Lattices and Homomorphic Encryption, Spring 2013 Instructors: Shai Halevi, Tal Malkin

Ideal Lattices and NTRU

April 23-30, 2013 Scribe: Kina Winoto

1 Algebraic Background (Reminders)

Definition 1. A *commutative ring with unity* $(R, +, \times)$ satisfies the following properties:

- $(R, +)$ is an abelian group;
- $(R, \times)$ is associative, commutative and has unity;
- $\times$ distributes over $+$

(Similar to a field, except not every non-zero element has an inverse)

Examples: $\mathbb{Z}, \mathbb{Z}[x]$

Definition 2. An *ideal* $I \subseteq R$ is a subset that satisfies:

- $(I, +)$ is a subgroup of $(R, +)$;
- I is closed under multiplication by R ($i \times r \in I \,\forall i \in I,\, r \in R$).

Definition 3. We say that an ideal is *finitely generated* if there is a finite set of generators $\{i_1, \ldots, i_t\}$ s.t. $I = \{\sum r_j \times i_j\} = \langle i_1, \ldots, i_t \rangle$.

Definition 4. For a ring R and an ideal I we can define the *quotient ring* to be the set $Q = R/I = \{[r]_I : r \in R\}$ where $[r]_I = \{r + i \colon i \in I\}$.

Examples:
$\mathbb{Z}_5 = \mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}[x]/\langle x^4+1\rangle$, $\mathbb{Z}_5[x]/\langle x^4+1\rangle = \mathbb{Z}[x]/\langle 5, x^4+1\rangle$.

We will mostly be interested in rings of the forms $\mathbb{Z}[x]/\langle f\rangle$ and $\mathbb{Z}_p[x]/\langle f\rangle$ for some monic polynomial f. Note that if f is not irreducible, then $\mathbb{Z}[x]/\langle f\rangle$ has zero divisors: $a \times b = f$, $0 < \deg a, b < \deg f$, therefore $a, b \in \mathbb{Z}[x]/\langle f\rangle$. Thus we will mostly be interested in quotient rings over irreducible polynomials.

We can represent an element of $R = \mathbb{Z}[x]/\langle f\rangle$ by the vector of its coefficients:

$$\begin{aligned} (\deg \le n-1)\text{-polynomial } g \in R &\iff \text{vector } \vec{g} \in \mathbb{Z}^n \\ \text{additive subgroup of } R &\iff \text{lattice in } \mathbb{Z}^n \end{aligned}$$

Other representations are also possible, but we do not deal with them here.

Definition 5. A lattice $\Lambda \in \mathbb{Z}^n$ is an *ideal lattice* if there exist a ring $R = \mathbb{Z}[x]/\langle f\rangle$ and an ideal $I \subseteq R$ s.t. Λ is associated with I.

For example:

$$\Lambda = \left\{\text{coeff. vector of } g\left(\right) \mid \exists h\left(\right) \text{ s.t. } g(x) = h(x) \times \left(x^2+5\right) \pmod{\left(x^4+1, 8\right)}\right\} \subset \mathbb{Z}^4$$

is associated with the ideal

$$\left\langle x^2+5\right\rangle \subset \mathbb{Z}_8[X]/\left\langle x^4+1\right\rangle$$

Lemma 1. *$\mathbb{Z}[X]$ is a Unique Factorization Domain (UFD)*

Proof. Follows since (a) $\mathbb{Z}$ is a UFD; and (b) if a ring R is a UFD then so is $R[X]$. □

Corollary 1. *If $f \in \mathbb{Z}[X]$ is irreducible and $f \mid g \times h$ then $f \mid g$ or $f \mid h$.*

Lemma 2. *If f is irreducible and $I \subseteq \mathbb{Z}[X] / \langle f \rangle$ is a non-zero ideal then Λ_I is a full-rank lattice in $\mathbb{Z}^n$.*

Proof. Let $R = \mathbb{Z}[X]/\langle f \rangle$ and $I \subseteq R$ and let $g \in I$ be a non-zero element. We will show that the coefficient vectors of $\{g, X \times g, \ldots, X^{n-1} \times g\} \subset R$ are linearly independent. Assume $\sum h_i \cdot (X^i \times g(X)) = 0 \in R$, and we show that the h_i's must be all be zeros. Since the coefficient vectors of $X^i \times g(X)$ are all integer vectors, then we can assume w.l.o.g. that the h_i's are all rational coefficients, and by multiplying by the common denominator we can assume that they are in fact integers.

Denote $h(X) = \sum h_i X^i$. Then $h \times g = 0$ in the ring, (which is the same as $f \mid h \times g$, since we are working modulo f). Thus by the previous corollary, and since $g \neq 0$, we have that $h = 0$ in the ring, so $h_i = 0$ for all i. □

Definition 6. For any polynomial f we define:

$$\theta(f) = \max_{a \in \mathbb{Z}[X]/\langle f \rangle,\, i < \deg f} \frac{\left\| X^i \times a \bmod f \right\|_\infty}{\|a\|_\infty}$$

For any two polynomials $a, b \in \mathbb{Z}[X] / \langle f \rangle$:

$$\|a \times b \bmod f\|_\infty \leq \|a\|_\infty \cdot \|b\|_\infty \cdot n\theta(f)$$

Lemma 3. *If f is an n-degree irreducible polynomial and $I \subseteq \mathbb{Z}[X] / \langle f \rangle$ is a non-zero ideal then*

$$\lambda_n^\infty(\Lambda_I) \leq \lambda_1^\infty(\Lambda_I) \cdot \theta(f)$$

Proof. Let $\vec{g}$ be the shortest vector in Λ, and $g(X)$ the corresponding polynomial. Then the vectors that correspond to $\{g_i(X) = X^i \times g(X)\}$ are linearly independent. Clearly,

$$\lambda_n^\infty(\Lambda_I) \;\leq\; \max_{i=0}^{n-1} \|\vec{g}_i\|_\infty \;\leq\; \|\vec{g}\|_\infty \cdot \theta(f) \;=\; \lambda_1^\infty(\Lambda_I) \cdot \theta(f)$$

□

2 The Shortest Vector Problem in Ideal Lattices

Just as in any lattice, we can ask how easy / hard it is to find a (good approximaiton of) the shortest vector in the lattice. Note that if $\theta(f)$ is small, then by the previous lemma estimating the *size* of the smallest vector is easy:

$$\begin{aligned}\frac{1}{\sqrt{n}}\lambda_1(\Lambda) &\leq \det(\Lambda)^{1/n}\\ &\leq \lambda_n(\Lambda)\\ &\leq \sqrt{n}\lambda_n^\infty(\Lambda)\\ &\leq \sqrt{n}\lambda_1^\infty(\Lambda)\cdot\theta(f)\\ &\leq \sqrt{n}\lambda_1(\Lambda)\cdot\theta(f)\end{aligned}$$

Still, finding the shortest vectors themselves seems hard. In particular, we don't know of methods that do much better on ideal lattices than on regular lattices. (Sometimes we can do slightly better, for example in [GS02] they are able to reduce an ideal lattice problem in dimension $2n$ to a non-ideal lattice problem in dimension n.)

2.1 The f-SVP$_\gamma$ Problem

For a family of polynomials $f = \{f_n\}$ (with $\deg f_n = n$): Given a lattice Λ_I corresponding to ideal $I \subseteq \mathbb{Z}[x] / \langle f_n \rangle$, find a non-zero vector $\vec{v} \in \Lambda_I$ s.t. $\|\vec{v}\| \leq \gamma \lambda_1(n)$. (Can also be stated with l_∞ or any other l_p norm).

Below we will typically use $f_n(x) = x^n + 1$, where n is a power of 2. Thus $f_n(x)$ is irreducible. Also, $\theta(f) = 1$ because:

- For any $g(x)$ with coefficient vector $(g_1, g_2, \ldots, g_n)$, we have that the coefficient vector of $x \times g(x)$ is $(-g_n, g_1, \ldots, g_{n-1})$.
- This means that lattices over $\mathbb{Z}[x] / \langle f_n \rangle$ are "almost circular": If $(v_i) \in \Lambda_I$, then also $\left(\text{sign}(i-k-1) \cdot v_{i-k \pmod n}\right) \in \Lambda_I$.

3 The NTRU Cryptosystem [HPS98]

Below we describe a variant similar to [SS11] and [LTV12]. This variant is also somewhat similar to Regev's crypto system with dimension 1, but it uses LSB to encode the message rather MSB. Namely, whereas in Regev's scheme we recover upon decryption something like small-error + $m\frac{q}{2}$, in NTRU we get $2 \cdot \text{small-error} + m$. (We can easily get a variant of Regev with LSB encoding, but getting a variant of NTRU with MSB encoding is a little tricky.) This NTRU variant is defined as follows:

Parameters:

- n - security parameter
- q - modulus
- error distribution

We assume that n is power of two so $x^n + 1$ is irreducible, we consider $R = \mathbb{Z}[X]/(x^n + 1)$ and $R_q = R(\text{mod } q)$, i.e. $R_q = \mathbb{Z}_q[X]/(x^n + 1)$. We assume that q is odd (and sometimes it is even convenient to assume $q = 1 \pmod{2n}$).

Key Generation. Choose at random the coefficients for the polynomials g, f' from the error distribution (so coefficients are small): $\vec{g}, \vec{f'} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$. (Note that $\vec{g}, \vec{f'}$ are now the coefficient vectors of functions g, f'.) Set $f = 2f' + 1$ so that f is small and $f = 1 \pmod 2$. If f is not irreducible in R_q, then try again. (If f was random in R_q, it would have been invertible with probability at least $1 - \frac{n}{q}$. For small f this still holds with high probability, see proof in [SS11]. The public key is $h = g/f \in R_q$ and the secret key is f.

Note the analogy between this cryptosystem and Regev's: In Regev's system, we have public key A, secret key $\vec{s}$, and sA=small. In NTRU, we have public key h, secret key f, and $f \times h = g =$ small.

Enccypt$_h(m \in R_2)$. Choose a small element $\vec{s} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$. The ciphertext is $c = 2s \times h + m \bmod q$.

Decrypt$_f(c)$. Set $a = f \times c \bmod q$, and output $a \bmod 2$. (In fact this is exactly the same procedure as in the LSB-variant of Regev's cryptosustem, except product is in the ring R_q.)

Correctness. Since s, g, m, f are all small then $a = 2s \times g + m \times f$ holds also in R, not just in R_q. Hence $a = m \times f = m \times (2f' + 1) = m \pmod 2$.

Security. We don't have much to say about the security of the variant above, except that we do not know how to break it. (We also do not know how to reduce its security to "better known" hardness assumptions.)

Note, however, that decryption works even if we encrypt using $c = 2(s \times h + e) + m$, for a small e. In this case we would get $f \times c = 2s \times g + 2e \times f + f \times m = m \pmod 2$. This version is secure if $(h, s \times h + e)$ is pseudorandom, which is similar to "ring-LWE" except h is not uniformly random.

- But if you also assume that $h = g/f$ itself is pseudorandom (this is called the "NTRU assumption"), then you get security. So "NTRU Assumption + ring-LWE" $\Rightarrow$ the NTRU cryptosystem is secure.

[SS11] proved that if $\sigma > q^{\frac{1}{2}+\varepsilon}$ (and also n is a power of two and $q = 1 \bmod 2n$), then choosing f, g – where $\vec{f}, \vec{g} \leftarrow \mathcal{D}_{\mathbb{Z}^n,\sigma}$ – to be invertible in R_q and setting $h = g/f$, h is close to uniform among all invertible elements. Hence with these parameters you get security under ring-LWE by itself. (We note that these parameters will not be enough to get homomorphic encryption, though.)

3.1 Homomorphic NTRU

Note that c is a valid encryption of m if $f \times c = 2e + m$ for small e. This is the same as the expression you get for the LSB variant of Regev's scheme, and indeed you can get a homomorphic scheme from NTRU in the same way that you do for Regev's cryptosystem. As usual, additive homomorphism is easy: If $f \times c_i = 2e_i + m_i$, $i = 1, 2$ then $f \times (c_1 + c_2) = 2(e_1 + e_2 + e') + (m_1 \oplus m_2)$. Also for multiplicative homomorphism we have

$$\begin{aligned} f^2 \times (c_1 \times c_2) &= (2e_1 + m_1)(2e_2 + m_2) \\ &= 2(2e_1e_2 + m_1e_2 + e_1m_2) + m_1m_2 \;=\; 2e'' + m_1m_2 \end{aligned}$$

The noise doubles on addition, gets squared on multiplication. This is worse than what we had before, where the noise doubles on addition and $\times \mathrm{poly}(n)$ for multiplication. It means that we can only support depth $\Omega(\log\log q)$. This is an artifact of the LSB-encoding method (we have the same issue with the LSB variant of Regev's crytosystem), and we will see how to handle it shortly.

Note also that we do not have the dimension explosion that we had with tensor products in Regev's cryptosystem. The dimension stays 1, but the size of the key grows: $f, f^2, f^4, \ldots$. This too limits the applicability to depth: $\Omega(\log\log q)$. Controlling the secret key growth is done using key-switching. For the other problem we use a different trick called "modulus switching".

Key Switching. We add to the public key an "encryption of f^2 under f", namely w such that $w \times f = 2e + qf^2 \pmod Q$, for $Q = q^2$. Then, given c^* such that $c^* \times f^2 = 2e^* + m \pmod q$, we set $c' = c \times w \bmod Q$. Therefore:

$$\begin{aligned} c' \times f = c^* \times w \times f \;&=\; c^* \times (2e + qf^2) \\ &= (2c^* \times e) + (qc^* \times f^2) \;=\; (2c^* \times e) + q(2e^* + m + kq) \\ &= 2(c^* \times e + qe^*) + qm + kQ \;=\; 2\left(c^* \times e + qe^* + \frac{q-1}{2}m\right) + m \pmod Q \end{aligned}$$

Call $\left(c^* \times e + qe^* + \frac{q-1}{2}m\right) = e'$, where we note that $\|e'\| \ll Q$ since $Q = q^2$, $\|c^*\| \sim q$, and $\|e\|, \|e^*\|, \|m\| \ll q$. So we now have a ciphertext c' valid relative to f and Q.

Modulus switching. Given c' such that $c' \times f = 2e' + m \pmod{Q}$ with $\|e'\| \ll Q$ and $\|f\| \ll q$, we set $c'' = \text{round}(c' \cdot \frac{q}{Q})$, where rounding is done so $c'' = c' \pmod 2$.

Note that $c'' = c' \cdot \frac{q}{Q} + \varepsilon$ where ε is the rounding error, $\|\varepsilon\| \leq 1$. Let k' be the factor of Q, namely $c' \times f - kQ = (c' \times f \bmod Q) = 2e' + m$. Then we have

$$c'' \times f - kq = (\frac{q}{Q} c' \times f + \varepsilon \times f) - \frac{q}{Q} \cdot kQ \ = \ \frac{q}{Q}(c' \times f - kQ) + \varepsilon \times f \ = \ \underbrace{\frac{q}{Q}(\overbrace{2e' + m}^{\ll Q})}_{\ll q} + \underbrace{\varepsilon \times f}_{\ll q}$$

Hence $\|c'' \times f - kq\| \ll q$ and therefore $c'' \times f - kq = (c'' \times f \bmod q)$. But $c'' = c' \pmod 2$ and also $q = Q = 1 \pmod 2$, so $c'' \times f - kq = c' \times f - kQ \pmod 2$. We conclude that $(c'' \times f \bmod q) = (c' \times f \bmod Q) = m \pmod 2$. Hence $c'' \times f = 2e'' + m$, where $\|2e'' + m\| \leq \frac{q}{Q}\|2e' + m\| + \|\varepsilon \times f\|$.

Note: We did not use here that $Q = q^2$; we can modulo switch to any other q' and the "noise term" decreases from $\|2e' + m\|$ to $\leq \frac{q'}{Q}\|2e'_m\| + \|\varepsilon \times f\|$. This can be used to control the noise: start from q_i, then after every multiplication switch from q_i to $q_{i+1} \ll q_i$, decreasing the noise.

Multi-key Homomorphic Encryption [LTV12]. Suppose we have two ciphertexts encrypted relative to two different keys (and the same q): $c_i \times f_i = 2e_i + m_i$ (and recall that $f_i = 2f'_i + 1$), then clearly we get:

$$(c_1 \times c_2) \times f_1 f_2 = 2(2e_1 e_2 + e_1 m_2 + e_2 m_1) + m_1 m_2$$

But also for addition we get:

$$\begin{aligned}(c_1 + c_2) \times f_1 f_2 &= c_1 \times f_1 \times f_2 + c_2 \times f_2 \times f_1 \\ &= (2e_1 + m_1)(2f'_2 + 1) + (2e_2 + m_2)(2f'_1 + 1) \\ &= 2(2e_1 f'_2 + m_1 f'_2 + 2e_2 f'_1 + m_2 f'_1 + e_2) + m_1 + m_2 \\ &= 2e' + (m_1 \oplus m_2)\end{aligned}$$

So we can add/multiply cipher texts relative to different keys, then decrypt using the products of the keys.

Note that if we have a complicated circuit, we can get ciphertexts relative to keys like $f_1^3 \times f_2 \times f_3^5 \ldots$. We can reduce the degree in each f_i separately to 1, by putting in the public key the terms $w[f_i^2 \Rightarrow f_i]$, and reduce everything back to a ciphertext relative to $f_1 \times f_2 \times \ldots \times f_t$, but we cannot reduce anymore without interaction between the key-holders.

References

[GS02] Craig Gentry and Michael Szydlo, *Cryptanalysis of the revised ntru signature scheme*, Advances in Cryptology - EUROCRYPT'02, Lecture Notes in Computer Science, vol. 2332, Springer, 2002, pp. 299–320.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and JosephH. Silverman, *Ntru: A ring-based public key cryptosystem*, Algorithmic Number Theory (JoeP. Buhler, ed.), Lecture Notes in Computer Science, vol. 1423, Springer Berlin Heidelberg, 1998, pp. 267–288.

[LTV12] Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan, *On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption*, Proceedings of the 44th Symposium on Theory of Computing Conference, STOC'12, ACM, 2012, pp. 1219–1234.

[SS11] Damien Stehlé and Ron Steinfeld, *Making ntru as secure as worst-case problems over ideal lattices*, Advances in Cryptology - EUROCRYPT'11, Lecture Notes in Computer Science, vol. 6632, Springer, 2011, pp. 27–47.