A subfield lattice attack on overstretched NTRU assumptions

Martin R. Albrecht
Oxford Lattice School

Outline

Martin Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and Graded Encoding Schemes. Cryptology ePrint Archive, Report 2016/127. http://eprint.iacr.org/2016/127. 2016

Introduction

NTRUEncrypt

Key Generation $\mathcal{R} = \mathbb{Z}[X]/(X^n + 1)$, modulus q, width parameter σ

- Sample $f \leftarrow D_{\mathcal{R},\sigma}$ (invertible mod q)
- Sample $g \leftarrow D_{\mathcal{R},\sigma}$
- Publish $h = [g/f]_q$

Encrypt $m \in \{0,1\}^n$

- Sample $s, e \leftarrow D_{\mathcal{R},\chi}, D_{\mathcal{R},\chi}$
- Return $2\,(h \cdot s + e) + m$

Decrypt $c \in \mathcal{R}_q$

- $m' = f \cdot c = 2\,(g \cdot s + f \cdot e) + f \cdot m$
- Return $m' \bmod 2 \equiv f \cdot m \bmod 2$

The NTRU lattice Λ_h^q

```
sage: K.<zeta> = CyclotomicField(8)
sage: OK = K.ring_of_integers()
sage: h = -36*zeta^3 + 44*zeta^2 + 14*zeta + 28
sage: h
```

$$-36\zeta_8^3 + 44\zeta_8^2 + 14\zeta_8 + 28$$

```
sage: H = h.matrix(); q = 97
sage: block_matrix([[1, H],[0, q]])
```

$$\left(\begin{array}{cccc|cccc}
1 & & & & 28 & 14 & 44 & -36 \\
 & 1 & & & 36 & 28 & 14 & 44 \\
 & & 1 & & -44 & 36 & 28 & 14 \\
 & & & 1 & -14 & -44 & 36 & 28 \\
\hline
 & & & & 97 & & & \\
 & & & & & 97 & & \\
 & & & & & & 97 & \\
 & & & & & & & 97
\end{array}\right)$$

The NTRU lattice Λ_h^q

- The lattice Λ_h^q defined by an NTRU instance for parameters $\mathcal{R}, q, \sigma$ has dimension $2n$ and volume q^n.
- If h were uniformly random, the Gaussian heuristic predicts that the shortest vectors of Λ_h^q have norm $\approx \sqrt{nq}$.
- Whenever

$$\|f\| \approx \|g\| \approx \sqrt{n}\,\sigma \ll \sqrt{n\,q},$$

then Λ_h^q has unusually short vectors.

NTRU

Definition (NTRU Assumption)

It is hard to find a short vector in the $\mathcal{R}$-module

$$\Lambda_h^q = \{(x, y) \in \mathcal{R}^2 \text{ s.t. } hx - y = 0 \bmod q\}$$

with $\mathcal{R} = \mathbb{Z}[X]/(P(X))$ and the promise that a short solution (f, g) — the private key — exists.[1][2]

[1] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A New High Speed Public Key Cryptosystem. Draft Distributed at Crypto'96, available at `http://web.securityinnovation.com/hubfs/files/ntru-orig.pdf`. 1996.

[2] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. In: *ANTS*. 1998, pp. 267–288.

NTRU Applications

The NTRU assumption has been utilised for

- signatures schemes,[3]
- fully homomorphic encryption,[4]
- candidate constructions for multi-linear maps.[5]

---

[3] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice Signatures and Bimodal Gaussians. In: *CRYPTO 2013, Part I*. ed. by Ran Canetti and Juan A. Garay. Vol. 8042. LNCS. Springer, Heidelberg, Aug. 2013, pp. 40–56. DOI: 10.1007/978-3-642-40041-4_3.

[4] Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: *44th ACM STOC*. ed. by Howard J. Karloff and Toniann Pitassi. ACM Press, May 2012, pp. 1219–1234. DOI: 10.1145/2213977.2214086; Joppe W. Bos, Kristin Lauter, Jake Loftus, and Michael Naehrig. Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme. In: *14th IMA International Conference on Cryptography and Coding*. Ed. by Martijn Stam. Vol. 8308. LNCS. Springer, Heidelberg, Dec. 2013, pp. 45–64. DOI: 10.1007/978-3-642-45239-0_4.

[5] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate Multilinear Maps from Ideal Lattices. In: *EUROCRYPT 2013*. Ed. by Thomas Johansson and Phong Q. Nguyen. Vol. 7881. LNCS. Springer, Heidelberg, May 2013, pp. 1–17. DOI: 10.1007/978-3-642-38348-9_1.

Lattice Attacks

- Recovering a short enough vector of some target norm τ, potentially longer than (f, g), is sufficient for an attack.[6]
- In particular, finding a vector $o(q)$ would break many applications such as encryption.
- This requires strong lattice reduction and NTRU remains asymptotically secure.[7][8]

[6] Don Coppersmith and Adi Shamir. Lattice Attacks on NTRU. In: *EUROCRYPT'97*. Ed. by Walter Fumy. Vol. 1233. LNCS. Springer, Heidelberg, May 1997, pp. 52–61. DOI: `10.1007/3-540-69053-0_5`.
[7] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. In: *ANTS*. 1998, pp. 267–288.
[8] Jeff Hoffstein et al. Choosing Parameters for NTRUEncrypt. Cryptology ePrint Archive, Report 2015/708. `http://eprint.iacr.org/2015/708`. 2015.

Best Attacks

Practical combined lattice-reduction and meet-in-the-middle attack[9] of Howgrave-Graham.[10][11]

Asymptotic BKW variant, with a heuristic complexity $2^{\Theta(n/\log\log q)}$.[12]

---

[9] Jeffrey Hoffstein, Joseph H. Silverman, and William Whyte. Meet-in-the-middle Attack on an NTRU private key. Technical report, NTRU Cryptosystems, July 2006. Report #04, available at http://www.ntru.com. 2006.

[10] Nick Howgrave-Graham. A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU. In: *CRYPTO 2007*. Ed. by Alfred Menezes. Vol. 4622. LNCS. Springer, Heidelberg, Aug. 2007, pp. 150–169. DOI: 10.1007/978-3-540-74143-5_9.

[11] Thomas Wunderer. Revisiting the Hybrid Attack: Improved Analysis and Refined Security Estimates. Cryptology ePrint Archive, Report 2016/733. http://eprint.iacr.org/2016/733. 2016.

[12] Paul Kirchner and Pierre-Alain Fouque. An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices. In: *CRYPTO 2015, Part I*. ed. by Rosario Gennaro and Matthew J. B. Robshaw. Vol. 9215. LNCS. Springer, Heidelberg, Aug. 2015, pp. 43–62. DOI: 10.1007/978-3-662-47989-6_3.

Preliminaries

Cyclotomic Number Fields and Subfields

- I'll focus on Cyclotomic number rings of degree $n = 2^k$ for ease of exposure, but everything can be made general.
- Let $\mathcal{R} \simeq \mathbb{Z}[X]/(X^n + 1)$ be the ring of integers of the Cylotomic number field $\mathbb{K} = \mathbb{Q}(\zeta_m)$ for some $m = 2^k$ and $n = m/2$.
- Let $\mathbb{L} = \mathbb{Q}(\zeta_{m'})$ with $m'|m$ be a subfield of $\mathbb{K}$.
- The ring of integers of $\mathbb{L}$ is $\mathcal{R}' \simeq \mathbb{Z}[X]/(X^{n'} + 1)$ with $n' = m'/2$.
- We write the canonical inclusion $\mathcal{R}' \subset \mathcal{R}$ explicitly as $L : \mathcal{R}' \to \mathcal{R}$.
- The norm $\mathsf{N}_{\mathbb{K}/\mathbb{L}} : \mathbb{K} \to \mathbb{L}$ is the multiplicative map defined by

$$\mathsf{N}_{\mathbb{K}/\mathbb{L}} : f \mapsto \prod_{\psi \in G'} \psi(f)$$

  where G' is the Galois subgroup corresponding to $\mathbb{L}$.

Geometry

The ring $\mathcal{R}$ is viewed as a lattice by endowing it with the inner product

$$\langle a, b \rangle = \sum_{i=0}^{n-1} a_i \cdot b_i.$$

- This defines a Euclidean norm denoted by $\| \cdot \|$.
- We will make use of the operator's norm $| \cdot |$ defined by:

$$|a| = \sup_{x \in \mathbb{K}^*} \|ax\| / \|x\| = \max |a_i|.$$

- It holds that $\|a \cdot b\| \leq \sqrt{n} \cdot |a| \cdot \|b\|$ and

$$|\, \mathrm{N}_{\mathbb{K}/\mathbb{L}}(a)| \leq \sqrt{n}^{r-1} |a|^r \leq \sqrt{n}^{r-1} \|a\|^r.$$

Lattice Reduction

Lattice reduction algorithms produce vectors of length

$$\beta^{\Theta(n/\beta)} \cdot \lambda_1(\Lambda)$$

for a computational cost

$$\mathrm{poly}(\lambda) \cdot 2^{\Theta(\beta)},$$

with $\lambda_1(\Lambda)$ the length of a shortest vector of Λ.[13]

[13] Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better Lattice Security Estimates. In: *ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. LNCS. Springer, Heidelberg, Dec. 2011, pp. 1–20. DOI: `10.1007/978-3-642-25385-0_1`.

Subfield Lattice Attack

Overview

$$
\begin{tikzcd}
\mathbb{K} = \mathbb{Q}(\zeta_m) \arrow[dd, dash] \arrow[dr, dash] & \\
 & \mathcal{R} = \mathbb{Z}[\zeta_m] \arrow[dd, dash] \\
\mathbb{L} = \mathbb{Q}(\zeta_{m'}) \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q} \arrow[dr, dash] & \mathcal{R}' = \mathbb{Z}[\zeta_{m'}] \arrow[d, dash] \\
 & \mathbb{Z}
\end{tikzcd}
$$

$$
\begin{tikzcd}
(h, f, g) \arrow[d] & (x, y) = u \cdot (f, g) \\
(h', f', g') \arrow[r, dash] & (h' \to (x', y')) \arrow[u]
\end{tikzcd}
$$

Define $f' = \mathrm{N}_{\mathbb{K}/\mathbb{L}}(f)$, $g' = \mathrm{N}_{\mathbb{K}/\mathbb{L}}(g)$, and $h' = \mathrm{N}_{\mathbb{K}/\mathbb{L}}(h)$, then (f', g') is a vector of $\Lambda^q_{h'}$, and it may be an unusually short one.

n	$\log q$	r	$\|f\|$	$\sqrt{2/3 \cdot n}$	$\|f'\|$	$\left(\sqrt{2/3 \cdot n}\right)^r$
256	300	8	3.70893	3.70752	29.21967	29.66015
256	300	32	3.66546	3.70752	103.69970	118.64060
256	300	64	3.71731	3.70752	210.20853	237.28120

Table 1: Observed norms, after relative norm operation. All norms are logs.

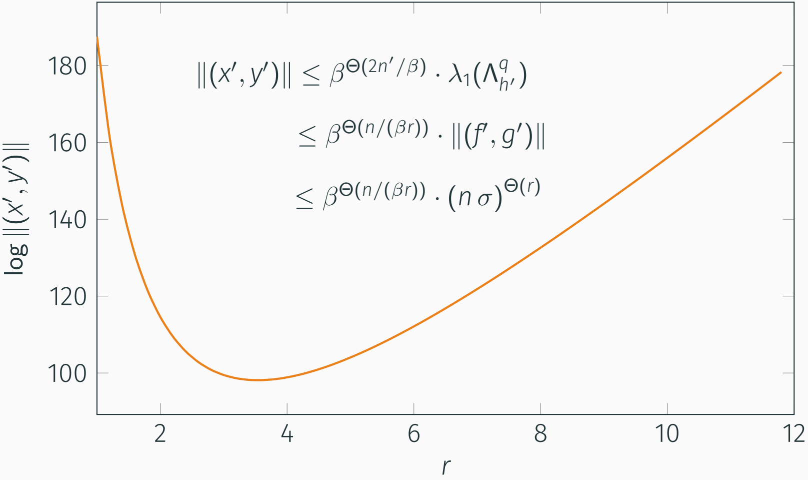
We assume that the following lemma holds also for all reasonable distributions considered in cryptographic constructions:

Let f be sampled from spherical Gaussians of variance σ^2. Then,

$$\|f^r\| \leq \sqrt{n}^{r-1} \cdot \|f\|^r$$

2. Lattice Reduction in the Subfield

Run lattice reduction with block size β on lattice $\Lambda^q_{h'}$, to obtain a vector $(x', y') \in \Lambda^q_{h'}$ with



The Right Kind of (x', y')

(x', y') is a solution in the subfield, how could that be useful?

The Right Kind of (x', y')

(x', y') is a solution in the subfield, how could that be useful?

1. If (x', y') is short enough, then it is an $\mathcal{R}'$-multiple of (f', g').
2. This will allow us to lift (x', y') to a short vector in Λ_h^q.

$(x', y') = v \cdot (f', g')$

Theorem

Let $f', g' \in \mathcal{R}'$ be such that $\langle f' \rangle$ and $\langle g' \rangle$ are coprime ideals and that $h' \cdot f' = g' \bmod q$ for some $h' \in \mathcal{R}'$. If $(x', y') \in \Lambda_{h'}^q$ has length verifying

$$\|(x', y')\| < \frac{q}{\|(f', g')\|},$$

then $(x', y') = v \cdot (f', g')$ for some $v \in \mathcal{R}'$.

3. Lifting the Short Vector

To lift the solution from the sub-ring $\mathcal{R}'$ to $\mathcal{R}$ compute (x, y) as

- $x = L(x')$ and
- $y = L(y') \cdot h/L(h') \bmod q$,

where L is the canonical inclusion map.

Performance

Can solve in time complexity $\mathrm{poly}(n) \cdot 2^{\Theta(\beta)}$ when

- Direct lattice attack: $\beta / \log \beta = \Theta\left(n / \log q\right)$

Performance

Can solve in time complexity $\mathrm{poly}(n) \cdot 2^{\Theta(\beta)}$ when

- Direct lattice attack: $\beta / \log \beta = \Theta\left(n / \log q\right)$
- Subfield attack: $\beta / \log \beta = \Theta\left(n \, \log n / \log^2 q\right)$ whenever $r = \Theta(\log q / \log n) > 1$

Thank You