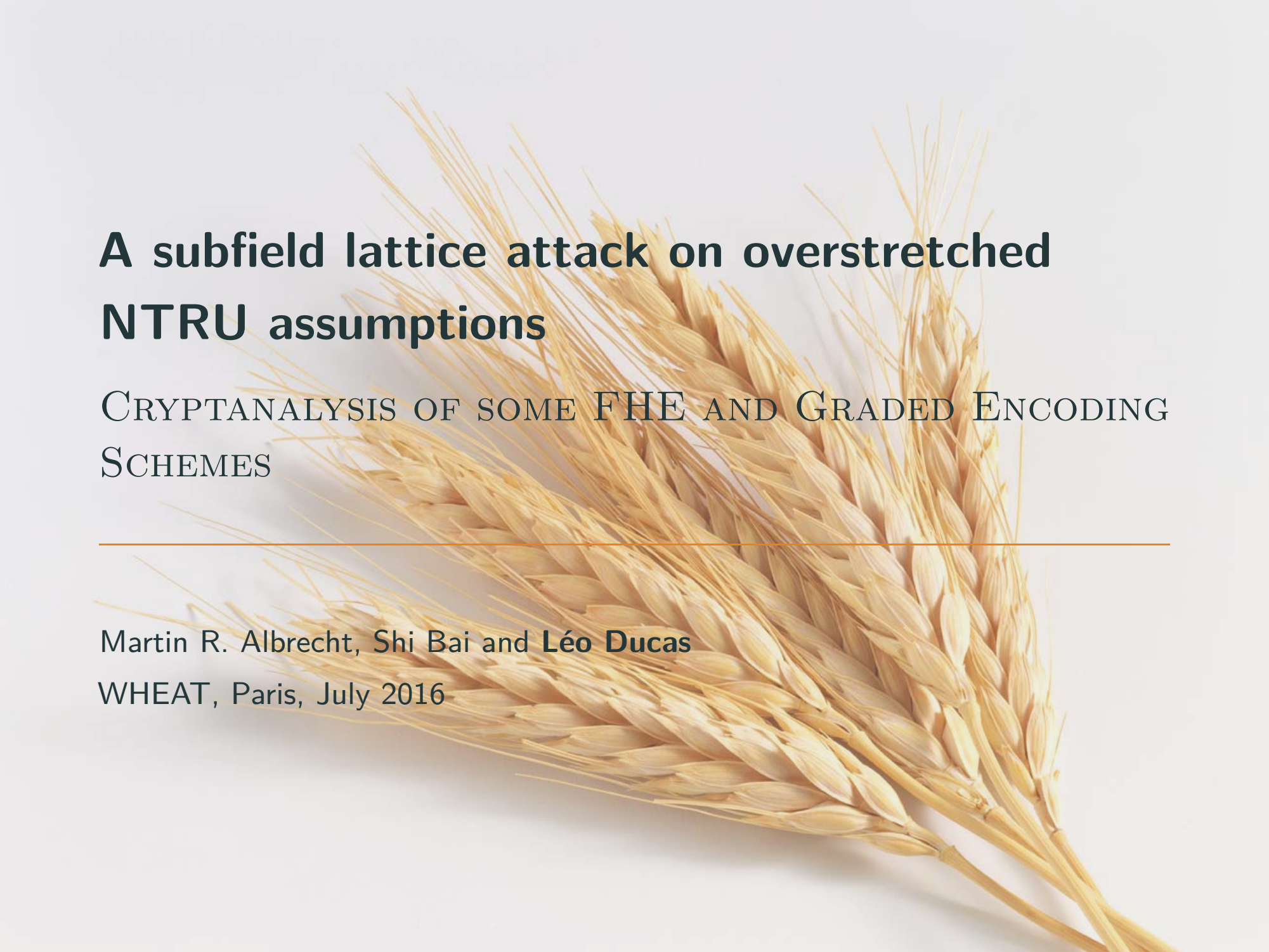


A subfield lattice attack on overstretched NTRU assumptions

Cryptanalysis of some FHE and Graded Encoding Schemes

Martin R. Albrecht, Shi Bai and **Léo Ducas**

WHEAT, Paris, July 2016

Outline

Outline

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 $m \in \{0, 1\}$

- 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;
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.

[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]

Asymptotic BKW variant, with a heuristic complexity $2^{\Theta(n/\log\log q)}$.[11]

---

[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.

[11] 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.

TL;DR

- We use lattice reduction in a **subfield** to attack the NTRU assumption for large moduli q.
- This attack is asymptotically faster than the previously known attacks as soon as q is super-polynomial.
- Strategy
  1. Map the NTRU instance to the chosen subfield.
  2. Apply lattice reduction.
  3. Lift the solution to the full field.

Related work

- approach already sketched by Gentry, Szydlo, Jonsson, Nguyen and Stern[12]. Dismissed at that time because irrelevant against NTRU itself.
- Concurrently and independently, Cheon, Jeong and Lee[13] also investigated subfield attacks on GGH-like graded encoding schemes.
- The general approach is similar to ours, but [CJL16]
  - uses the Trace map instead of the Norm,
  - only considers Graded Encoding Schemes,
  - restricts attention to power of two Cyclotomic rings and
  - has more powerful results against Graded Encoding Schemes.

---

[12] Craig Gentry and Michael Szydlo. **Cryptanalysis of the Revised NTRU Signature Scheme**. In: *EUROCRYPT 2002*. Ed. by Lars R. Knudsen. Vol. 2332. LNCS. Springer, Heidelberg, 2002, pp. 299–320.

[13] Jung Hee Cheon, Jinhyuck Jeong, and Changmin Lee. **An Algorithm for NTRU Problems and Cryptanalysis of the GGH Multilinear Map without an encoding of zero**. Cryptology ePrint Archive, Report 2016/139. `http://eprint.iacr.org/`. 2016.

Outline

Rings

- Our work is presented for arbitrary number fields, their ring of integers and their subfields.
- In this talk, I'll focus on Cyclotomic number rings of degree $n = 2^k$ for ease of exposure.

Cyclotomic Number Fields and Subfields

- 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 $n = m/2$.

```
sage: K.<zeta> = CyclotomicField(8)
sage: OK = K.ring_of_integers()
sage: K.polynomial()
```

$x^4 + 1$

Cyclotomic Number Fields and Subfields

- 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 $L : \mathcal{R}' \to \mathcal{R}$.

```
sage: KK, L = K.subfield(zeta^2)
sage: zeta_ = KK.gen()
sage: L(zeta_)
```

ζ_8^2

Cyclotomic Number Fields and Subfields

- $\mathbb{K}$ is a Galois extension of $\mathbb{Q}$, and its Galois group G is isomorphic to $\mathbb{Z}_m^*$: $i \in \mathbb{Z}_m^* \leftrightarrow (X \mapsto X^i) \in G$.

```
sage: G = K.galois_group(); G
```

$\langle (1,2)(3,4), (1,3)(2,4) \rangle$

Cyclotomic Number Fields and Subfields

- There is a one-to-one correspondence between the subgroups G' of G, and the subfields $\mathbb{L}$ of $\mathbb{K}$.
- $\mathbb{L}$ is the subfield such that an automorphism of $a \in G$ is the identity on $\mathbb{L}$ if an only if $a \in G'$.

```
sage: G_ = [a for a in G if a(zeta_) == zeta_]
sage: G_ = G.subgroup(G_); G_
```

$\langle , (1,2)(3,4) \rangle$

Cyclotomic Number Fields and Subfields

- The norm $\mathsf{N}_{\mathbb{K}/\mathbb{L}} : \mathbb{K} \to \mathbb{L}$ is the multiplicative map defined by

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

```
sage: f = OK.random_element(); f
```

$6\zeta_8^3 - \zeta_8^2 - 5\zeta_8 - 6$

```
sage: f.norm(KK) == prod([a(f) for a in G_])
```

True

```
sage: ff = f.norm(KK);
sage: ff, L(ff)
```

$\left(23\zeta_0 - 25, 23\zeta_8^2 - 25\right)$

Geometry

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

$$\langle a, b \rangle = \sum_{e} e(a)\bar{e}(b) \tag{1}$$

where e ranges over all the n embeddings $\mathbb{K} \to \mathbb{C}$.

This defines a Euclidean norm denoted by $\| \cdot \|$.

Operator's Norm

- We will make use of the operator's norm $|\cdot|$ defined by:

$$|a| = \sup_{x \in \mathbb{K}^*} \|ax\|/\|x\| = \max_e |e(a)|$$

where e ranges over all the embeddings.

Operator's Norm

- We will make use of the operator's norm $|\cdot|$ defined by:

$$|a| = \sup_{x \in \mathbb{K}^*} \|ax\|/\|x\| = \max_e |e(a)|$$

  where e ranges over all the embeddings.

- It holds that

$$\|a \cdot b\| \leq |a| \cdot \|b\|$$

  and

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

Lattice Reduction

Lattice reduction algorithms produce vectors of length

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

for a computational cost

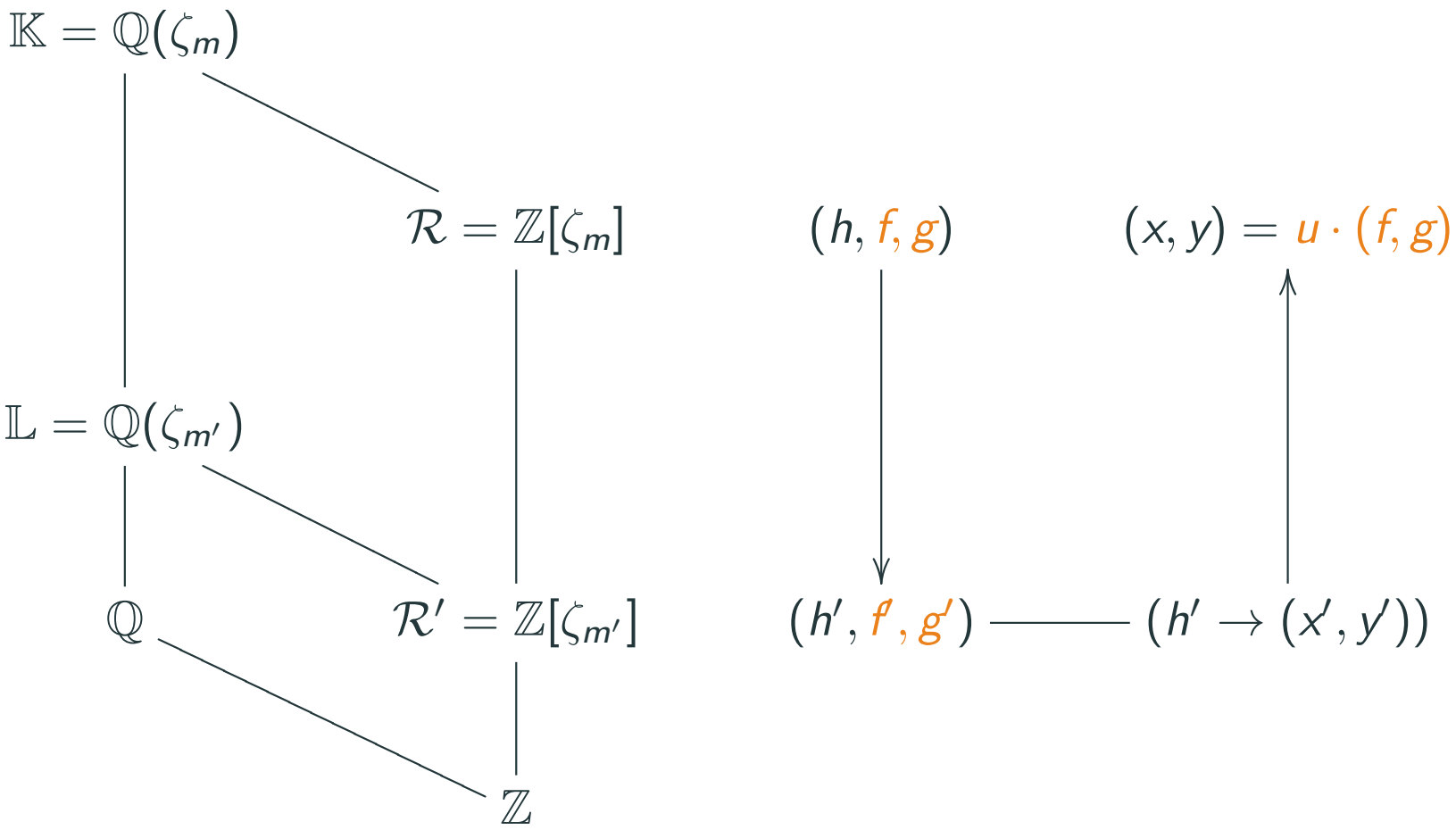
$$\mathrm{poly}(\lambda) \cdot 2^{\Theta(\beta)},$$

with $\lambda_1(\Lambda)$ the length of a shortest vector of Λ.[14]

[14] 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.

Outline

Overview


$\mathbb{K} = \mathbb{Q}(\zeta_m)$
$\mathcal{R} = \mathbb{Z}[\zeta_m]$
$\mathbb{L} = \mathbb{Q}(\zeta_{m'})$
$\mathbb{Q}$
$\mathcal{R}' = \mathbb{Z}[\zeta_{m'}]$
$\mathbb{Z}$
(h, f, g)
(h', f', g')
$(x, y) = u \cdot (f, g)$
$(h' \to (x', y'))$

1. Norming Down

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.

1. Norming Down

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

Lemma

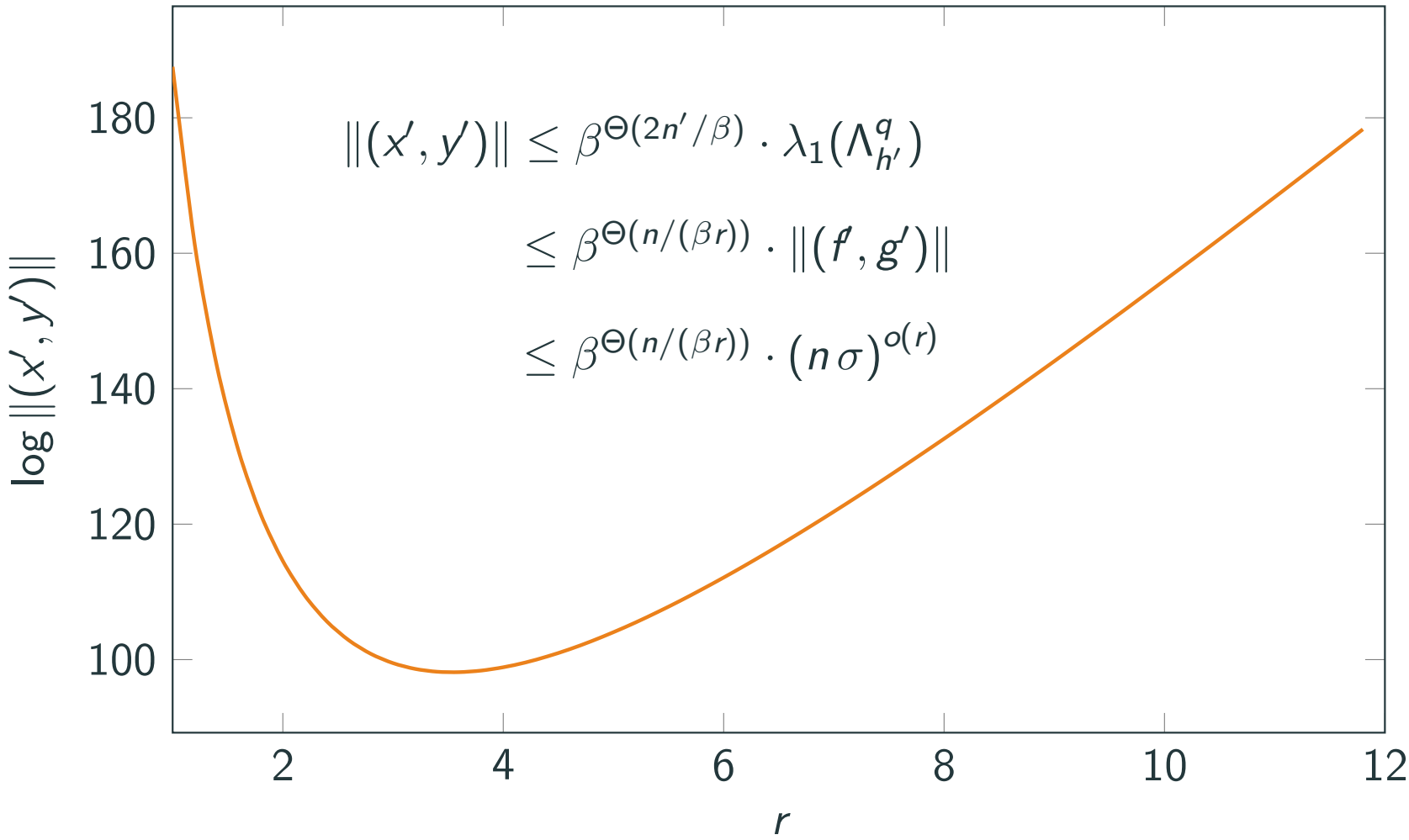
Let f, g be sampled from continuous spherical Gaussians of variance σ^2. For any constant $c > 0$, there exists a constant C, such that,

$$\|g'\| \leq \left(\sigma n^C\right)^r, \quad \|f'\| \leq \left(\sigma n^C\right)^r, \quad |f'| \leq \left(\sigma n^C\right)^r, \quad |f'^{-1}| \leq \left(n^C/\sigma\right)^r$$

except with probability $O(n^{-c})$.

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 $(x', y') \in \Lambda^q_{h'}$ has length verifying

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

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

Proof

1. $B = \{(f', g'), (F', G')\}$ is a basis of $\Lambda^q_{h'}$ for some (F', G')
   - By coprimality, there exists (F', G') such that $f'G' - g'F' = q \in \mathcal{R}$.

$$f'(F', G') - F'(f', g') = (0, q)$$
$$g'(F', G') - G'(f', g') = (-q, 0)$$
$$[f'^{-1}]_q(f', g') = (1, h') \bmod q.$$

   - This implies $\Lambda^q_{h'} \subset M$, the module generated by B.
   - Because

$$\det_{\mathbb{L}}(B) = f'G' - g'F' = q = \det_{\mathbb{L}}(\{(1, h'), (0, q)\})$$

   we have $\mathrm{Vol}(M) = q^{n'} = \mathrm{Vol}(\Lambda^q_{h'})$, and therefore $M = \Lambda^q_{h'}$.

Proof

2. A short enough vector in $\Lambda_{h'}^{q}$ belongs to $\Lambda = (f', g')\mathcal{R}'$
   - Denote the projection of $(F', G')\mathcal{R}$ orthogonally to Λ as Λ^*.
   - Let v^* of length λ_1^* be a shortest vector of Λ^*.
   - We have

$$\mathrm{Vol}(\Lambda) \leq \|(f', g')\|^{n'} \text{ and } \mathrm{Vol}(\Lambda^*) \leq \|v^*\|^{n'}$$

   - From $\mathrm{Vol}(\Lambda) \cdot \mathrm{Vol}(\Lambda^*) = \mathrm{Vol}(\Lambda_{h'}^{q}) = q^{n'}$, we deduce that

$$\lambda_1^* = \|v^*\| \geq \frac{q}{\|(f', g')\|}.$$

   - The hypothesis ensures that $\|(x', y')\| < \lambda_1^*$ and we conclude that $(x', y') \in \Lambda = (f', g')\mathcal{R}'$.

Satisfying Conditions of the Theorem

1. The length condition is satisfied asymptotically when

$$\beta^{\Theta(n/\beta r)} \cdot (n\sigma)^{\Theta(r)} < q.$$

2. Heuristically, the probability of satisfying the coprimality condition for random f', g' is larger than a constant: the density of coprime pairs of ideals[15] and elements[16] in $\mathcal{R}$ is $1/\zeta_{\mathbb{K}}(2)$ where $\zeta_{\mathbb{K}}$ denotes the Dedekind zeta function over $\mathbb{K}$.

---

[15] Brian D Sittinger. **The probability that random algebraic integers are relatively r-prime**. In: *Journal of Number Theory* 130.1 (2010), pp. 164–171.

[16] Andrea Ferraguti and Giacomo Micheli. **On The Mertens–Cesàro Theorem for Number Fields**. In: *Bulletin of the Australian Mathematical Society* (2014), pp. 1–12.

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.

Rationale

Recall that $(x', y') = v(f', g')$ and set

- $\tilde{f} = L(f')/f$,
- $\tilde{g} = L(g')/g$ and
- $\tilde{h} = L(h')/h$.

Write

$$x = L(x') = L(v) \cdot \tilde{f} \cdot f \bmod q.$$

and

$$\begin{aligned} y &= L(y') \cdot h / L(h') \\ &= L(v) \cdot L(g')/\tilde{h} \\ &= L(v) \cdot g \cdot \tilde{g}/\tilde{h} \\ &= L(v) \cdot \tilde{f} \cdot g \bmod q. \end{aligned}$$

Summary

We have found a short multiple of (f, g):

$$(x, y) = u \cdot (f, g) \in \Lambda_h^q \quad \text{with } u = L(v) \cdot \tilde{f} \in \mathcal{R}$$

Summary

We have found a short multiple of (f, g):

$$(x, y) = u \cdot (f, g) \in \Lambda_h^q \quad \text{with } u = L(v) \cdot \tilde{f} \in \mathcal{R}$$

We have

$$\|(x, y)\| \leq |v| \cdot |f|^{r-1} \cdot \|(f, g)\|$$

by writing $\tilde{f}$ as the product of $r - 1$ many $\psi(f)$ where the ψ's are automorphisms of $\mathbb{K}$.

Summary

We have found a short multiple of (f, g):

$$(x, y) = u \cdot (f, g) \in \Lambda_h^q \quad \text{with } u = L(v) \cdot \tilde{f} \in \mathcal{R}$$

We have

$$\|(x, y)\| \leq |v| \cdot |f|^{r-1} \cdot \|(f, g)\|$$

by writing $\tilde{f}$ as the product of $r - 1$ many $\psi(f)$ where the ψ's are automorphisms of $\mathbb{K}$.

$$\|(x, y)\| \leq |x'| \cdot |f'^{-1}| \cdot |f|^{r-1} \cdot \|(f, g)\|$$

by decomposing $v = x'/f'$.

Summary

We have found a short multiple of (f, g):

$$(x, y) = u \cdot (f, g) \in \Lambda_h^q \quad \text{with } u = L(v) \cdot \tilde{f} \in \mathcal{R}$$

We have

$$\|(x, y)\| \leq |v| \cdot |f|^{r-1} \cdot \|(f, g)\|$$

by writing $\tilde{f}$ as the product of $r - 1$ many $\psi(f)$ where the ψ's are automorphisms of $\mathbb{K}$.

$$\|(x, y)\| \leq |x'| \cdot |f'^{-1}| \cdot |f|^{r-1} \cdot \|(f, g)\|$$

by decomposing $v = x'/f'$.

$$\|(x, y)\| \leq \beta^{\Theta(n/(\beta r))} \cdot (n\sigma)^{\Theta(r)}$$

by our heuristic.

(Super-)Exponential q

- Consider $n = \Theta(\lambda^2 \log^2 \lambda)$ and $q = \exp(\Theta(\lambda \log^2 \lambda))$.

(Super-)Exponential q

- Consider $n = \Theta(\lambda^2 \log^2 \lambda)$ and $q = \exp(\Theta(\lambda \log^2 \lambda))$.
- **Direct lattice attack**: reduction up to block-size $\beta = \Theta(\lambda)$.

(Super-)Exponential q

- Consider $n = \Theta(\lambda^2 \log^2 \lambda)$ and $q = \exp(\Theta(\lambda \log^2 \lambda))$.
- **Direct lattice attack**: reduction up to block-size $\beta = \Theta(\lambda)$.
  - Expected norm for recovered vector:

$$\beta^{\Theta(n/\beta)} = \exp\left(\Theta(\lambda^2 \log^3 \lambda/\lambda)\right) > q.$$

(Super-)Exponential q

- Consider $n = \Theta(\lambda^2 \log^2 \lambda)$ and $q = \exp(\Theta(\lambda \log^2 \lambda))$.
- **Direct lattice attack**: reduction up to block-size $\beta = \Theta(\lambda)$.
  - Expected norm for recovered vector:

$$\beta^{\Theta(n/\beta)} = \exp\left(\Theta(\lambda^2 \log^3 \lambda/\lambda)\right) > q.$$

- **Subfield attack**: set $r = \Theta(\lambda)$ and $\beta = \Theta(\log \lambda)$.

(Super-)Exponential q

- Consider $n = \Theta(\lambda^2 \log^2 \lambda)$ and $q = \exp(\Theta(\lambda \log^2 \lambda))$.
- **Direct lattice attack**: reduction up to block-size $\beta = \Theta(\lambda)$.
  - Expected norm for recovered vector:

$$\beta^{\Theta(n/\beta)} = \exp\left(\Theta(\lambda^2 \log^3 \lambda/\lambda)\right) > q.$$

- **Subfield attack**: set $r = \Theta(\lambda)$ and $\beta = \Theta(\log \lambda)$.
  - Expected norm for recovered vector:

$$\beta^{\Theta(n/\beta r)} \cdot n^{\Theta(r)} = \exp\left(\Theta(\lambda \log \lambda \log\log \lambda)\right) < \sqrt{q}.$$

(Super-)Exponential q

- Consider $n = \Theta(\lambda^2 \log^2 \lambda)$ and $q = \exp(\Theta(\lambda \log^2 \lambda))$.
- **Direct lattice attack**: reduction up to block-size $\beta = \Theta(\lambda)$.
  - Expected norm for recovered vector:

$$\beta^{\Theta(n/\beta)} = \exp\left(\Theta(\lambda^2 \log^3 \lambda/\lambda)\right) > q.$$

- **Subfield attack**: set $r = \Theta(\lambda)$ and $\beta = \Theta(\log \lambda)$.
  - Expected norm for recovered vector:

$$\beta^{\Theta(n/\beta r)} \cdot n^{\Theta(r)} = \exp\left(\Theta(\lambda \log \lambda \log\log \lambda)\right) < \sqrt{q}.$$

- There is also a quasi-polynomial version for exponential q.

Quasi-polynomial q

- Consider $n = \Theta\left(\lambda \log^{\varepsilon} \lambda \log\log \lambda\right)$ and $q = \exp(\Theta(\log^{1+\varepsilon} \lambda))$

Quasi-polynomial q

- Consider $n = \Theta\left(\lambda \log^{\varepsilon} \lambda \log\log \lambda\right)$ and $q = \exp(\Theta(\log^{1+\varepsilon} \lambda))$
- **Direct lattice attack**: reduction up to block-size $\beta = \Theta(\lambda)$.

Quasi-polynomial q

- Consider $n = \Theta\left(\lambda \log^{\varepsilon} \lambda \log\log \lambda\right)$ and $q = \exp(\Theta(\log^{1+\varepsilon} \lambda))$
- **Direct lattice attack**: reduction up to block-size $\beta = \Theta(\lambda)$.
  - Expected norm of recovered vector:

$$\beta^{\Theta(n/\beta)} = \exp\left(\Theta\left(\log^{1+\varepsilon} \lambda \log\log \lambda\right)\right) > q.$$

Quasi-polynomial q

- Consider $n = \Theta\left(\lambda \log^{\varepsilon} \lambda \log\log \lambda\right)$ and $q = \exp(\Theta(\log^{1+\varepsilon} \lambda))$
- **Direct lattice attack**: reduction up to block-size $\beta = \Theta(\lambda)$.
  - Expected norm of recovered vector:

$$\beta^{\Theta(n/\beta)} = \exp\left(\Theta\left(\log^{1+\varepsilon} \lambda \log\log \lambda\right)\right) > q.$$

- **Subfield attack**: set $r = \Theta(\log^{2\varepsilon/3} \lambda)$ and $\beta = \Theta(\lambda/\log^{\varepsilon/3} \lambda)$.

Quasi-polynomial q

- Consider $n = \Theta\left(\lambda \log^{\varepsilon} \lambda \log\log \lambda\right)$ and $q = \exp(\Theta(\log^{1+\varepsilon} \lambda))$
- **Direct lattice attack**: reduction up to block-size $\beta = \Theta(\lambda)$.
  - Expected norm of recovered vector:

$$\beta^{\Theta(n/\beta)} = \exp\left(\Theta\left(\log^{1+\varepsilon} \lambda \log\log \lambda\right)\right) > q.$$

- **Subfield attack**: set $r = \Theta(\log^{2\varepsilon/3} \lambda)$ and $\beta = \Theta(\lambda/\log^{\varepsilon/3} \lambda)$.
  - Expected norm of recovered vector:

$$\beta^{\Theta(n/\beta r)} \cdot n^{\Theta(r)} = \exp\left(\Theta\left(\log^{1+\frac{2}{3}\varepsilon} \lambda \log\log \lambda\right)\right) < \sqrt{q}.$$

Outline

NTRU-based FHE: LTV

- NTRU-like schemes are used to realise fully homomorphic encryption starting with the LTV scheme.[17]
- LTV can evaluate circuits of depth $L = \mathcal{O}(n^{\varepsilon}/\log n)$ for $q = 2^{n^{\varepsilon}}$ with $\varepsilon \in (0, 1)$ and its decryption circuit can be implemented in depth $\mathcal{O}(\log\log q + \log n)$.
- This implies

$$(\varepsilon + 1)\log n < n^{\varepsilon}/\log n = \log q/\log n,$$

  i.e. q is super-polynomial in n for FHE.

[17] 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.

NTRU-based FHE: YASHE

- YASHE[18] reduces noise growth compared to LTV.
- This allows f and g to be sampled from a wide Gaussian.
- Sampling f and g this way allows to evaluate circuits of depth

$$L = \mathcal{O}\left(\frac{\log q}{\log\log q + \log n}\right).$$

- Under the same parameters as LTV, YASHE can evaluate circuits of depth $L = \mathcal{O}(\log q / \log n)$.

Usually YASHE uses short f and g, too, and q is super-polynomial in n for FHE.

---

[18] 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.

NTRU-based FHE: Attack

The subfield attack is subexponential in the security parameter λ for LTV and YASHE, if

1. L is sufficiently big to enable fully homomorphic encryption and
2. n is chosen to be minimal such that a lattice attack on the full field does not succeed.

Subfield Attack

Pick $\beta = \Theta\left(\lambda/\log^{1/3}\lambda\right)$ and $r = \Theta\left(\log^{\frac{2}{3}}\lambda\right)$ to obtain a vector $< \sqrt{q}$.

Graded Encoding Schemes

- Our attack also applies to Graded Encoding Schemes based on ideal lattices.[19]
- In these schemes, short elements $m_i \in \mathbb{Z}[X]/(X^n + 1)$ are encoded as

$$[(r_i \cdot g + m_i)/z]_q \in \mathcal{R}/q\mathcal{R}$$

  for some r_i, g with norms of size $\text{poly}(\lambda)$ and some random z.
- For correctness, the latest improvements require a modulus $q = \text{poly}(\lambda)^\kappa$, where κ is the multiplication degree.[20]

---

[19] 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.

[20] Martin R. Albrecht, Catalin Cocis, Fabien Laguillaumie, and Adeline Langlois. **Implementing Candidate Graded Encoding Schemes from Ideal Lattices**. In: *ASIACRYPT 2015, Part II*. ed. by Tetsu Iwata and Jung Hee Cheon. Vol. 9453. LNCS. Springer, Heidelberg, 2015, pp. 752–775. DOI: 10.1007/978-3-662-48800-3_31.

Graded Encoding Schemes: Attack

- Given encodings $x_0 = [(r_0 \cdot g + m_0)/z]_q$ and $x_1 = [(r_1 \cdot g + m_1)/z]_q$ for unknown $m_0, m_1 \neq 0$ we may consider the NTRU lattice Λ_h^q where $h = [x_0/x_1]_q$.
- The subfield lattice attack does not yield the vector $(r_0 \cdot g + m_0, r_1 \cdot g + m_1)$ but only

$$u \cdot (r_0 \cdot g + m_0, r_1 \cdot g + m_1).$$

- Two approaches to extend these elements to complete break:
  1. Solve a principal ideal problem (quantum polynomial-time attack).
  2. Use statistical leak via the Gentry-Szydlo algorithm[21], but this is just outside reach with current tools.

[21] Craig Gentry and Michael Szydlo. **Cryptanalysis of the Revised NTRU Signature Scheme**. In: *EUROCRYPT 2002*. Ed. by Lars R. Knudsen. Vol. 2332. LNCS. Springer, Heidelberg, 2002, pp. 299–320.

Outline

Practicality of the Attack

- We were able to break an instance with parameter $n = 2^{12}$, $q \approx 2^{190}$ in practice.
- Choosing a relative degree $r = 16$, the attack required to run LLL in 512 dimensions, which took 120 hours, single-threaded, using Sage and `Fplll`.
- The direct lattice reduction attack, according to root-hermite-factor based predictions[22], should have required running BKZ with block-size ≈ 130, and in 8192 dimensions. Such a computation has never been reported to have been completed.

[22] 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.

Obstructions to Concrete Predictions

There are two issues for predictions of how a given set of parameters would be affected.

1. We make use of LLL/BKZ in the approximation-factor regime, not in the Hermite-factor regime. While the behavior of LLL/BKZ is quite well modeled in the latter regime, we are not aware of precise models for the former.
2. We do not know the actual size of the shortest vector of $\Lambda^q_{h'}$, all we know is that it is no larger than (f', g').

Immunity of NTRU Encryption and BLISS Signature Schemes

- If (f', g') is not an unusually short vector of $\Lambda^q_{h'}$, then lattice reduction would not recover information on this vector.
- This happens when $\|(f', g')\| \approx \sigma^2 \cdot n' > \sqrt{n'q/\pi e}$.
- This is not the case of `NTRUencrypt`[23] or `Bliss`[24], where which (f', g') is an unusually short vector, but not by a large factor.

[23] Jeff Hoffstein et al. **Choosing Parameters for NTRUEncrypt**. Cryptology ePrint Archive, Report 2015/708. http://eprint.iacr.org/2015/708. 2015.

[24] 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.

When NTRU = Ring-LWE

- If $\sigma = \omega(q^{1/2})$ then h is statistically close to uniform and NTRU is as secure as Ring-LWE.[25]
- Immunity to our attack is achieved at $\sigma \approx \Theta(q^{1/4})$: h does not have enough entropy to be statistically close to random.
- But we might have enough entropy for the normed-down public key h' to be almost uniform.

[25] Damien Stehlé and Ron Steinfeld. **Making NTRU as Secure as Worst-Case Problems over Ideal Lattices**. In: *EUROCRYPT 2011*. Ed. by Kenneth G. Paterson. Vol. 6632. LNCS. Springer, Heidelberg, May 2011, pp. 27–47.

Attacks only get better

It is likely that the attack may be improved.

1. After having found several subfield solutions $(x', y') = v(f', g')$, run lattice reduction in the lattice $f' \cdot \mathcal{R}$ of dimension n'.
2. Improve lifting step when $\mathcal{R}'$ is a real subfield using the Gentry-Syzdlo algorithm[26] or by considering the relative norm equation problem[27] in general.

Recommendation

We therefore recommend that this set-up — NTRU assumption, presence of subfields, large modulus — be considered insecure.

[26] Craig Gentry and Michael Szydlo. **Cryptanalysis of the Revised NTRU Signature Scheme**. In: *EUROCRYPT 2002*. Ed. by Lars R. Knudsen. Vol. 2332. LNCS. Springer, Heidelberg, 2002, pp. 299–320.

[27] Claus Fieker, Andreas Jurk, and M Pohst. **On solving relative norm equations in algebraic number fields**. In: *Mathematics of Computation of the American Mathematical Society* 66.217 (1997), pp. 399–410.

Interesting Rings without Subfields

NTRU can is weaker than Ring-LWE in certain case. If you really want NTRU, you may consider:

$\mathcal{R} = \mathbb{Z}[X]/(X^p - X - 1)$ as suggested by Berstein,[28] but no roots unity nor non-trivial automorphisms. Lead to the design of NTRUprime[29].

$\mathbb{K} = \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ with safe prime p, remains Galois, automorphism group may allow a quantum worst-case (Ideal-SVP) to average-case reduction, $\mathbb{K}$ has no proper subfields.

---

[28] Dan Bernstein. **A subfield-logarithm attack against ideal lattices**. http://blog.cr.yp.to/20140213-ideal.html. 2014.

[29] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. **NTRU Prime**. Cryptology ePrint Archive, Report 2016/461. http://eprint.iacr.org/. 2016.

Thank You

Martin Albrecht, Shi Bai, and Léo Ducas. **A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and Graded Encoding Schemes**. In: *IACR Cryptology ePrint Archive* 2016 (2016). URL: http://ia.cr/2016/127