LATTICE-BASED CRYPTOGRAPHY AND A COLLISION RESISTANT HASH FUNCTION

NATALIE HOLLENBAUGH

Contents

1. Introduction

The knapsack function, in its elementary form, given a particular integer vector $a = (a_1, \cdots, a_m)$, is the function from $\mathbb{Z}^m \to \mathbb{Z}$ given by

$$f_a(x) = \sum_{i=1}^{m} a_i \cdot x_i.$$

There is a natrual generalization of this funciton to arbitrary rings. For a ring R, a suset S of R, and $a \in R^m$, we define $f_a : S^m \to R$ in the same way as above.

There have been many attempts at cryptographic applications of these functions that have been broken, most notably the Merkle-Hellman cryptosystem, constructed in [3] by Ralph Merkle and Martin Hellman in 1978 (which is very early; for comparison, RSAwas first published in 1977), which is based on the assumption that it is intractible to, in general, find some nonzero $x \in \{0,1\}^m$ so that $f_a(x) = 0$. (This problem is called the subset-sum problem). It was shown by Adi Shamir [10] that this assumption is false.

In this paper, however, we examine a different instance of this problem, in particular taking $R = \mathbb{Z}[\alpha]/\langle \alpha^n - 1 \rangle$. Closely following Peikert and Rosen [8], we will show that, assuming the worst-case intractibility of a particular problem on integer lattices that the resulting family of functions $\{f_a\}$ is collision resistant. That is, we will show that it is intractible to find distinct x, x' so that $f_a(x) = f_a(x')$, which, because f_a is linear, is, in fact, a stronger condition than that it be intractible to find nonzero x such that $f_a(x) = 0$.

A hash function is one that shrinks its input. In particular, we take functions $h : \{1, 2, \cdots K\} \to \{1, 2, \cdots k\}$ for k much smaller than K. The hash functions $h : S \to$ that are useful in cryptography are those with (some of) the properties:

(1) Given some $h(m)$, it is infeasible to reconstruct m.

(2) It is infeasible to construct m, m' so that $h(m) = h(m')$.
(3) For no meaning of "similar" (independent of h) do similar but distinct m, m' have similar hash values $h(m)$ and $h(m')$.
(4) It is computationally fast to compute h.

Note that property 2 is stronger than property 1. In [4], Micciancio proved that, assuming hardness results of a problem on cyclic lattices (which will be discussed later), a particular collection of knapsack functions have the property 1. Peikert and Rosen [8], which we will reproduce, consider a different (but similar) collection of knapsack functions, and demonstrate that they have the proprty 2.

One of the foundational problems of lattice-based cryptography is the shortest vector problem (SVP, see Definition 4.4.1), which asks that, given an additive subset of $\mathbb{Z}^n$, expressed in terms of a lattice basis (that is, we are given an integer matrix B which yields a lattice $B\mathbb{Z}^n$), we find a vector with the shortest magnitude. This has been proven (for example, by Micciancio, in [5], even within an approximation factor $\sqrt{2}$) to be not solvable in polynomial time (under unproved but foundational conjectures) in the dimension n. In particular, he proves that SVP is not in RP.

Our result is based on the assumption that subIncSVP (see Definition 4.4.4) is hard. That is, our proof is a reduction from subIncSVP to finding collisions in our hash functions. In subIncSVP, we restrict the lattices that we consider to the cyclic lattices, those closed under the map $(a_1, \cdots, a_n) \mapsto (a_2, \cdots, a_n, a_1)$, and subIncSVP asks that, given some large enough lattice vector c, we find another lattice vector c' with $\|c'\| \leq \|c\|$. There is not (currently) a sufficient hardness result on subIncSVP, but subIncSVP is equivalent to the restriction of SVP to cyclic lattices (see [8]), and it is conjectured that this problem is also hard.

An interesting (and appealing) fact about lattice cryptography is that many of its proofs of hardness of average-case problems, which are those that allow useful cryptographic constructions, go by way of a reduction from that average-case problem to some worst-case problem. Ajtai's initial constructions of one-way hash functions in [1] is of this form, as is our result.

In practice, lattice-based cryptosystems are often slower than their more common counterparts, and cannot be implemented for practical applications (although the restriction to cyclic lattices makes things somewhat faster). They do not, however, seem to be vulnerable to quantum attacks, as are the conventional cyrptosystems, which are based on integer factorizaion or the discrete logarithm problem.

2. Algebra

2.1. **Definitions and elementary results.** We will give an ad hoc collection of definitions and results of elementary ring theory, a more thorough exposition of which can be found in, for example, [2].

Definition 2.1.1. A commutative[1] ring $(X, +, \cdot)$ is a set X equipped with two operations $+, \cdot : X^2 \to X$ (and we write $x_1 + x_2$ and $x_1 \cdot x_2$ or simply $x_1 x_2$) satisfying the following:

(1) *Associativity of addition:* $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$ for all $x_1, x_2, x_3 \in X$.
(2) *Commutativity of addition:* $x_1 + x_2 = x_2 + x_1$ for all $x_1, x_2 \in X$.

[1]The qualifier *commutative* refers to the axiom 6. If we omit 6 (and require that the other multiplicitive properties be two-sided), we are left with a ring.

(3) *Additive identity:* There is an element of X, denoted by 0 and called an additive identity, such that $x + 0 = x$ for all $x \in X$.
(4) *Additive inverses:* For each $x \in X$, there is an element of X, which can be shown to be unique, denoted by $-x$ and called the additive inverse of x such that $x + (-x) = 0$.
(5) *Associativity of multiplication:* $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$ for all $x_1, x_2, x_3 \in X$.
(6) *Commutativity of multiplication:* $x_1 \cdot x_2 = x_2 \cdot x_1$ for all $x_1, x_2 \in X$.
(7) *Multiplicitive identity:* There is an element of X, denoted by 1 and called a multiplicitive identity, such that $x \cdot 1 = x$ for all $x \in X$.
(8) *Distributivity:* $x_1 \cdot (x_2 + x_3) = x_1 \cdot x_2 + x_1 \cdot x_3$ and for all $x_1, x_2, x_3 \in X$.

We will say that a subset S of a ring R is a subring of R if S itself satisfies the ring axioms under the addition and multiplication operations it inherits from R.

Through most of this paper, we will consider only the following rings:

- $\mathbb{R}$, the real numbers,
- $\mathbb{Z}$, the integers,
- $\mathbb{Z}_m$, the integers reduced modulo some $m \in \mathbb{Z}$,
- the Cartesian product K^n, where K is one of the above rings, addition is defined component-wise, and multiplication by convolution (see Definition 4.1.1),
- $K[\alpha]$, the ring of polynomials in α with coefficients in K, where K is any of the fields above, where addition and multiplication are naturally extended from K, and
- the quotient rings $K[\alpha]/\langle \alpha^n - 1 \rangle$ for a ring K, which will be discussed shortly, and of which $\mathbb{Z}_m$ is a special case.

The verification that these are in fact commutative rings follows from their familiar properties.

Definition 2.1.2. An element x of a ring R is a *zero divisor* if there is some $y \neq 0$ such that $xy = yz = 0$.

As a concrete example, notice that although $\mathbb{Z}$ does not have zero divisors, Z_m for m not prime does have zero divisors, because if q divides m, then we can write $pq = m = 0$ for some p.

Definition 2.1.3. An *integer domain* is a ring that has no zero divisors.

Then it can be shown that $\mathbb{Z}$ is an integer domain, and that $\mathbb{Z}_p$ is an integer domain if and only if p is prime.

Definition 2.1.4. A finitely generated ideal in a commutative ring R is a set of the form $\{y_1 a_1 + \cdots + y_m a_m : y_i \in R\}$ for some subset $A = \{a_1, \cdots, a_m\} \subset R$, and we write $\{y_1 a_1 + \cdots + y_m a_m : y_i \in R\} = \langle A \rangle$.

Definition 2.1.5. For an ideal J of a commutative ring R, the *quotient ring* R/J is the collection of subsets of R of the form $\overline{x} = \{y : x - y \in J\}$.

Proposition 2.1.6. *The sets $\overline{y}$ of a quotient ring R/J partition R and have the structure of a ring, with operations induced by the map $\phi : R/J \to R$ given by $\overline{y} \mapsto y$.*

We will make extensive use of this construction with quotient groups similar to $\mathbb{Z}[\alpha]/\langle \alpha^n - 1 \rangle$, which we give here as an example.

Example 2.1.7. By $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$, we denote a set of polynomials in α of degree less than n, with coefficients in $\mathbb{Z}$, along with a multiplicative structure by which we identify $\alpha^n - 1$ with 0. That is, we can multiply two elements $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$ as we would in $\mathbb{Z}[\alpha]$, then *reduce modulo* $\alpha^n - 1$, much as we do when we deal with modular arithmetic in $\mathbb{Z}$. For example, with $n = 4$, we write

$$(\alpha^3 + 2\alpha)(\alpha^2) = \alpha^5 + 2\alpha^3 = (\alpha^4)(\alpha) + 2\alpha^3 = \alpha + 2\alpha^3.$$

One of the properties of $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$ that we will use (see Theorem 6.1.1) is that it is not an integral domain. For example, the elephant-teacup identity gives

$$(\alpha - 1)(\alpha^{n-1} + \cdots + \alpha + 1) = \alpha^n - 1 = 0,$$

but neither $\alpha - 1$ nor $\alpha^{n-1} + \cdots + \alpha + 1$ is zero in $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$.

Proposition 2.1.8. *Let a, b, and c in some ring R, and suppose that $ab = c$. Let $I = \langle a\rangle$, $J = \langle b\rangle$, and $K = \langle c\rangle$ be principal ideals in R, then $I/J \cong R/K$.*

3. Computability

3.1. Asymptotic Analysis and Polynomial Time Algorithms.

Definition 3.1.1. A function $f(n)$ is said to be $O(g(n))$, written as $f(n) \in O(g(n))$ or $f(n) = O(g(n))$, if

$$\limsup_{n\to\infty} f(n)/g(n)$$

is finite. Also, we write $f(n) \in \Theta(g(n))$ if $f(n) \in O(g(n))$ and $g(n) \in O(f(n))$.

We will use these ideas to consider the runtime of an algorithm. Roughly, the runtime is a measure of the number of simple calculations that a computer has to perform in order to complete the algorithm. We will not be more precise about these concepts than to use the rather intuitive definitions of an algorithm as a sequence of steps that can be performed by a computer to solve some problem, given some parameters, and the runtime the number of arithmetic operations, dependent on the parameters passed to the algorithm, required to perform them.

To illustrate these ideas, in place of a formal definition, we will give a well-known example from linear algebra.

Example 3.1.2 (Gram-Schmidt Orthogonalization Algorithm)**.** We will construct an algorithm $\mathcal{A}$ that takes as input a list of vectors in $\mathbb{R}^m$ and produces an orthogonal list of vectors such that the first k elements of both lists span the same space, and we write $A(\{b_1, \cdots b_n\}) = \left\{\tilde{b}_1, \cdots \tilde{b}_n\right\}$. The algorithm proceeds as follows:

(1) Let $B = (b_1)$.
(2) For each $i \in [2, \cdots n]$, compute

$$\tilde{b}_i = b_i - \sum_{j=1}^{i-1} \frac{\langle b_i, b_j\rangle}{\langle b_j, b_j\rangle} b_j,$$

and let $B \leftarrow (B|\tilde{b}_i)$.
(3) Output B.

A proof of the correctness of the algorithm is an elementary result of linear algebra, and we will analyze its runtime. In doing so, we will assume that simple operations

such as arithmetic operations on two real numbers[2] or the definition something (let $a = 4$) take time 1. Then the first step is performed in $O(1)$ time. The second step requires that we compute this sum for each value of i. For fixed i, to compute the summand requires $3m + 1$ operations (m each to compute $\langle b_i, b_j \rangle$ and $\langle b_j, b_j \rangle$, one to divide these results, and m to multiply this through b_j), which we repeat $(i-1)$ times, for a total of $(i-1)(3m+1)+i$ operations. Then, since we compute this, we sum over i, so the second step requires a total of

$$n + \sum_{i=1}^{n} [(i-1)(3m+1)+i] = \tfrac{3}{2}mn^2 + n^2 + \tfrac{9}{2}mn - 6m + 3n - 3$$

operations and note that this expression is in $O(mn^2)$ (in writing this, we mean to consider the expression separately as a function of m and as a function of n). The final step runs in $O(1)$ time, so the entire algorithm runs in time $O(1 + mn^2 + 1) = O(mn^2)$ time.

Determining the smallest possible runtime over any algorithm that solves a particular problem is of primary interest to many areas of computer science, including ours, because of the direct effects these minimum runtimes have on our ability to solve the problems in practice. For this reason, we often consider together collections of runtimes that behave similarly. For example, any algorithm with a runtime in $O(n^c)$ for some constant c is said to be polynomial-time, and any algorithm with a runtime in $O(\exp(n^c))$ for some constant c is said to run in exponential time. Finally, we will say that a function $\epsilon(n)$ is negligable if ϵ grows more slowly than any polynomial in $1/n$, that is if $\epsilon(n) \notin O(1/n^c)$ for all constants c.

3.2. **Reductions.**

Definition 3.2.1. Given two problems A and B, we will say that there is a polynomial time recuction from A to B if it is the case that if there is an algorithm for B that runs in time $O(g(n))$, then there is also an algorithm for A that runs in time $O(n^c g(n))$ for some c.

The emphasis given to polynomial time algorithms is not unintentional; we could certainly consider other classes of reductions, but we often consider problems that can be solved in polynomial time to be easy and those that cannot to be hard. One reason for this is that this provides a noticible threshold for theoretical considerations; it is often the case that we consider a problem that can be solved easily in exponential time, but determining whether it can be solved in polynomial time is not trivial. The other reason for this division is that it provides a reasonable approximation to a distinciton between problems that are feasible to solve using physical computers and those that are not.

Notice, then, that the existance of a reduction from A to B means that B is at least as hard to solve as A, because if we can solve B, then we have an algorithm to solve A in time greater only by a polynomial factor. This is not, however a

[2]In fact, we consider operations that require a single CPU operation to take time 1, and neglect operations that a computer would perform as allocating memory. Then division of two numbers requires (often) significantly more time than addition of two numbers, and the time to add two numbers grows with the magnitude of the numbers if the numbers become too large for the computer to process in a single operation. However, we will usually implicitly assume that the numbers we work with are bounded so that these differences will appear only as constant factors, which we can disregard in considering asymptotic behaviour.

symmetric relation. A reduction from A to B does not mean that A and B are in any sense equivalent; even if A reduces to B, it is possible that A be much easier than B.

In constructing a reduction from A to B, we often make use of an oracle for B. That is, we assume an object $\mathcal{F}$ which we can supply with a particular instance of a problem, and it will give us a solution in constant time. Then to construct a reduction from A to B, we need only to construct a polynomial time algorithm for A assuming $\mathcal{O}$. As a trivial example, consider the following:

Example 3.2.2. *There is a polynomial time reduction to from factoring integers to factoring integers divisible by* 7*.*

We will assume an oracle $\mathcal{F}$ that, given a number m known to be divisible by 7, will return an ordered list $(p_1, \cdots, p_r)$ of primes so that $p_1 \cdots p_r = m$.

Using $\mathcal{F}$, can factor an arbitrary integer m in the following way:

(1) Compute $M = 7m$
(2) Give M to $\mathcal{F}$, which will return a list $(p_1, \cdots, p_n)$ of primes, one of which is 7.
(3) Remove a 7 from the list $(p_1, \cdots, p_n)$.

4. Lattices

4.1. **Identification of $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$ with $\mathbb{Z}^n$.** The elements of $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$ can be uniquely represented as polynomials of degree at most $n-1$, so we can identify $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$ with $\mathbb{Z}^n$ as $a_0 + \cdots + a_{n-1}z^{n-1} \xrightarrow{j} (a_0, \cdots a_{n-1})$. Certainly j respects the additive structure (that is, $j(s_1 + s_2) = j(s_1) + j(s_2)$ for $s_1, s_2 \in \mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$) of the two sets, and moreover, it induces a multiplicitive structure on $\mathbb{Z}^n$:

Definition 4.1.1. The convolution of $a \in \mathbb{Z}^n$ and $b \in \mathbb{Z}^n$, writen as $a \otimes b$ is the element $j(j^{-1}(a) \cdot j^{-1}(b))$ of $\mathbb{Z}^n$, where j is the identification described above.

With this multiplicitive structure, $\mathbb{Z}^n$ is isomorphic to $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$.

Finally, the introduction of $\mathbb{Z}^n$ gives us a norm on $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$, and we will write $\|a\|$ for the Euclidean L^2 norm $\|a\| = \sqrt{a_0^2 + \cdots + a_n^2}$, and $\|a\|_\infty$ for the maximum norm $\|a\|_\infty = \max\{|a_i|\}$, We will change between the notations $x(\alpha) \in \mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$ and $x \in \mathbb{Z}^n$ readily and without comment.

4.2. **Cyclic Lattices.**

Definition 4.2.1. Given some $B = [b_1, \cdots, b_m] \in \mathbb{Z}^{n\times m}$ where the b_j are linearly independent in $\mathbb{R}^n$ and have coefficients in $\mathbb{Z}^n$, we define the set $\mathcal{L}(B) = \{\beta_0 b_0 + \cdots + \beta_m b_m : \beta_k \in \mathbb{Z}\}$, and we say that $\mathcal{L}(B)$ is a lattice with basis B.

For $a = (a_1, a_2, \cdots, a_n) \in \mathbb{Z}^n$, we define the rotation of a to be the vector $\mathrm{rot}(a) = (a_n, a_1, \cdots, a_{n-1})$ and the matrix $\mathrm{Rot}^d(a)\mathbb{R}^{n\times d}$ with jth column $\mathrm{rot}^j(c)$ (where the superscript is a composition).

Proposition 4.2.2. *$b = \mathrm{rot}\, c$ if and only if $b(\alpha) = \alpha c(\alpha)$.*

Proof. Let ψ be be the bijection given by

$$(a_0, a_1, \cdots c_{n-1}) \mapsto a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}.$$

Then we want to show that $b = \operatorname{rot} c$ if and only if $\psi(b) = \alpha\psi(c)$, which holds if and only if $b = \psi^{-1}(\alpha\psi(c))$. We write $b = (b_0, \cdots, b_{n-1})$ and $a = (a_0, \cdots, b_{n-1})$. Then

$$\alpha\psi(c) = c_0\alpha + \cdots + c_{n-1}\alpha^n = c_0\alpha + \cdots + c_{n-2}\alpha^{n-1} + c_{n-1},$$

so

$$\psi^{-1}(\alpha\psi(c)) = (c_{n-1}, c_0, \cdots, c_{n-2}),$$

which is equal to b if and only if $b = \operatorname{rot} c$. □

We say that a lattice $\mathcal{L}(B)$ is *cyclic* if it is closed under rotation, that is if $\operatorname{rot} v \in \mathcal{L}(B)$ whenever $v \in \mathcal{L}(B)$. But this is equivalent to requiring that the lattice generated by B be an ideal in $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$. That is,

Proposition 4.2.3. *A lattice basis $B = (b_1, \cdots, b_n)$ generates a cyclic lattice if and only if the subring $\{c_1b_1(\alpha) + \cdots + c_nb_n(\alpha)\}$ is an ideal in $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$.*

Proof. We first show that that an ideal J in $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$ is a cyclic lattice. But this is the case if J is closed under rot, which we have shown to be equivalent to multiplication by α. But certainly J is closed under multiplication by α.

Now consider an cyclic lattice $\mathcal{L}(B)$, and we show that the subring $\{c_1b_1(\alpha) + \cdots + c_nb_n(\alpha)\}$ is closed under multiplication by elements of $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$. But for some $a_0 + \cdots + a_n\alpha^{n-1}$,

$$(a_0 + \cdots + a_{n-1}\alpha^{n-1})(c_1b_1 + \cdots + c_nb_n) = \sum_{j=0}^{n-1} \alpha^j(a_jc_1b_1 + \cdots + a_jc_nb_n).$$

but each of the $a_jc_1b_1 + \cdots + a_jc_nb_n$ is in $\mathcal{L}(B)$ because $\mathcal{L}(B)$ is additive. Then $\alpha^j(a_jc_1b_1 + \cdots + a_jc_nb_n)$ is in $\mathcal{L}(B)$ because $\mathcal{L}(B)$ is closed under rot, which is equivalent to multiplication by α, and finally the sum is in $\mathcal{L}(B)$ again because B is additive. □

Lemma 4.2.4. *Let $c \in \mathbb{Z}^n$, and $\Phi(\alpha) \in \mathbb{Z}[\alpha]$ so that $\Phi(\alpha)$ divides $\alpha^n - 1$, and suppose that $c(\alpha)$ and $\Phi(\alpha)$ are coprime over $\mathbb{C}[\alpha]$, and say that $\Phi(\alpha)$ has degree d Then the set $\{c, \operatorname{rot}(c), \cdots, \operatorname{rot}^{d-1}(c)\}$ is linearly independent.*

Proof. Let $t_0, \cdots, t_{d-1}$ such that $0 = \sum_i t_i \operatorname{rot}^i(c)$, and we will show the t_j are zero. Define $t(\alpha) = t_0 + \cdots + t_{d-1}\alpha^{n-1}$, and $t(\alpha)c(\alpha) = 0$ in $\mathbb{Z}[\alpha]/\langle\alpha^n - 1\rangle$, so $(\alpha^n - 1)$ divides $t(\alpha)c(\alpha)$, and we write $t(\alpha)c(\alpha) = h_1(\alpha)(\alpha^n - 1)$. But also $\Phi(\alpha)$ divides $\alpha^n - 1$, so we write $\alpha^n - 1 = h_2(\alpha)\Phi(\alpha)$. But then

$$t(\alpha)c(\alpha) = h_1(\alpha)(\alpha^n - 1) = h_1(\alpha)h_2(\alpha)\Phi(\alpha),$$

so each root of $\Phi(\alpha)$ must also be a root of $t(\alpha)c(\alpha)$. But $c(\alpha)$ and $\Phi(\alpha)$ are coprime over $\mathbb{R}[\alpha]$, so all of the roots of $\Phi(\alpha)$ must be roots of $t(\alpha)$. But if $t(\alpha)$ is nonzero, this is impossible because $\Phi(\alpha)$ has degree d, and $t(\alpha)$ has degree at most $d - 1$. Then each t_j must be zero. □

This is not an insignificant additional structure to place on the lattices we consider; not only does it, as in [8], give us more control over the lattices in the theoretical context, but the resulting practical applications seem to be much faster to compute. Moreover, it seems to be the case that the worst-case problems on general lattices that we would like to consider can be restricted to cyclic lattices without sacrificing hardness.

4.3. **Cyclotomic Polynomials.** In addition to the restriction to cyclic lattices we will propose a restriction to *cyclotomic subspaces* of $\mathbb{R}^n$, which makes use of the factorization of $\alpha^n - 1$ in $\mathbb{Z}[\alpha]/\langle \alpha^n - 1 \rangle$.

Definition 4.3.1. The cyclotomic polynomial $\Phi_k(\alpha)$ is the monic polynomial with roots exactly the kth primitive roots of unity. That is, for a primitive kth root ζ of unity,

$$\Phi_k(\alpha) = \prod_{\substack{j \in [1,k] \\ \gcd(j,k)=1}} (\alpha - \zeta^j)$$

Proposition 4.3.2. *The cyclotomic polynomials $\Phi_k(\alpha)$ are irreducible over $\mathbb{Z}[\alpha]$, and $\alpha^n - 1$ is a product of the cyclotomic polynomials, as*

$$\alpha^n - 1 = \prod_{j|n} \Phi_k(\alpha).$$

Definition 4.3.3. The *cyclotomic subspace* H_Φ for some product of cyclotomic polynomials Φ, is the subset of $\mathbb{R}^n$ given by

$$H_\Phi = \{x \in \mathbb{R}^n : \Phi(\alpha) \text{ divides } x(\alpha) \text{ over } \mathbb{R}[\alpha]\}.$$

Proposition 4.3.4. *H_Φ is a linear subspace of $\mathbb{R}^n$.*

Proposition 4.3.5. *H_Φ is closed under* rot*.*

4.4. **Worst-case Problems on Lattices.** We will define some of the standard problems on lattices. These will be parametrized by an approximation factor $\gamma(n)$, which is a function of our security parameter, and by a lattice parameter ζ, which is some parameter of the lattice, usually taken to be, for example, $\lambda_1(B)$, the length of the shortest vector in $\mathcal{L}(B)$ in Definition 4.4.1 or $\eta_\epsilon(B)$, the smoothing parameter in Definition 4.4.4

Definition 4.4.1. The *short vector problem* SVP, for an approximation factor $\gamma(n)$ and a lattice parameter ζ, requires that, for a lattice $\mathcal{L}(B)$ of dimension n, we compute some lattice vector $v \in \mathcal{L}(B)$ with magnitude $\|v\| \leq \gamma(n)\zeta(\mathcal{L}(B))$.

Definition 4.4.2. The *short independent vectors problem* SIVP, for an approximation factor $\gamma(n)$ and a lattice parameter ζ, requires that, for a lattice $\mathcal{L}(B)$ of dimension n, we compute a list of n linearly independent lattice vectors $(v_1, \cdots, v_n)$ such that $\|v_i\| \leq \gamma(n)\zeta(\mathcal{L}(B))$.

Definition 4.4.3. The *incremental short vector problem* IncSVP, for an approximation factor $\gamma(n)$ and a lattice parameter ζ, requires that, for a lattice $\mathcal{L}(B)$ of dimension n, and a lattice vector c with $\|c\| \geq \gamma(n)\zeta(\mathcal{L}(B))$, we compute a non-zero lattice vector c' with $\|c'\| \leq \|c\|/2$.

In this paper and in ring-based lattice cryptography, we use generalized versions of these problems. For example, the problem used in the main reduction of this paper in Section 6.3 is:

Definition 4.4.4. The *cyclotomic incremental short vector problem* $\text{subIncSVP}_\gamma^\zeta$, for an approximation factor $\gamma(n)$ and a lattice parameter ζ, requires that, given a cyclic lattice $\mathcal{L}(B)$ of dimension n, a polynomial $\Phi(\alpha) = (\alpha^n - 1)/\Phi_k(\alpha)$ for some cyclotomic polynomial $\Phi_k(\alpha)$, and a lattice vector $c \in \mathcal{L}(B) \cap H_\Phi$, with $\|c\| \geq \gamma(n)\zeta(\mathcal{L}(B) \cap H_\Phi)$, we compute a nonzero lattice vector $c' \in \mathcal{L}(B) \cap H_\Phi$ with $\|c'\| \leq \|c\|/2$.

In the course of working with SVP, we consider a function $f_A : \mathbb{Z}^{n\times m} \to \mathbb{Z}^n$. This function itself can yield a useful hash function. Inded it is a special case of the more general collection of hash functions of interest for us here.

Definition 4.4.5. For a ring R and a subset S of R, along with some integer m, we define $\mathcal{H}(R, S, m)$ to be the collection of functions from S^m to R of the form

$$f_a(x) = \sum_{j=1}^{m} a_j x_j$$

for $a \in R^m$, where we have written $a = (a_1, \cdots, a_m)$ and $x = (x_1, \cdots, x_m)$.

5. Probabiliy Measures on Lattices

5.1. The main theorem of this paper is a probabilistic reduction from an average case problem. In this section, we will develop the framework to work with the required concepts concerning probability

Definition 5.1.1. A *probability distribution* on a set S is a function $\chi : S \to [0, 1]$ with $\int_S \chi(x) = 1$, were $\int$ represents some appropriate integral, including, should S be countable, a sum.

Definition 5.1.2. For a probability distribution ψ over S and a subset A of S, we define

$$\Pr[A] = \int_S a \in A\chi(a)\, da,$$

and we often write $\Pr[Q(a)]$ for $\Pr[\{a \in S : Q(a)\}]$.

We will also consider the natural probability measure induced on the cartesian product of two sets. If we have χ_1 and χ_2 probability distributions over X_1 and X_1 respectively, then we define the function ψ on $X \times Y$ given by $\psi(a, b) = \chi_1(a)\chi_2(b)$, which is in fact a probability measure.

We will also define a distance over probability measures.

Definition 5.1.3. For two probability distributions δ_X and δ_Y on a set S, we define the *statistical distance* $\Delta(\delta_X, \delta_Y)$ to be

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

where we again take some appropriate integral $\int$.

The statistical distance is a semimetric. That is,

(1) $\Delta(\delta_X, \delta_Y) \geq 0$,
(2) $\Delta(\delta_X, \delta_X) = 0$,
(3) $\Delta(\delta_X, \delta_Y) = \Delta(\delta_Y, \delta_X)$, and
(4) $\Delta(\delta_X, \delta_Y) + \Delta(\delta_Y, \delta_Z) \leq \Delta(\delta_X, \delta_Z)$,

and these properties follow from the familiar properties of the integral. We will also write $\Delta(a, b)$ for $\Delta(\psi, \chi)$ when a and b are random variables distribued according to ψ and χ respectively.

Proposition 5.1.4. *Let ψ_1 and χ_1 be probability measures over some set S and let ψ_2 and χ_2 be probability measures over some set T, and let $\psi(a, b) = \psi_1(a)\psi_2(b)$ and $\chi(a, b) = \chi_1(a)\chi_2(b)$ be the induced probability measures over $S \times T$. Then $\Delta(\psi, \chi) \leq \Delta(\psi_1, \chi_1) + \Delta(\psi_2, \chi_2)$.*

Proposition 5.1.5. *For two random variables X and Y over a set A, and an function f with domain A,*

$$\Delta\left(f(X), f(Y)\right) \leq \Delta\left(X, Y\right),$$

with equality of f is bijective.

Proposition 5.1.6. *Let X be distributed to χ over S and let Y be destributed to ψ over S, and suppose that $\Pr\left[X \in T\right] \geq q$ and that $\Delta\left(\chi, \psi\right) \leq \epsilon$. Then $\Pr\left[Y \in T\right] \geq q - \epsilon$.*

Proof. We will bound $\Pr\left[X \in T\right] - \Pr\left[Y \in T\right]$.

$$\begin{aligned}
\left|\Pr\left[X \in T\right] - \Pr\left[Y \in T\right]\right| &= \left|\int_T \chi(a)\, da - \int_T \psi(a)\, da\right| \\
&\leq \int_T \left|\chi(a) - \psi(a)\right| da \\
&\leq \int_S \left|\chi(a) - \psi(a)\right| da \\
&= 2\,\Delta\left(\chi, \psi\right) \\
&\leq \epsilon,
\end{aligned}$$

so $\Pr\left[Y \in T\right] \geq \Pr\left[X \in T\right] - \epsilon \geq q - \epsilon$. □

We now define a few probability measures that we will make use of. The first is the uniform distribution U_A over some (finite) set A. This is the distribution with the property that $U_A(a) = U_A(b)$ for any $a, b \in A$.

We also define a normal distribution over a subspace $\mathbb{R}^n$.

Definition 5.1.7. The Gaussian distribution over a subset H of $\mathbb{R}^n$ with dimsension d with width $s > 0$, and centered at $c \in H$ is given by

$$D_{H,s,c}(x) = \frac{\exp\left(-\pi \left\|x - c\right\|^2 / s^2\right)}{s^d}$$

for $x \in H$, and $D_{H,x,c}(x) = 0$ otherwise.

$D_{H,s,c}$ gives a probability distribution over H. In fact, it can be expressed as a product of one dimensional Gaussian distributions over an orthonormal basis for H. More precisely, consider an orthogonal basis $(e_1, \cdots, e_d)$ for H. Then we write $u = u_1 e_1 + \cdots + u_d e_d$ so that $\left\|u\right\|^2 = u_1^2 + \cdots + u_d^2$. Then

$$\begin{aligned}
\int_H D_{H,s,c}(x) &= \int_H e^{-\pi \|x-c\|^2 / s^2}\, dx \\
&= \prod_{j=1}^{d} \int_{-\infty}^{\infty} e^{-\pi (x_j - c_j)^2 / s^2}\, dx_j = 1.
\end{aligned}$$

We also define a Gaussian measure over lattices. For a lattice $\mathcal{L}\left(B\right) \subset H$ with dimension equal to the dimension of H, define

$$D_{\mathcal{L}(B),s,c}(x) = \frac{D_{H,s,c}(x)}{\sum_{v \in \mathcal{L}(B)} D_{H,s,c}(v)},$$

which is a probability distribution over $\mathcal{L}(B)$, because

$$\sum_{x\in\mathcal{L}(B)} D_{\mathcal{L}(B),s,c}(x) = \frac{\sum_{x\in\mathcal{L}(B)} D_{\mathcal{L}(B),s,c}(x)}{\sum_{x\in\mathcal{L}(B)} D_{\mathcal{L}(B),s,c}(x)} = 1.$$

We now introduce a lattice parameter $\eta_\epsilon(\mathcal{L}(B))$ for small $\epsilon > 0$, called the smoothing parameter, that will allow us to control this distribution in the following way:

Lemma 5.1.8. *For a lattice $\mathcal{L}(B)$ spanning the subspace H of $\mathbb{R}^n$ and $\epsilon > 0$,*

$$\Delta\left(D_{H,s,c} \pmod{\mathcal{P}(B)}, U(\mathcal{P}(B))\right) \leq \epsilon/2$$

for any c and for $s > \eta_\epsilon(\mathcal{L}(B))$.

Equivalently, the distribution resulting from the addition of noise distributed according to $D_{H,s,c}$ to the lattice $\mathcal{L}(B)$ is almost uniform. We will use the following property (proved in [8], 2.16) of Gaussian distributions with width greater than $\eta_\epsilon(\mathcal{L}(B))$:

Lemma 5.1.9. *Let $\mathcal{L}(B)$ be a lattice spanning the subspace H of $\mathbb{R}^n$, let $c \in H$, and $s > \eta_\epsilon(\mathcal{L}(B))$. Then for any $v \in \mathcal{L}(B)$,*

$$D_{\mathcal{L}(B),s,c}(v) \leq s^{-d}\frac{1+\epsilon}{1-\epsilon}.$$

We will also use a bound on the product of a lattice vector distributed according to a Gaussian didstribution with width greater than $\eta_\epsilon(\mathcal{L}(B))$. This was proved[3] in [9], Lemma 4.1.

Lemma 5.1.10. *For a subspace H of $\mathbb{R}^n$ with dimension d, a lattice $\mathcal{L}(B)$ spanning H, positive reals ρ, ϵ and $s > 2\eta_\epsilon(\mathcal{L}(b))$, vectors c and x, and a vector v distributed according to $D_{\mathcal{L}(B),s,c}$,*

$$\Pr\left[\|(v-c)\otimes x\| > \rho\right] \leq \frac{s\sqrt{d}\,\|x\|}{\rho}.$$

The lattice parameter was first introduced by Micciancio and Regev [6] The explicit definition of η_ϵ and subsequent proofs of Lemmas 5.1.8, 5.1.9, and 5.1.10 require some constructions that do not provide additional insight in our context. They can be found in [8], Definition 2.10ff.

6. Main Results

We now give the main results of [8]. In section 6.1, we will consider the hash functions $\mathcal{H}(\mathbb{Z}_p^n, [0,D]^n, m)$ for $p(n)$ and $D(n)$ polynomially bounded, which are the functions considered by Micciancio in [4]. We will show, in section 6.3, that these are not collision resistant. We will then show that if we restrict the functions $f_A(X)$ to cyclotomic subspaces, the resulting family of hash functions is collision resistant, assuming that subIncSVP is hard.

[3]Micciancio [5] gives this result for full-rank lattices, and [8] generalizes to subspaces. The result actually proved is that $E_{v\sim D_{\mathcal{L}(B),s,c}}\left[\|(v-c)\otimes x\|^2\right] \leq s^2 d\,\|x\|^2$, and our result follows from Markov's inequality and that $\mathrm{Var}[X] = E[X^2] - E[X]^2 \geq 0$ for any random variable X.

6.1. Finding Collisions in $\mathcal{H}(\mathbb{Z}^n_{p(n)}, [0,D]^n, m(n))$. We will consider the family of functions $\mathcal{H}(\mathbb{Z}^n_{p(n)}, [0,D(n)]^n, m(n))$ where $p(n) \in n^{\Theta(1)}$ and $D(n) \in n^{O(1)}$ (that is, $p(n)$ and $D(n)$ are polynomially bounded), and we will show that for an integer q that divides n, there is an $X \in [0,D]^{n\times m}$ such that $\|X\|_\infty = 1$ and $f_A(X) = 0$ with probability $1/p^q$ (with respect to uniformly chosen $A \in \mathbb{Z}_p^{n\times m}$). This will give us something rather stronger than collisions: it gives us second preimages on $[0,D)^{n\times m}$. This is because f_A is additive. In particular, for $X' \in [0,D)^{n\times m}$, both X' and $X'+X$ are in $[0,D]^{n\times m}$ and $f_A(X'+X) = f_A(X') + f_A(X) = f_A(X')$.

To do this, we will take advantage of the fact that $\mathbb{Z}_p[\alpha]/\langle \alpha^n - 1\rangle$ has zero divisors for any n. In fact, if $q \mid n$ (including $q = 1$), the $0 = \alpha^n - 1 = (\alpha^q - 1)(\alpha^{n-q} + \alpha^{n-2q} + \cdots + 1)$. Then:

Theorem 6.1.1. *Let $X = (x_1, \cdots, x_n)$ with $x_1(\alpha) = (\alpha^n - 1)/(\alpha^q - 1)$ and $x_j = 0$ for $j \neq 1$. Then for $A \in \mathbb{Z}_p^{n\times m}$ uniformly random, $f_A(X) = 0$ with non-negligible probablity.*

Proof. For $A = (a_1, \cdots a_n)$,

$$\begin{aligned} f_A(X) &= \sum_{j=1}^{n} a_j(\alpha)x_j(\alpha) \\ &= a_1(\alpha)\left(\frac{\alpha^n - 1}{\alpha^q - 1}\right) + \sum_{j=1}^{n} a_j(\alpha)x_j(\alpha) \\ &= a_1(\alpha)\left(\frac{\alpha^n - 1}{\alpha^q - 1}\right), \end{aligned}$$

which is zero if $\alpha^q - 1$ divides $a_1(\alpha)$. But consider that there are unique $s(\alpha), r(\alpha) \in \mathbb{Z}_p[\alpha]$ with $(r(\alpha)) < q$ so that $a_1(\alpha) = s(\alpha)(\alpha^q - 1) + r(\alpha)$. But there is a one-to-one correspondance between $s(\alpha)$ and $r(\alpha)$ over polynomials of degree less than n/q and q respectively and $a_1(\alpha)$ over polynomials of degree less than n, so because we $a_1(\alpha)$ is uniformly random, then so is $r(\alpha)$. But there are p^q polynomials of degree less than q with coefficients in $\mathbb{Z}_p$, and exactly one of them, namely 0, will make a_1 divisible by $\alpha^q - 1$, so a_1 is divisible by $\alpha^q - 1$ with probability $1/p^q$, and so $f_A(X) = 0$ with probability $1/p^q$. □

This result is sufficient to find second preimages with non-negligible probability because $\|X\|_\infty = \|x_1\|_\infty = 1$.

6.2. Preventing This Attack. The attack given in the previous section relied heavily on the fact that $\mathbb{Z}_p[\alpha]/\langle \alpha^n - 1\rangle$ has zero divisors. A reasonable strategy to modify our hash funcitons, then, might be to use some integral domain in place of $\mathbb{Z}_p[\alpha]/\langle \alpha^n - 1\rangle$. However, we need not make so strong a change; the sufficient modification that we will now consider is that we require each x_i to be divisible (in $\mathbb{Z}[\alpha]/\langle \alpha^n - 1\rangle$) by $\Phi = (\alpha^n - 1)/\Phi_k(\alpha)$ for some $k \mid n$, $k \neq 1$. That is, rather than working with $X \in [0,D]^m$, we instead work with a smaller subset of our ring, namely $S_{D,\Phi}$ given by

$$S_{D,\Phi} = [0,D]^n \cap H_\Phi,$$

where H_Φ is the cyclotomic subspace (see Definition 4.3.3) Then our particular attack will fail because,$(\alpha^n - 1)/(\alpha^q - 1)$, is no longer a valid choice for $x_1(\alpha)$.

Restricting X in this way, we effectively work with $\mathbb{Z}[\alpha]/\langle \Phi_k(\alpha)\rangle$, rather than with $\mathbb{Z}[\alpha]/\langle \alpha^n - 1\rangle$, because $(\mathbb{Z}[\alpha]\Phi(\alpha))/\langle \alpha^n - 1\rangle \cong \mathbb{Z}[\alpha]/\langle \Phi_k(\alpha)\rangle$ by Proposition

2.1.8. Note that although $\mathbb{Z}[\alpha]/\langle\Phi_k(\alpha)\rangle$ is an integral domain, $\mathbb{Z}_p[\alpha]/\langle\Phi_k(\alpha)\rangle$ need not be, so it may seem that although this modification prevents our particular attack there could be a similar attack using the reducibility of $\Phi(\alpha)$ over $\mathbb{Z}_p[\alpha]$, but, assuming the worst case hardness of some well-studied cyclic lattice problems, we will show that there is not.

6.3. Finding Collisions in $\mathcal{H}(\mathbb{Z}^n_{p(n)}, S_{D(n),\Phi}, m(n))$ is Hard.

Informal Theorem. *Under sufficient (reasonable) hypotheses on D, m, p, ϵ, and γ there is a probabilistic polynomial time reduction from* $\text{subIncSVP}^{\eta_\epsilon}_{\gamma}$ *to finding collisions in $\mathcal{H}(\mathbb{Z}^n_{p(n)}, S_{D(n),\Phi_k}, c)$.*

We have thus far only considered non-probabilistic algorithms, but the necessary modification is a natural one. We will assume an oracle $\mathcal{F}$ that, given a uniformly distributed $A \in \mathbb{Z}^n_{p(n)}$, gives a collision (X, X') with nonnegligible probability. Then we will construct a c', and show that, with nonnegligible probability, c' solves $\text{subIncSVP}^{\eta_{\epsilon(n)}}_{\gamma(n)}(B, \Phi(\alpha), c)$. It is important to recognize the source of the uncertainty in this approach to understand the significance of the result. The probability that c' solves $\text{subIncSVP}^{\eta_{\epsilon(n)}}_{\gamma(n)}(B, \Phi(\alpha), c)$ is not dependent on the instance $(B, \Phi(\alpha), c)$. This is in contrast to, for example, the attack given in section 6.1, where we found collisions in $\mathcal{H}(\mathbb{Z}_p[\alpha]/\langle\alpha^n - 1\rangle, S_{D,\Phi(\alpha)}, m)$ with nonnegligible probability, but the uncertainty was due to that our algorithm would work only for some A, rather than that our algorithm would work for any any instance, but only sometimes. The distinction is important because in the latter case, we are able to amplify the probability of success by repetition, but in the former, we cannot. Then, we were able to invalidate the attack simply by removing those instances on which the attack would be successful. We cannot, however, do something similar in the case of Theorem 6.3.7 in order to invalidate our result. This is why this theorem in fact proves that the hash functions $\mathcal{H}(\mathbb{Z}_p[\alpha]/\langle\alpha^n - 1\rangle, S_{D,\Phi(\alpha)}, m)$ have desirable cryptographic properties.

The proof of this theorem will go by way of several lemmas concerning an explicitly constructed value of c' as a candidate solution for a particular instance of $\text{subIncSVP}^{\eta_{\epsilon(n)}}_{\gamma(n)}$.

For an instance $(B, \Phi(\alpha) = (\alpha^n - 1)/\Phi_k, c)$ of $\text{subIncSVP}^{\eta_\epsilon}_{\gamma}$, and assuming an oracle $\mathcal{F}$ that finds collisions in $\mathcal{H}(\mathbb{Z}^n_p, S_{D,\Phi(\alpha)}, m)$ with non-negligible probability (that is, whose decay is at most $1/q(n)$ for some polynomial q), we construct (in polynomial time) a vector c' as follows:

Algorithm 6.3.1.

(1) Let B' be a basis[4] for $\mathcal{L}(B) \cap H$, which is itself a cyclic lattice. B' can be computed easily because we do not require that it be short.
(2) For each integer $i \in [1, m]$,
   - Generate $v_i \in \mathcal{L}(B) \cap H \cap \mathcal{P}(\text{Rot}^d(c))$ uniformly.
   - Generate noise $y_i \in H$ from $D_{H,s}$ for $s = \|c\|/\gamma(n)$, and let $y'_i \in \mathcal{P}(\mathcal{L}(B'))$ with $y'_i - y_i \in \mathcal{L}(B')$.
   - Choose $b_i = (b^1_i | b^2_i)$ for $b^1_i \in \mathbb{R}^d$ and $b^2_i \in \mathbb{R}^{n-d}$ as follows: Choose $b^2_i = ((b_i)_d, \cdots, (b_i)_{n-1})$ uniformly from $[0, 1)^{n-d}$. and let $w_i = \text{Rot}^n(c)(0, \cdots, 0, (b_i)_d, \cdots, (b_i)_{n-1})$.

[4]The paper [8] omits B' and incorrectly uses B in its place. The natural fix for this can be found at [7].

Then let $G \in \mathbb{R}^{d\times n}$ so that $G\mathrm{Rot}^d(c) = \mathrm{id}_d$ the identity in $\mathbb{R}^{d\times d}$. Such a G exists by Proposition **??**, and it can be computed in polynomial time by Gaussian elimination. Then let $b_i^1 = ((b_i)_0, \cdots, (b_i)_{d-1}) = G(v_i + y_i - w_i)$.

- Let $a_i = \lfloor b_i \cdot p \rceil$.

(3) Let $A = (a_1 \pmod p, \cdots, a_m \pmod p)$, and give A to $\mathcal{F}$, yielding a collision (X, X'). Then let $Z = X - X'$.
(4) Output the vector

$$\begin{aligned} c' &= \sum_{i=1}^{m} [(v_i + y_i' - y_i) \otimes z_i] - c \otimes \frac{\sum_{i=1}^{m} a_i \otimes z_i}{p} \\ &= \sum_{i=1}^{m} \left[\left(v_i + y_i' - y_i - \frac{c \otimes a_i}{p} \right) \otimes z_i \right]. \end{aligned}$$

Lemma 6.3.2. *Under the hypotheses of Theorem 6.3.7,* $\mathrm{Rot}^n(c) \cdot b_i = v_i - y_i'$

Proof. We write b_i as $(b_i^1|0, \cdots, 0) + (0, \cdots, 0|b_i^2)$. Then

$$\begin{aligned} \mathrm{Rot}^n(c) \cdot b_i &= \mathrm{Rot}^n(c) \cdot (b_i^1|0, \cdots, 0) + \mathrm{Rot}^n(c)(0, \cdots, 0|b_i^2) \\ &= \mathrm{Rot}^n(c) \cdot (b_i^1|0, \cdots, 0) + w_i \\ &= \mathrm{Rot}^d(c) \cdot G \cdot (v_i + y_i' - w_i) + w_i, \end{aligned}$$

from which we want to show that

$$\mathrm{Rot}^d(c) \cdot G \cdot (v_i + y_i' - w_i) = v_i + y_i' - w_i.$$

But the image of $\mathrm{Rot}^n(c)$ is equal to the span of the lattice $\mathcal{L}(B')$ because $\left\{\mathrm{rot}^j(c) : 0 \le j < d\right\}$, which are the first d columns of $\mathrm{Rot}^n(c)$, is linearly independant by **??**, and each rotation of c is in $\mathcal{L}(B')$ because B' is cyclic. Also, G is surjective because any $v \in \mathbb{R}^d$ is equal to $G(\mathrm{Rot}^n(c)v)$. Then the image of $\mathrm{Rot}^n(c)G$ is the span of the lattice $\mathcal{L}(B')$, and there is some v in $\mathrm{span}(\{\mathrm{Rot}^n(c)\})$ so that

$$\mathrm{Rot}^d(c) \cdot G \cdot v = v_i + y_i' - w_i.$$

Now, G is injective over the span of $\mathrm{Rot}^d(c)$ because $G\mathrm{Rot}^d(c) = \mathrm{id}_d$. Then

$$Gv = G\mathrm{Rot}^d(c) \cdot G \cdot v = G \cdot (v_i + y_i' - w_i),$$

and by the injectivity of G, we have $v = v_i + y_i' - w_i$. □

Lemma 6.3.3. *Under the hypotheses of Theorem 6.3.7, the probability that $\mathcal{F}$ returns a valid collision in step 3 in the algorithm 6.3.1 is nonnegligible. In particular,*

$$\Pr[f_A(X) = f_A(X')] \ge \frac{1}{q(n)} - m(n)\epsilon(n)/2.$$

Proof. By Proposition 5.1.6,it will be sufficient to bound $\Delta\left(A, U(\mathbb{Z}_p^{m\times n})\right)$ by $m\epsilon/2$. But we will show that $\Delta\left(a_i \pmod p, U(\mathbb{Z}_p^n)\right) < \epsilon/2$, so that

$$\Delta\left(A, U(\mathbb{Z}_p^{m\times n})\right) \le \sum_{1}^{m} \Delta\left(a_i \pmod p, U(\mathbb{Z}_p^n)\right) \le \frac{m\epsilon}{2}.$$

But $a_i \pmod p = \lfloor (b_i \pmod 1) \cdot p \rceil$ because $a_i = \lfloor pb_i \rceil$, so

$$\Delta\left(a_i \pmod p, U(\mathbb{Z}_p^n)\right) \le \Delta\left(b_i \pmod 1, U([0,1))^n\right).$$

We consider the construction $b_i = (b_i^1 | b_i^2)$. By construction, b_i^2 is uniform over $[0,1)^{n-d}$, so by Proposition 5.1.4,

$$\begin{aligned}\Delta\left(b_i \pmod 1, U([0,1)^n)\right) &\leq \Delta\left(b_i^1 \pmod 1, U([0,1))^d\right) + \Delta\left(b_i^2 \pmod 1, U([0,1))^{n-d}\right) \\ &= \Delta\left(b_i^1 \pmod 1, U([0,1))^d\right).\end{aligned}$$

By construction $b_i^1 = G(v_i + y_i' - w_i) = G(v_i + y_i') - G(w_i)$ and w_i was constructed injectively from b_i^2, and G is injective, so since b_i^2 is uniform over $[0,1)^{n-d}$, then $G(w_i)$ is unifom over the values it can take. Then

$$\Delta\left(b_i^1 \pmod 1, U([0,1))^n\right) = \Delta\left(G(v_i + y_i') \pmod 1, U([0,1))^n\right).$$

Intuitively, this is true because adding $G(w_i)$ permutes $G(v_i + y_i')$ nicely in $\mathbb{R}^n \pmod 1$. Now by Proposition 5.1.5,

$$\begin{aligned}\Delta\left(G(v_i + y_i') \pmod 1, U([0,1))^n\right) &\leq \Delta\left(\mathrm{Rot}^d(c) G(v_i + y_i') \pmod 1, U(\mathrm{Rot}^d(c)[0,1)^n)\right) \\ &= \Delta\left(v_i + y_i', U(\mathcal{P}(\mathrm{Rot}^d(c)))\right).\end{aligned}$$

Now, v_i is uniform over $\mathcal{L}(B') \cap \mathcal{P}(\mathrm{Rot}^d(c))$, and $\Delta\left(y_i', U(\mathcal{P}(\mathcal{L}(B')))\right) \leq \epsilon/2$ by Lemma 5.1.8.

Let $\{u_1, \cdots, u_k\} = \mathcal{L}(B') \cap \mathcal{P}(\mathrm{Rot}^d(c))$, so that v_i is uniform over $\{u_1, \cdots, u_k\}$. Then $v_i + y_i'$ is almost uniform over $\bigcup (\mathcal{P}(\mathcal{L}(B')) + u_i)$, which is partitioned by $\{\mathcal{P}(\mathcal{L}(B')) + u_j\}$, because $v_i + y_i$ is in $\mathcal{P}(\mathcal{L}(B')) + v_i$, and given v_i fixed, is almost uniform over that translate. That is,

$$\Delta\left(v_i + y_i', U\left(\bigcup (\mathcal{P}(\mathcal{L}(B')) + u_i)\right)\right) \leq \epsilon/2.$$

But then

$$\begin{aligned}&\Delta\left((v_i + y_i') \left(\mathrm{mod}\ \mathcal{P}(\mathrm{Rot}^d(c))\right), U\left(\mathcal{P}(\mathrm{rot}^d(c))\right)\right) \\ &\quad = \Delta\left((v_i + y_i') \left(\mathrm{mod}\ \mathcal{P}(\mathrm{Rot}^d(c))\right), U\left(\bigcup (\mathcal{P}(\mathcal{L}(B')) + u_i) \left(\mathrm{mod}\ \mathcal{P}(\mathrm{Rot}^d(c))\right)\right)\right) \\ &\quad = \Delta\left(v_i + y_i', U\left(\bigcup (\mathcal{P}(\mathcal{L}(B')) + u_i)\right)\right) \leq \epsilon/2.\end{aligned}$$

Putting everything together, then

$$\Delta\left(A, U(\mathbb{Z}_p^{m \times n})\right) \leq \frac{\epsilon}{2},$$

so by Proposition 5.1.6,

$$\Pr\left[f_A(X) = f_A(X')\right] \geq \frac{1}{q(n)} - \epsilon(n) m(n),$$

which is nonnegligible. □

Lemma 6.3.4. *Under the hypotheses of Theorem 6.3.7, if $\mathcal{F}$ returns a valid collision in step 3, c' returned by the algorithm 6.3.1 is in the lattice $\mathcal{L}(B')$.*

Proof. We will show that each of the terms of the first expression for c' is in $\mathcal{L}(B')$. Indeed, both v_i and $y_i' - y_i$ are in $\mathcal{L}(B')$ by construction, and $z_i \in \mathbb{Z}^n$ by the definition of $\mathcal{F}$. Then $(v_i + y_i' - y_i) \otimes z_i$ is also in $\mathcal{L}(B')$ because $\mathcal{L}(B')$ is a cyclic lattice. For the term $c \otimes \frac{1}{p} \sum a_i \otimes z_i$, we'll show that $\frac{1}{p} \sum a_i \otimes z_i \in \mathbb{Z}^n$, so that we have the convolution of $c \in H$ with an integer vector, which will also be in $\mathcal{L}(B')$. But by the construction of the z_i, $a_i(\alpha) \cdot z_i(\alpha) = 0$ in $\mathbb{Z}_p[\alpha]/\langle \alpha^n - 1 \rangle$, so $\frac{1}{p} a_i(\alpha) \cdot z_i(\alpha) \in \mathbb{Z}[\alpha]/\langle \alpha^n - 1 \rangle$, and $\frac{1}{p} a_i \otimes z_i \in \mathbb{Z}^n$. □

Lemma 6.3.5. *Under the hypotheses of Theorem 6.3.7,* $\Pr[c' \neq 0] \geq 3/4$*, conditioned on that* $\mathcal{F}$ *return a valid collision in step 3 of the algorithm 6.3.1.*

Proof. Since $z \neq 0$, we assume witout loss of generality that $z_1 \neq 0$. Then $c = 0$ exactly when

$$\left(v_1(\alpha) + y_1'(\alpha) - y_1 + \frac{c(\alpha)a_1(\alpha)}{p}\right) z_1(\alpha) = \sum_{j=2}^{m} \left(v_j(\alpha) + y_j'(\alpha) - y_j + \frac{c(\alpha)a_j(\alpha)}{p}\right) z_j(\alpha)$$

in $\mathbb{Z}[\alpha]/\langle \alpha^n - 1\rangle$, and we call the right hand side of this equality $h(\alpha)$. But because everything is in $\mathbb{Z}[\alpha]\Phi(\alpha)$, this occurs if and only if

$$\left(v_1(\alpha) + y_1'(\alpha) - y_1 + \frac{c(\alpha)a_1(\alpha)}{p}\right) z_1(\alpha) = h(\alpha)$$

in $\mathbb{Z}[\alpha]/\langle \Phi_k(\alpha)\rangle$. But z_1 cannot be zero in $\mathbb{Z}[\alpha]/\langle \Phi_k(\alpha)\rangle$ because if it were, because $\Phi(\alpha)$ divides $z_1(\alpha)$, then $z_1(\alpha) = \Phi(\alpha)\Phi_k(\alpha)r(\alpha)$ for some $r(\alpha)$, but $\Phi(\alpha)\Phi_k(\alpha) = \alpha^n - 1$, so $z_1(\alpha) = 0$ in $\mathbb{Z}[\alpha]/\langle \alpha^n - 1\rangle$, contrary to assumption. Then because $\mathbb{Z}_p[\alpha]/\langle \alpha^n - 1\rangle$ is an integral domain, there is at most one $w(\alpha)$ so that $w(\alpha)z_1(\alpha) = h(\alpha)$, and we will bound the probability that $y_1'(\alpha) - y_1(\alpha) = w(\alpha)$.

If there is no such w, then certainly

$$\left(v_1(\alpha) + y_1'(\alpha) - y_1 + \frac{c(\alpha)a_1(\alpha)}{p}\right) z_1(\alpha) \neq h(\alpha),$$

and c cannot be zero, so we assume that there is such a $w(\alpha)$, and we bound the probability that

$$y_1'(\alpha) - y_1(\alpha) = w(\alpha) - v_1(\alpha) - \frac{c(\alpha)a_1(\alpha)}{p}$$

in $\mathbb{Z}[\alpha]/\langle \Phi_k(\alpha)\rangle$. In fact, v_1 was chosen independently from y_1, and w and a_1 depend only on y_1', not on y_1, so for any fixed y_1', $y_1' - y_1$ and $w - v_1 - c \otimes a_1/p$ are independent. Then note that for a y_1' fixed, $y_1' = y_1$ is distributed according to $D_{\mathcal{L}(B'),s,-y_1'}$ because y_1 is distributed according to $D_{H_\Phi,s,0}$. Then

$$\begin{aligned}\Pr\left[y_1' - y_1 = w - v - \frac{c \otimes a}{p}\right] &\leq \max\left\{\Pr[u = y_1' - y_1] : u \in \mathcal{L}(B')\right\} \\ &\leq \max\left\{\Pr\left[D_{\mathcal{L}(B'),s,-y_1'}(w)\right] : w \in \mathcal{L}(B')\right\},\end{aligned}$$

which, by Lemma 5.1.9, is at most $s^{-d}(1+\epsilon)(1-\epsilon)$. But we have already argued that if $c = 0$, then $y_1' - y_1 = w - v_1 - c \otimes a_1/p$, so

$$\begin{aligned}\Pr[c = 0] &\leq \Pr\left[y_1' - y_1 = w - v_1 - \frac{c \otimes a_1}{p}\right] \\ &\leq s^{-d}\frac{1+\epsilon}{1-\epsilon} \\ &= (2\gamma\|c\|)^{-d}\frac{1+\epsilon}{1-\epsilon} \\ &\leq \frac{1}{8} \cdot \frac{1+\epsilon}{1-\epsilon} \leq \frac{1}{4}\end{aligned}$$

for large n. We have assumed without loss of generality that $d \geq 3$, because there are known efficient algorithms for $d = 1$ and $d = 2$, so in these cases, the reduction from subIncSVP to $\mathcal{H}(\mathbb{Z}_p^n, S_{D,\Phi_k}, m)$ is trivial. □

Lemma 6.3.6. *Under the hypotheses of Theorem 6.3.7,* $\Pr\left[\|c'\| \leq \|c\|/2\right] \geq 1/2$, *conditioned on that* $\mathcal{F}$ *return a valid collision in step 3 of the algorithm 6.3.1.*

Proof. We assume throughout the proof that (X, X') is a valid collision. We will show that

$$\Pr\left[\|c'\| \geq \|c\| \left(\frac{mn^{5/2}D}{p} + \frac{4mnD}{\gamma}\right)\right] \leq \frac{1}{2}$$

By showing

$$\|c'\| \leq \sum_{i=0}^{m-1} \left\| \left(v_i + y_i' - \frac{c \otimes a_i}{p}\right) \otimes z_i \right\| + \sum_{i=0}^{m-1} \|y_i \otimes z_i\|, \tag{1}$$

$$\left\| \left(v_i + y_i' - \frac{c \otimes a_i}{p}\right) \otimes z_i \right\| \leq \frac{n^{5/2}D}{p}, \tag{2}$$

and

$$\Pr\left[\|y_i \otimes z_i\| \geq \|c\| \frac{4mnD}{\gamma}\right] \leq \frac{1}{2}. \tag{3}$$

Then by (2),

$$\sum_{i=0}^{m-1} \left\| v_i + y_i' + \frac{c \otimes a_i}{p} \right\| \leq \frac{mn^{5/2}D}{p},$$

and by (3)

$$\Pr\left[\sum_{i=0}^{m-1} \|y_i \otimes z_i\| \geq \|c\| \frac{4mnD}{\gamma}\right] \leq \frac{1}{2}.$$

By the hypotheses $p(n) \geq 8mn^{5/2}D$ and $\gamma n \geq 16mnD$,

$$\frac{1}{2} \geq \frac{mn^{5/2}D}{p} + \frac{4mnD}{\gamma}.$$

Then

$$\Pr\left[\|c'\| \geq \|c\|/2\right] \leq \Pr\left[\|c'\| \geq \|c\| \left(\frac{mn^{5/2}D}{p} + \frac{4mnD}{\gamma}\right)\right] \leq \frac{1}{2}.$$

In fact, (1) follows from an application of the triangle inequality to the second expression for c' given in Algorithm 6.3.1.

For (2), $v_i + y_i' = \mathrm{Rot}^n(c)$ by the construction of b_i and $c \otimes a_i = \mathrm{Rot}^n(c)a_i$ by Proposition **??**. Then

$$v_i + y_i' - \frac{c \otimes a_i}{p} = \mathrm{Rot}^n(c)b_i - \frac{\mathrm{Rot}^n(c)a_i}{p} = \tfrac{1}{p}\mathrm{Rot}^n(c)(pb_i - a_i).$$

But $\|pb_i - a_i\|_\infty \leq 1/2$ by choice of a_i, so $\|pb_i - a_i\|_2 \leq \sqrt{n}/2$ and $\mathrm{Rot}^n(c)$ has jth row $\mathrm{rot}^j(c)$, so

$$\begin{aligned}\left\|v_i + y_i' + \frac{c \otimes a_i}{p}\right\|_\infty &= \tfrac{1}{p}\left\|\mathrm{Rot}^n(c)(pb_i - a_i)\right\|_\infty \\ &= \tfrac{1}{p}\max_j\left\{\left|\left\langle \mathrm{rot}^j(c), pb_i - a_i\right\rangle\right|\right\} \\ &\leq \tfrac{1}{p}\max_j\left\{\|\mathrm{rot}^n(c)\|_2 \cdot \|pb_i - a_i\|_2\right\} \\ &= \frac{\|c\|_2 \cdot \|pb_i - a_i\|_2}{p} \\ &\leq \frac{\sqrt{n}\,\|c\|}{2p},\end{aligned}$$

and

$$\left\|v_i + y_i + \frac{c \otimes a_i}{p}\right\|_2 \leq \sqrt{n}\left\|v_i +_i + \frac{c \otimes a_i}{p}\right\|_\infty \leq \frac{n\,\|c\|}{2p}.$$

Now, because $X, X' \in [0, D)^{n \times m}$, we have $\|z_i\|_\infty \leq 2D$, and $\|z_i\|_2 \leq 2\sqrt{n}D$. Finally, by the commutativity of $\otimes$ (inherited from the commutativity of multiplication in $\mathbb{Z}[\alpha]/\langle \alpha^n - 1\rangle$), and Proposition **??**,

$$\begin{aligned}\left\|\left(v_i + y_i' + \frac{c \otimes a_i}{p}\right) \otimes z_i\right\|_\infty &= \left\|\mathrm{Rot}^n z_i(v_i + y_i' + \frac{c \otimes a_i}{p}\right\|_\infty \\ &= \max_j\left\{\left|\left\langle \mathrm{rot}^j(z_i), \left(v_i + y_i' + \frac{c \otimes a_i}{p}\right)\right\rangle\right|\right\} \\ &\leq \|z_i\|_2 \cdot \left\|v_i + y_i' + \frac{c \otimes a_i}{p}\right\|_2 \\ &\leq \|c\|\,\frac{n^{3/2}D}{p},\end{aligned}$$

and

$$\begin{aligned}\left\|\left(v_i + y_i' + \frac{c \otimes a_i}{p}\right) \otimes z_i\right\|_2 &\leq \sqrt{n}\left\|\left(v_i + y_i' + \frac{c \otimes a_i}{p}\right) \otimes z_i\right\|_\infty \\ &\leq \|c\|\,\frac{n^2 D}{p}.\end{aligned}$$

For the equation (3), we write $y_i \otimes z_i = ((y_i - y_i') - (-y_i')) \otimes z_i$, and notice that, with y_i' fixed, $y_i - y_i'$ is distributed according to $D_{\mathcal{L}(B'),s,-y_i'}$ because y_i is distributed according to $D_{\mathcal{L}(B'),s,0}$ by construction, and recall that, as above, $\|z_i\| \leq \sqrt{n}D$. But then by Lemma 5.1.10, holding y_i fixed,

$$\begin{aligned}\Pr\left[y_i \otimes z_i \geq \|c\|\,\frac{4nD}{\gamma}\right]_{y_i'} &= \Pr\left[((y_i - y_i') - (-y_i')) \otimes z_i \geq \|c\|\,\frac{4nD}{\gamma}\right]_{y_i'} \\ &\leq \frac{s\sqrt{d}\,\|z_i\|}{4\,\|c\|\,nD/\gamma} \\ &\leq \frac{s\sqrt{d}(\sqrt{n}D}{4\,\|c\|\,nd/\gamma} \leq \frac{s\gamma}{4\,\|c\|} = \frac{1}{2}.\end{aligned}$$

□

Theorem 6.3.7. *For any polynomially bounded functions $D(n)$, $m(n)$ and $p(n)$ such that $p(n) \geq 8n^{5/2}m(n)D(n)$, negligible function $\epsilon(n)$, and approximation factor $\gamma(n) \geq 16nm(n)D(n)$, there is a probablistic polynomial time reduction from the instances $(B, \Phi(\alpha) = (\alpha^n - 1)/\Phi_k, c)$ of $\text{subIncSVP}^{\eta_{\epsilon(n)}}_{\gamma(n)}$ for $k|n$ to finding collisions in $\mathcal{H}(\mathbb{Z}^n_{p(n)}, S_{D(n),\Phi(\alpha)}, m(n))$*

Proof. Algorithm 6.3.1 constructs c' in polynomial time. Assuming that $\mathcal{F}$ returns a valid collision, c' is a solution to $\text{subIncSVP}^{\eta_\epsilon}_{\gamma}$ with probability at least $1/4$ by Boole's inequality and Lemmas 6.3.5 and 6.3.6. By Lemma 6.3.3, the probability that $\mathcal{F}$ returns a valid collision is nonnegligible, so c' solves $\text{subIncSVP}^{\eta_\epsilon}_{\gamma}$ with nonnegligible probability. □

References

[1] Miklós Ajtai. "Generating Hard Instances of Lattice Problems (Extened Abstract)". In: *STOC96* (1996).

[2] David Dummit and Richard Foote. *Abstract Algebra*. Prentice Hall, 1990. ISBN: 0130047716.

[3] Ralph Merkle and Martin Hellman. "Hiding information and signatures in trapdoor knapsacks". In: *IEEE Transactions Information Theory* 24 (1978), pp. 525–530.

[4] Daniele Micciancio. "Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions". In: *Proc. 43rd Annual Symposium on Foundations of Computer Science* (2002).

[5] Daniele Micciancio. "The shortest vector problem is NP-hard to approximate to within some constant". In: *SIAM Journal on Computing* 30 (2001), pp. 2008–2035.

[6] Daniele Micciancio and Oded Regev. "Worst-case to average case reductions based on Gaussian meassures". In: *SIAM Journal on Computing* 34 (2005), pp. 267–302.

[7] Chris Peikert. *Collisions in the cyclotomic knapsack function*. StackExchange. URL: `http://crypto.stackexchange.com/a/35597` (visited on 06/26/2016).

[8] Chris Peikert and Alon Rosen. "Lattices that Admit Logarithmic Worst Case to Average Case Connection Factors". In: *Proc. of TCC06* (2006).

[9] Oded Regev. "New lattice-based cryptographic constructions". In: *J. ACM* 51 (2004), pp. 899–942.

[10] Adi Shamir. "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem". In: *IEEE Transactions on Information Theory* 30 (1984), pp. 699–704.