An Algorithm for NTRU Problems

Jung Hee Cheon, Jinhyuck Jeong, Changmin Lee

Seoul National University

August 29, 2016

Introduction

- The NTRU encryption algorithm is a lattice-based public key cryptosystem alternative to RSA and ECC.
  - This system is fully accepted to IEEE P1363 standards under the specifications for lattice-based public-key cryptography.
  - Speedy and low memory use.
- The security of it depends on the NTRU problem.

Applications of NTRU problems

- Public key Encryption-NTRU scheme
  - [HPS98]
- Signature Scheme
  - [HHGP+03]
  - [DDLL13]
- Fully Homomorphic Encryption
  - [LATV12]
  - [BLLN13]
- Multilinear Maps
  - [GGH13]
  - [LSS14]
  - [ACLL14]

Notation

- $\mathbb{Z}_q := (-q/2, q/2] \cap \mathbb{Z}$
- $\phi_n(X) := X^n + 1$, where n is a power of two
- $K := \mathbb{Q}[X]/\langle \phi_n(X) \rangle$, $K_i := \mathbb{Q}[X^{2^i}]/\langle \phi_n(X) \rangle$
- $R := \mathbb{Z}[X]/\langle \phi_n(X) \rangle$, $R_i = \mathbb{Z}[X^{2^i}]/\langle \phi_n(X) \rangle$
- $[R]_q := \mathbb{Z}_q[X]/\langle \phi_n(X) \rangle$
- $\mathrm{Gal}(K/F)$: the Galois group of K over F
- For $\mathbf{u} = \sum_{i=0}^{n-1} u_i X^i \in R$,
  - $[\mathbf{u}]_q = \sum_{i=0}^{n-1} [u_i]_q X^i \in [R]_q$
  - $\|\mathbf{u}\| = \sqrt{\sum_{i=0}^{n-1} u_i^2}$
  - $V : R \to \mathbb{Z}^n$ is defined by $V(\mathbf{u}) = (u_0, \cdots, u_{n-1})^T$

NTRU problems

Problem (A variant of NTRU Problem)

Let q be an integer, D, N and B be real numbers.
The NTRU Problem $NTRU_{\phi_n,q,D,N,B}$ is to find $\mathbf{a}$, $\mathbf{b} \in R$ with Euclidean norm smaller than B such that

$$[\mathbf{b}/\mathbf{a}]_q = \mathbf{f}$$

for given a polynomial $\mathbf{f} = [\mathbf{h}/\mathbf{g}]_q$, where $\mathbf{g}$ and $\mathbf{h}$ are sampled from R and have Euclidean norms bounded by D and N, respectively.

Without loss of generality, we can assume $\|\mathbf{h}\| \geq \|\mathbf{g}\|$

Contributions

- We reduce a NTRU problem on a given field to one in a subfield
- We propose an attack algorithm to GCDH problem, which is a security ground of the GGH multilinear maps

Warm-up: Naive approach to solve the NTRU problem

Basic lemma 1

Lemma (1)

For any $\mathbf{a}, \mathbf{b} \in R$, $\|\mathbf{ab}\| \leq \|\mathbf{a}\| \cdot \|\mathbf{b}\| \cdot \sqrt{n}$.

Proof
The X^k's coefficient of $\mathbf{ab}$:

$$\sum_{i+j=k} a_i b_j - \sum_{i+j=n+k} a_i b_j.$$

By the Cauchy - Schwartz inequality, it is smaller than $\|\mathbf{a}\| \cdot \|\mathbf{b}\|$.
Since each coefficient is smaller than $\|\mathbf{a}\| \cdot \|\mathbf{b}\|$, we have
$\|\mathbf{ab}\| \leq \|\mathbf{a}\| \cdot \|\mathbf{b}\| \cdot \sqrt{n}$. □

Basic lemma 2

Lemma (2)

Let $\mathbf{g}$ *be an element of* R*, and* $\mathbf{h} \in R$ *be relative prime to* $\mathbf{g}$*.*
If $\mathbf{c} \in R$ *satisfies* $\|\mathbf{c}\| < q/(2\|\mathbf{h}\|\sqrt{n})$ *and* $\|[\mathbf{c} \cdot \mathbf{h} \cdot \mathbf{g}^{-1}]_q\| < q/(2\|\mathbf{g}\|\sqrt{n})$*, then* $\mathbf{c}$ *is contained in the ideal* $\langle \mathbf{g} \rangle$*.*

Proof
Let $\mathbf{w} := [\mathbf{c} \cdot \mathbf{h} \cdot \mathbf{g}^{-1}]_{\mathbf{q}}$. Then,

$$[\mathbf{ch}]_q = [\mathbf{gw}]_q.$$

By assumption, we have
$\|\mathbf{ch}\| \leq \|\mathbf{c}\| \cdot \|\mathbf{h}\| \cdot \sqrt{n} \leq q/2$ and $\|\mathbf{gw}\| \leq \|\mathbf{g}\| \cdot \|\mathbf{w}\| \cdot \sqrt{n} \leq q/2$.
Therefore, $\mathbf{ch} = \mathbf{gw}$ in R and so $\mathbf{ch} \in \langle \mathbf{g} \rangle$.
Since $\mathbf{h}$ is relative prime to $\mathbf{g}$, we can conclude $\mathbf{c} \in \langle \mathbf{g} \rangle$. □

Naive approach

- Strategy : Find $\mathbf{c} \in R$ s.t $\|\mathbf{c}\|$ and $\|[\mathbf{c} \cdot \mathbf{f}]_q\|$ are small.
- For $\mathbf{f} = \sum_{i=0}^{n-1} f_i X^i$, consider the matrix defined by

$$\begin{bmatrix} - & I_n & - \\ - & M_{\mathbf{f}} & - \end{bmatrix} := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ f_0 & -f_{n-1} & \cdots & -f_1 \\ f_1 & f_0 & \cdots & -f_2 \\ \vdots & \vdots & \ddots & \vdots \\ f_{n-1} & f_{n-2} & \cdots & f_0 \end{bmatrix}.$$

Naive approach

- Define $V : R \to \mathbb{Z}^n$ as $V\left(\sum_{i=0}^{n-1} u_i X^i\right) = (u_0, \cdots, u_{n-1})^T$.

  Then we can observe that

$$\begin{bmatrix} I_n \\ M_{\mathbf{f}} \end{bmatrix} = \begin{bmatrix} V(1) & \cdots & V(X^{n-1}) \\ V(\mathbf{f}) & \cdots & V(X^{n-1}\mathbf{f}) \end{bmatrix}$$

  and

$$\begin{bmatrix} V(\mathbf{c}) \\ V(\mathbf{c}\cdot\mathbf{f}) \end{bmatrix} = \sum_{i=0}^{n-1} c_i \begin{bmatrix} V(X^i) \\ V(X^i\mathbf{f}) \end{bmatrix} \text{ for } \mathbf{c} = \sum_{i=0}^{n-1} c_i X^i \in R.$$

Naive approach

- To obtain $\begin{bmatrix} V(\mathbf{c}) \\ [V(\mathbf{c}\cdot\mathbf{f})]_q \end{bmatrix}$ instead of $\begin{bmatrix} V(\mathbf{c}) \\ V(\mathbf{c}\cdot\mathbf{f}) \end{bmatrix}$, define the column lattice $\Lambda_{\mathbf{f}}$ generated by

$$\begin{bmatrix} I_n & 0 \\ M_{\mathbf{f}} & qI_n \end{bmatrix}.$$

- Since $\begin{bmatrix} V(\mathbf{c}) \\ V(\mathbf{c}\cdot\mathbf{f}) \end{bmatrix} = \sum_{i=0}^{n-1} c_i \begin{bmatrix} V(X^i) \\ V(X^i\mathbf{f}) \end{bmatrix}$, a short vector in $\Lambda_{\mathbf{f}}$ corresponds to $(\mathbf{c}\ ,\ [\mathbf{c}\cdot\mathbf{f}]_q) \in R^2$ such that both $\|\mathbf{c}\|$ and $\|[\mathbf{c}\cdot\mathbf{f}]_q\|$ are small.

However, the dimension of lattice is too big to find a short vector.
Hence, to solve the NTRU problem, one needs to reduce a dimension.

Our attack algorithm

Motivation

- $n = 2^s$

$$
\begin{array}{c}
K_0 = \mathbb{Q}[X]/\langle X^n + 1\rangle \\
| \\
K_1 = \mathbb{Q}[X^2]/\langle X^n + 1\rangle \\
| \\
\vdots \\
| \\
K_{s-1} = \mathbb{Q}[X^{2^{s-1}}]/\langle X^n + 1\rangle \\
| \\
\mathbb{Q} = K_s
\end{array}
$$

- an instance in $K_0 \longrightarrow$ an instance in K_1

Preliminary

For a finite Galois extension K over F, *the trace* $\mathrm{Tr}_{K/F}(\alpha) \in F$ and *norm* $N_{K/F}(\alpha) \in F$ of $\alpha \in K$ over F are defined as:

- $\mathrm{Tr}_{K/F}(\alpha) = \sum_{\sigma \in Gal(K/F)} \sigma(\alpha), \qquad N_{K/F}(\alpha) = \prod_{\sigma \in Gal(K/F)} \sigma(\alpha)$

For a Number field $K_i = \mathbb{Q}[X^{2^i}]/\langle X^n + 1 \rangle$, $0 \leq i \leq \log n$, one have the following properties:

- For $0 \leq i < j \leq \log n$, K_i is a finite Galois extension over K_j
- $|\mathrm{Gal}(K_i/K_j)| = 2^{j-i}$

Idea sketch

- $\mathrm{Gal}(\mathrm{K}_0/\mathrm{K}_1) = \{\mathrm{id}, \sigma\}$ satisfying $\sigma(X) = -X$ and so $\sigma^2 = id$ where id is the identity map.
- For elements $\mathbf{f}, \mathbf{g} \in R \subset K_0$, the following elements are contained in $R_1 \subset K_1$:

$$\begin{aligned} Tr_{K_0/K_1}(\mathbf{f}) &= \mathbf{f} + \sigma(\mathbf{f}) \\ N_{K_0/K_1}(\mathbf{f}) &= \mathbf{f} \cdot \sigma(\mathbf{f}) \\ Tr_{K_0/K_t}(\mathbf{f}\sigma(\mathbf{g})) &= \mathbf{f}\sigma(\mathbf{g}) + \sigma(\mathbf{f})\mathbf{g}, \end{aligned}$$

since these are fixed by the $\mathrm{Gal}(\mathrm{K}_0/\mathrm{K}_1)$.
Note that these elements have only $n/2$ terms and the last one lies in $2 \cdot R_1$.

Idea sketch

For a given instance $\mathbf{f} = [\mathbf{h}/\mathbf{g}]_q$ for $NTRU_{\phi_n,q,D,N,B}$ with $\mathrm{Gal}(\mathrm{K}_0/\mathrm{K}_1) = \{\mathrm{id}, \sigma\}$,

$$\begin{aligned} [\mathrm{Tr}_{K_0/K_1}(\mathbf{f})]_q &= [\mathbf{f} + \sigma(\mathbf{f})]_q = [[\mathbf{h}/\mathbf{g}]_q + \sigma([\mathbf{h}/\mathbf{g}]_q)]_q \\ &= [(\mathbf{h}\sigma(\mathbf{g}) + \sigma(\mathbf{h})\mathbf{g})/\mathbf{g}\sigma(\mathbf{g})]_q \end{aligned}$$

You can see that:

- $\dfrac{\mathbf{g}\sigma(\mathbf{h}) + \sigma(\mathbf{g})\mathbf{h}}{2} \in R_1$, $\left\| \dfrac{\mathbf{g}\sigma(\mathbf{h}) + \sigma(\mathbf{g})\mathbf{h}}{2} \right\| \leq \|\mathbf{h}\| \cdot \|\mathbf{g}\| \cdot \sqrt{n/2}$
- $\mathbf{g}\sigma(\mathbf{g}) \in R_1$, $\|\mathbf{g}\sigma(\mathbf{g})\| \leq \|\mathbf{g}\|^2 \sqrt{n/2}$

Idea sketch

	R_0	$\Rightarrow$	R_1
$\mathbf{f}$	$\frac{\mathbf{h}}{\mathbf{g}}$	$\Rightarrow$	$\frac{\mathbf{h}}{\mathbf{g}} + \frac{\sigma(\mathbf{h})}{\sigma(\mathbf{g})}$
Denominator	$\mathbf{g}$	$\Rightarrow$	$\mathbf{g}\sigma(\mathbf{g})$
Numerator	$\mathbf{h}$	$\Rightarrow$	$\mathbf{h}\sigma(\mathbf{g}) + \sigma(\mathbf{h})\mathbf{g}$

Idea sketch

- We can consider $[\mathrm{Tr}_{K_0/K_1}(\mathbf{f})/2]_q$ as a new instance of the $NTRU_{\phi_{n/2},q,D_1,N_1,B_1}$ problem over K_1 where $D_1 = D^2\sqrt{n/2}$, $N_1 = ND\sqrt{n/2}$, $B_1 = \min\left\{\frac{q}{2D_1\sqrt{n}}, \frac{q}{2N_1\sqrt{n}}, \frac{q}{2nN^2\|\mathbf{g}^{-1}\|\sqrt{\mathbf{n}}}\right\}$

- Using the concept inductively, one can extend it to K_i

Idea sketch

	R_0	$\Rightarrow$	R_i
$\mathbf{f}$	$\frac{\mathbf{h}}{\mathbf{g}}$	$\Rightarrow$	$\sum_{\sigma} \sigma\left(\frac{\mathbf{h}}{\mathbf{g}}\right)$
Denominator	$\mathbf{g}$	$\Rightarrow$	$\prod_{\sigma} \sigma(\mathbf{g})$
Numerator	$\mathbf{h}$	$\Rightarrow$	$\sum_{\sigma} \sigma\left(\mathbf{h} \prod_{\sigma \neq id} \sigma(\mathbf{g})\right)$

Idea sketch

	R_0	R_i	R_i
$\mathbf{f}$	$\frac{\mathbf{h}}{\mathbf{g}}$	$Tr(\mathbf{f})$	$N(\mathbf{f})$
Denominator	$\mathbf{g}$	$N(\mathbf{g})$	$N(\mathbf{g})$
Numerator	$\mathbf{h}$	$Tr\left(\mathbf{h}\prod_{\sigma\neq id}\sigma(\mathbf{g})\right)$	$N(\mathbf{h})$

[ABD16] A subfield Lattice Attack on Overstretched NTRU Assumptions Cryptanalysis of Some FHE and Graded Encdoing Schemes

Idea sketch

- Suppose we have a solution (a, b) of $NTRU_{\phi_{n/2},q,D_1,N_1,B_1}$ s.t $\left[\frac{b}{a}\right]_q = \left[\frac{(\mathbf{g}\sigma(\mathbf{h}) + \sigma(\mathbf{g})\mathbf{h})/\mathbf{2}}{\mathbf{g}\sigma(\mathbf{g})}\right]_q$.

- Then by Lemma (2), a is of the form $a = \mathbf{dg}\sigma(\mathbf{g})$ and $[a \cdot \mathbf{f}]_\mathbf{q} = [\mathbf{dg}\sigma(\mathbf{g}) \cdot [\mathbf{h}/\mathbf{g}]_\mathbf{q}]_\mathbf{q} = [\mathbf{dh}\sigma(\mathbf{g})]_\mathbf{q}$

- If $B_1 = \min\left\{\frac{q}{2D_1\sqrt{n}}, \frac{q}{2N_1\sqrt{n}}, \frac{q}{2nN^2\|\mathbf{g}^{-\mathbf{1}}\|\sqrt{\mathbf{n}}}\right\}$, the both sizes of a and $[a\mathbf{f}]_\mathbf{q}$ are smaller than q.

- When is it extendable until?

Main Theorem

Theorem

We can reduce

$$NTRU_{\phi_n,q,D,N,B} \text{ into } NTRU_{\phi_{n/2^t},q,D_t,N_t,B_t}$$

where $D_t = D^{2^t} \prod_{j=1}^{t} \sqrt{n/2^j}$, $N_t = ND^{2^t-1} \prod_{j=1}^{t} \sqrt{n/2^j}$ *are smaller than* q,
and $B_t = \min\left\{ \frac{q}{2D_t\sqrt{n}}, \frac{q}{2N_t\sqrt{n}}, \frac{q}{2nN^2\|\mathbf{g}^{-1}\|\sqrt{n}} \right\}$.

Main Theorem

- Hence, if we solve the $NTRU_{\phi_{n/2^t},q,D_t,N_t,B_t}$ in $2^{O(\beta)}$ time, we can also solve the $NTRU_{\phi_n,q,D,N,B}$ in $2^{O(\beta)}$ time

- For $\beta > 0$ and $t \in \mathbb{Z}$ with

$$2\beta^{\frac{n_t}{2(\beta-1)}+\frac{3}{2}}\sqrt{q} \leq B_t$$

we can solve the $NTRU_{\phi_n,q,D,N,B}$ problem in $2^{O(\beta)}$ time.

GGH scheme: Algebraic Setup

- $R := \mathbb{Z}[x]/(x^n + 1)$ (n a power of 2), $\mathcal{P} := R/\langle \mathbf{g} \rangle$, $\mathcal{C} := R/qR \simeq \mathbb{Z}_q[x]/(x^n + 1)$
- Secret: $\mathbf{z} \in \mathcal{C}$, $\mathbf{g} \in R$ with small coeff, $\mathbf{h}, \mathbf{r_i}, \mathbf{r} \in R$ rel. small.
- The level-t encoding of $\mathbf{m}$, $\mathrm{enc}_t(\mathbf{m})$, is of the form:

$$\mathrm{enc}_t(\mathbf{m}) = \frac{\mathbf{rg} + \mathbf{m}}{\mathbf{z^t}}$$

- Public: $n, q, \kappa \in \mathbb{Z}, (\mathbf{x_1}, \ldots, \mathbf{x}_\tau, \mathbf{y}, P_{zt}) \in \mathcal{C}^{\tau+1}$
  - $\mathbf{x_i} = \dfrac{\mathbf{gr_i}}{\mathbf{z}^\kappa}$, $\mathbf{y} = \dfrac{\mathbf{r}}{\mathbf{z}^\kappa}$
  - Zero testing parameter: $P_{zt} := \left[\dfrac{\mathbf{hz}^\kappa}{\mathbf{g}}\right]_q$

Corollary

- GCDH problem, security ground of GGH scheme, heavily relies on finding a short vector of $\langle \mathbf{g} \rangle$.
- Applying our results to $[\mathbf{y}/\mathbf{x_i}]_\mathbf{q}$, one can recover a short multiple of $\mathbf{g}$.
- When given parameters in GGH scheme with some auxiliary inputs, we show that GGH scheme has not λ-bit security.
  - when n is $\Theta(\lambda^2)$ and $\log q = \Theta(\lambda)$, we can solve the GCDH problem in $2^{O(\log^2 \lambda)}$.

DANKE!