}) = O(n \lg q)$ except with probability $2^{-\Omega(n)}$. By the union bound and triangle inequality, we conclude that $\|\mathbf{S}_2\| \leq O(n \lg q)$ except with probability $2^{-\Omega(n)}$, as desired.

Length of Gram-Schmidt vectors. First we review some preliminary facts that are needed in the analysis. Let $\mathbf{X} \in \mathbb{R}^{m \times \ell}$ be any set of $\ell \leq m$ linearly independent vectors. Then $\mathbf{P}_{\mathbf{X}} = \mathbf{X} \cdot (\mathbf{X}^t\mathbf{X})^{-1} \cdot \mathbf{X}^t \in \mathbb{R}^{m \times m}$ is the projection matrix of the orthogonal linear projection from $\mathbb{R}^m$ to $\operatorname{span}(\mathbf{X}) \subseteq \mathbb{R}^m$. (Note that the Gram matrix $\mathbf{X}^t\mathbf{X}$ is invertible because the vectors in $\mathbf{X}$ are linearly independent.) This fact may be verified by observing that any $\mathbf{v} \in \operatorname{span}(\mathbf{X})$ may be written as $\mathbf{v} = \mathbf{X}\mathbf{c}$ for some $\mathbf{c} \in \mathbb{R}^\ell$, hence

$$\mathbf{P}_{\mathbf{X}} \cdot \mathbf{v} = \mathbf{X} \cdot (\mathbf{X}^t\mathbf{X})^{-1} \cdot \mathbf{X}^t\mathbf{X} \cdot \mathbf{c} = \mathbf{X}\mathbf{c} = \mathbf{v};$$

moreover, for any $\mathbf{v} \in \operatorname{span}^\perp(\mathbf{X})$ we have $\mathbf{X}^t\mathbf{v} = \mathbf{0}$ and hence $\mathbf{P}_{\mathbf{X}} \cdot \mathbf{v} = \mathbf{0}$. Also note that for any $\mathbf{v} \in \mathbb{R}^m$,

$$\|\mathbf{P}_{\mathbf{X}} \cdot \mathbf{v}\|^2 = \langle \mathbf{P}_{\mathbf{X}} \cdot \mathbf{v}, \mathbf{P}_{\mathbf{X}} \cdot \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{P}_{\mathbf{X}} \cdot \mathbf{v} \rangle = \mathbf{v}^t \cdot \mathbf{P}_{\mathbf{X}} \cdot \mathbf{v} = (\mathbf{X}^t\mathbf{v})^t \cdot (\mathbf{X}^t\mathbf{X})^{-1} \cdot (\mathbf{X}^t\mathbf{v}), \tag{3.6}$$

because $\mathbf{v} - \mathbf{P}_{\mathbf{X}} \cdot \mathbf{v}$ is orthogonal to $\mathbf{P}_{\mathbf{X}} \cdot \mathbf{v}$.

In particular, we define $\mathbf{X} \in \mathbb{R}^{m \times m_1}$ as

$$\mathbf{X}^t = [-\mathbf{I} | \mathbf{G} + \mathbf{R}],$$

and observe that $\mathbf{X}$ is a (linearly independent) basis for $\operatorname{span}^\perp(\mathbf{S}_1)$, because

$$\dim\operatorname{span}(\mathbf{X}) = m_1 = m - \dim\operatorname{span}(\mathbf{S}_1) \quad \text{and} \quad \mathbf{X}^t \cdot \mathbf{S}_1 = -(\mathbf{G} + \mathbf{R})\mathbf{B} + (\mathbf{G} + \mathbf{R})\mathbf{B} = \mathbf{0}.$$

We now analyze $\|\widetilde{\mathbf{S}}\|$. Observe that

$$\|\widetilde{\mathbf{S}}\| = \max_{j \in [m]} \|\widetilde{\mathbf{s}_j}\| \leq \max\{\|\mathbf{S}_1\|, \|\mathbf{P}_{\mathbf{X}} \cdot \mathbf{S}_2\|\}, \tag{3.7}$$

because $\|\widetilde{\mathbf{s}_j}\| \leq \|\mathbf{s}_j\|$ for all $j \in [m_2]$, and $\widetilde{\mathbf{s}_j}$ is the orthogonal projection of $\mathbf{s}_j$ onto a linear subspace of $\operatorname{span}(\mathbf{X})$ for all $j > m_2$. Equation (3.5) has already established that $\|\mathbf{S}_1\| \leq C\sqrt{d} + 1$.

Bounding $\|\mathbf{P}_{\mathbf{X}} \cdot \mathbf{S}_2\|$ is more involved. We start by setting up some additional notation that will make the analysis more convenient. Define

$$\hat{\mathbf{G}} = [-\mathbf{I}|\mathbf{G}],\ \hat{\mathbf{R}} = [\mathbf{0}|\mathbf{R}] \in \mathbb{Z}^{m_1 \times m}, \quad \hat{\mathbf{P}} = [\mathbf{0}; \mathbf{P}] \in \mathbb{Z}^{m \times m_1}, \quad \hat{\mathbf{S}}_2 = \mathbf{S}_2 + [\mathbf{I}; \mathbf{0}] = [\mathbf{R}; \mathbf{I}] \cdot \mathbf{P}.$$

Now because $\|\hat{\mathbf{S}}_2\| \leq 1 + \|\mathbf{S}_2\|$, it is enough to bound $\|\mathbf{P}_{\mathbf{X}} \cdot \hat{\mathbf{S}}_2\|$. To do so, we analyze the two main components of the right-hand side of Equation (3.6). We have

$$\begin{aligned} \mathbf{X}^t \cdot \hat{\mathbf{S}}_2 &= [-\mathbf{I}|\mathbf{G} + \mathbf{R}] \cdot [\mathbf{R}; \mathbf{I}] \cdot \mathbf{P} = \mathbf{G} \cdot \mathbf{P} = \hat{\mathbf{G}} \cdot \hat{\mathbf{P}} \\ \mathbf{X}^t \mathbf{X} &= (\hat{\mathbf{G}} + \hat{\mathbf{R}})(\hat{\mathbf{G}} + \hat{\mathbf{R}})^t. \end{aligned}$$

We therefore want to analyze the properties of the positive semidefinite matrix

$$\mathbf{Z} = \hat{\mathbf{G}}^t \cdot \left((\hat{\mathbf{G}} + \hat{\mathbf{R}})(\hat{\mathbf{G}} + \hat{\mathbf{R}})^t\right)^{-1} \cdot \hat{\mathbf{G}}.$$

Note that the rows of $\hat{\mathbf{G}}$ are orthogonal by construction (because the rows of $\mathbf{G}$ are), that all its rows have length at least 1, and that its first d rows have length at least $C'\sqrt{w} \geq C'\sqrt{m_2}/2$ by the properties of the block $\mathbf{M}$. Therefore, we may factor $\hat{\mathbf{G}}$ as

$$\hat{\mathbf{G}} = \mathbf{D} \cdot \mathbf{V}$$

where the rows of $\mathbf{V} \in \mathbb{R}^{m_1 \times m}$ are orthonormal (i.e., $\mathbf{V}\mathbf{V}^t = \mathbf{I}$), and $\mathbf{D} \in \mathbb{R}^{m_1 \times m_1}$ is a nonsingular square diagonal matrix whose first d diagonal entries are all at least $C'\sqrt{m_2}/2$. Bringing $\mathbf{D}$ into the inverted central term from both sides, we therefore have

$$\mathbf{Z} = \mathbf{V}^t \cdot \left((\mathbf{V} + \mathbf{D}^{-1}\hat{\mathbf{R}})(\mathbf{V} + \mathbf{D}^{-1}\hat{\mathbf{R}})^t\right)^{-1} \cdot \mathbf{V}.$$

Below, we show that the singular values of $\mathbf{Y} = \mathbf{V} + \mathbf{D}^{-1}\hat{\mathbf{R}}$ are all at least $\frac{1}{2}$, with very high probability. Given this fact, it follows that the eigenvalues of $\mathbf{Z}$ are all at most 4. Because $\mathbf{Z}$ is positive semidefinite, it may be factored as $\mathbf{Z} = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^{-1}$ for some unitary matrix $\mathbf{U}$ and diagonal matrix $\mathbf{\Lambda}$ whose diagonal entries are the eigenvalues of $\mathbf{Z}$. From this we have

$$\|\mathbf{P}_{\mathbf{X}} \cdot \hat{\mathbf{S}}_2\|^2 = \max_{j \in [m_1]} \|\hat{\mathbf{p}}_j^t \cdot \mathbf{Z} \cdot \hat{\mathbf{p}}_j\|^2 \leq \max_{j \in [m_1]} (4 \cdot \|\hat{\mathbf{p}}_j\|^2) \leq 8n \lg q < (3\sqrt{d})^2.$$

It remains to bound the singular values of $\mathbf{Y} = \mathbf{V} + \mathbf{D}^{-1}\hat{\mathbf{R}}$ from below by $\frac{1}{2}$. To do so, it suffices to bound the singular values of $\mathbf{D}^{-1}\hat{\mathbf{R}}$ from *above* by $\frac{1}{2}$, because by the triangle inequality and the fact that the rows of $\mathbf{V}$ are orthonormal, the smallest singular value of $\mathbf{Y}$ is

$$\min_{\mathbf{x} \in S^{m-1}} \|\mathbf{V}^t\mathbf{x} + (\mathbf{D}^{-1}\hat{\mathbf{R}})^t\mathbf{x}\| \geq 1 - \max_{\mathbf{x} \in S^{m-1}} \|(\mathbf{D}^{-1}\hat{\mathbf{R}})^t\mathbf{x}\| \geq \frac{1}{2}.$$

By definition of $\hat{\mathbf{R}}$ and the properties of $\mathbf{D}$, the matrix $\mathbf{D}^{-1}\hat{\mathbf{R}}$ is zero on all but a $d \times m_2$ submatrix whose entries are independent subgaussian random variables of parameter $1/(C''\sqrt{m_2})$, where $C'' > 0$ is some constant multiple of C'. Lemma 2.2 implies that with probability $1 - 2^{-\Omega(d)}$, the singular values of $\mathbf{D}^{-1}\hat{\mathbf{R}}$ are all at most

$$\frac{C(\sqrt{d} + \sqrt{m_2})}{C''\sqrt{m_2}} \leq \frac{1}{2}$$

(for sufficiently large constant C''), and the proof is complete.

References

[Ajt99] Miklós Ajtai. Generating hard instances of the short basis problem. In *ICALP*, pages 1–9, 1999.

[Ajt04] Miklós Ajtai. Generating hard instances of lattice problems. *Quaderni di Matematica*, 13:1–32, 2004. Preliminary version in STOC 1996.

[GGH96] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Collision-free hashing from lattice problems. *Electronic Colloquium on Computational Complexity (ECCC)*, 3(42), 1996.

[GGH97] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In *CRYPTO*, pages 112–131, 1997.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206, 2008.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

[LPRTJ05] A. E. Litvak, A. Pajor, M. Rudelson, and N. Tomczak-Jaegermann. Smallest singular value of random matrices and geometry of random polytopes. *Advances in Mathematics*, 195(2):491–523, August 2005.

[Mic01] Daniele Micciancio. Improving lattice based cryptosystems using the Hermite normal form. In *CaLC*, pages 126–145, 2001.

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM J. Comput.*, 37(1):267–302, 2007. Preliminary version in FOCS 2004.

[MR09] Daniele Micciancio and Oded Regev. Lattice-based cryptography. In *Post Quantum Cryptography*, pages 147–191. Springer, February 2009.

[MV03] Daniele Micciancio and Salil P. Vadhan. Statistical zero-knowledge proofs with efficient provers: Lattice problems and more. In *CRYPTO*, pages 282–298, 2003.

[MW01] Daniele Micciancio and Bogdan Warinschi. A linear space algorithm for computing the Hermite normal form. In *ISSAC*, pages 231–236, 2001.

[Ngu99] Phong Q. Nguyen. Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto '97. In *CRYPTO*, pages 288–304, 1999.

[NR06] Phong Q. Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In *EUROCRYPT*, pages 271–288, 2006.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *STOC*, pages 333–342, 2009.

[PV08] Chris Peikert and Vinod Vaikuntanathan. Noninteractive statistical zero-knowledge proofs for lattice problems. In *CRYPTO*, pages 536–553, 2008.

[PVW08] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In *CRYPTO*, pages 554–571, 2008.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC*, pages 84–93, 2005.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.