Revisiting Lattice Attacks on overstretched NTRU parameters

P. Kirchner & P-A. Fouque

Université de Rennes 1, France

EUROCRYPT 2017 – 05/01/17

Plan

1. Background on NTRU and Previous Attacks
2. A New Subring Attack
3. Simplification and Generalization
4. Prediction of our Attacks

NTRUEncrypt

Key Generation $\mathcal{R} = \mathbb{Z}[X]/(X^n + 1)$, modulus q, width 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 $c = 2(h \cdot s + e) + m$

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

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

NTRU lattice Λ_h^q

Recovering the secret key from the public key

$$\mathbf{A} = \begin{pmatrix} qI_n & M_h \\ 0 & I_n \end{pmatrix}$$

- The lattice Λ_h^q defined by $\mathbf{A}$ 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 the shortest vectors of Λ_h^q have norm $\approx \sqrt{nq}$
- While $\|f\| \approx \|g\| \approx \sqrt{n}\sigma \ll \sqrt{nq}$
- unusually short vectors: n vectors rotated of (f, g), $(x^i f, x^i g)$.

SS11 : for $\sigma \approx \sqrt{q}$, h is statistically indistinguisable from uniform, but NTRU chooses $f, g \in \{-1, 0, 1\}^n$!

NTRU lattice Λ_h^q

Recovering the secret key from the public key

$$\mathbf{A} = \begin{pmatrix} qI_n & M_h \\ 0 & I_n \end{pmatrix}$$

- The lattice Λ_h^q defined by $\mathbf{A}$ 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 the shortest vectors of Λ_h^q have norm $\approx \sqrt{nq}$
- While $\|f\| \approx \|g\| \approx \sqrt{n}\sigma \ll \sqrt{nq}$
- unusually short vectors: n vectors rotated of (f, g), $(x^i f, x^i g)$.

SS11 : for $\sigma \approx \sqrt{q}$, h is statistically indistinguisable from uniform, but NTRU chooses $f, g \in \{-1, 0, 1\}^n$!

NTRU lattice Λ_h^q

Recovering the secret key from the public key

$$\mathbf{A} = \begin{pmatrix} qI_n & M_h \\ 0 & I_n \end{pmatrix}$$

- The lattice Λ_h^q defined by $\mathbf{A}$ 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 the shortest vectors of Λ_h^q have norm $\approx \sqrt{nq}$
- While $\|f\| \approx \|g\| \approx \sqrt{n}\sigma \ll \sqrt{nq}$
- unusually short vectors: n vectors rotated of (f, g), $(x^i f, x^i g)$.

SS11 : for $\sigma \approx \sqrt{q}$, h is statistically indistinguisable from uniform, but NTRU chooses $f, g \in \{-1, 0, 1\}^n$!

NTRU lattice Λ_h^q

Recovering the secret key from the public key

$$\mathbf{A} = \begin{pmatrix} qI_n & M_h \\ 0 & I_n \end{pmatrix}$$

- The lattice Λ_h^q defined by $\mathbf{A}$ 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 the shortest vectors of Λ_h^q have norm $\approx \sqrt{nq}$
- While $\|f\| \approx \|g\| \approx \sqrt{n}\sigma \ll \sqrt{nq}$
- unusually short vectors: n vectors rotated of (f, g), $(x^i f, x^i g)$.

SS11 : for $\sigma \approx \sqrt{q}$, h is statistically indistinguisable from uniform, but NTRU chooses $f, g \in \{-1, 0, 1\}^n$!

NTRU Assumptions and Applications

Definition (NTRU Assumption)

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

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

$\mathcal{R} = \mathbb{Z}[X]/(P(X))$ and the promise a short solution (f, g) exists.

The NTRU assumption has been used for

- signature scheme: BLISS (Ducas, Durmus, Lepoint, Lyubashevsky), based on IBE (Ducas, Prest, Lyubashevsky)
- fully homomorphic encryption: LTV (Lopez-Alt, Tromer and Vaikuntanathan), YASHE (Bos, Lauter, Loftus, Naehrig)
- multilinear Maps from Ideal Lattices: GGH13

With very large modulus q compared to NTRUEncrypt!

NTRU Assumptions and Applications

Definition (NTRU Assumption)

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

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

$\mathcal{R} = \mathbb{Z}[X]/(P(X))$ and the promise a short solution (f, g) exists.

The NTRU assumption has been used for

- signature scheme: BLISS (Ducas, Durmus, Lepoint, Lyubashevsky), based on IBE (Ducas, Prest, Lyubashevsky)
- fully homomorphic encryption: LTV (Lopez-Alt, Tromer and Vaikuntanathan), YASHE (Bos, Lauter, Loftus, Naehrig)
- multilinear Maps from Ideal Lattices: GGH13

With very large modulus q compared to NTRUEncrypt!

NTRU Assumptions and Applications

Definition (NTRU Assumption)

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

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

$\mathcal{R} = \mathbb{Z}[X]/(P(X))$ and the promise a short solution (f, g) exists.

The NTRU assumption has been used for

- signature scheme: BLISS (Ducas, Durmus, Lepoint, Lyubashevsky), based on IBE (Ducas, Prest, Lyubashevsky)
- fully homomorphic encryption: LTV (Lopez-Alt, Tromer and Vaikuntanathan), YASHE (Bos, Lauter, Loftus, Naehrig)
- multilinear Maps from Ideal Lattices: GGH13

With very large modulus q compared to NTRUEncrypt!

Current Attacks on NTRU

- Recovering a short enough vector larger than (f, g) is sufficient to recover the secret key
- Finding a $o(q)$ vector would break many applications such as encryption
- Previous Lattice attacks:
  1. Direct Approach: we need a strong lattice reduction and NTRU is still secure
  2. May increases the $\lambda_1(L)/\lambda_2(L)$ by avoiding the rotated vectors and reduces the dimension by projecting the lattice
  3. Howgrave-Graham combines lattice-reduction and MITM: first reduces a submatrice in the middle of the lattice L

Asymptotically BKW variant: heuristic complexity of $2^{\Theta(n/\log\log q)}$

Current Attacks on NTRU

- Recovering a short enough vector larger than (f, g) is sufficient to recover the secret key
- Finding a $o(q)$ vector would break many applications such as encryption
- Previous Lattice attacks:
  1. Direct Approach: we need a strong lattice reduction and NTRU is still secure
  2. May increases the $\lambda_1(L)/\lambda_2(L)$ by avoiding the rotated vectors and reduces the dimension by projecting the lattice
  3. Howgrave-Graham combines lattice-reduction and MITM: first reduces a submatrice in the middle of the lattice L

Asymptotically BKW variant: heuristic complexity of $2^{\Theta(n/\log\log q)}$

Current Attacks on NTRU

- Recovering a short enough vector larger than (f, g) is sufficient to recover the secret key
- Finding a $o(q)$ vector would break many applications such as encryption
- Previous Lattice attacks:
  1. Direct Approach: we need a strong lattice reduction and NTRU is still secure
  2. May increases the $\lambda_1(L)/\lambda_2(L)$ by avoiding the rotated vectors and reduces the dimension by projecting the lattice
  3. Howgrave-Graham combines lattice-reduction and MITM: first reduces a submatrice in the middle of the lattice L

Asymptotically BKW variant: heuristic complexity of $2^{\Theta(n/\log\log q)}$

Subfield Attack

- Lattice reduction in a subfield to attack the NTRU assumption for large moduli q and $\sigma < q^{1/4}$
- Strategy: Reducing the dimension allows faster algorithms
  1. Map a NTRU instance to the chosen subfield (dim. $n/2$)
  2. Apply lattice reduction
  3. Lift the solution to the full field

- Albrecht, Bai, Ducas rediscovered this attack already sketched by Gentry, Szydlo, Jonsson, Nguyen and Stern
- Cheon, Jeong and Lee discovered a variant using the Trace instead of the Norm
- Work with any coefficient of the characteristic polynomial

Subfield Attack

- Lattice reduction in a subfield to attack the NTRU assumption for large moduli q and $\sigma < q^{1/4}$
- Strategy: Reducing the dimension allows faster algorithms
  1. Map a NTRU instance to the chosen subfield (dim. $n/2$)
  2. Apply lattice reduction
  3. Lift the solution to the full field

- Albrecht, Bai, Ducas rediscovered this attack already sketched by Gentry, Szydlo, Jonsson, Nguyen and Stern
- Cheon, Jeong and Lee discovered a variant using the Trace instead of the Norm
- Work with any coefficient of the characteristic polynomial

Subfield Attack

- Lattice reduction in a subfield to attack the NTRU assumption for large moduli q and $\sigma < q^{1/4}$
- Strategy: Reducing the dimension allows faster algorithms
  1. Map a NTRU instance to the chosen subfield (dim. $n/2$)
  2. Apply lattice reduction
  3. Lift the solution to the full field

- Albrecht, Bai, Ducas rediscovered this attack already sketched by Gentry, Szydlo, Jonsson, Nguyen and Stern
- Cheon, Jeong and Lee discovered a variant using the Trace instead of the Norm
- Work with any coefficient of the characteristic polynomial

Cyclotomic Number Field

- $\mathbb{K} = \mathbb{Q}[\omega_n] \simeq \mathbb{Q}[X]/(\Phi_n(X))$ where $\omega_n = \exp(2i\pi/n)$
- $\mathbb{L} = \mathbb{Q}(\omega_n + \bar{\omega_n})$: maximal real subfield of $\mathbb{K}$ of dim. $(n-1)/2$

- Conjugate: $\bar{a} = a_0 + \sum_{i=1}^{\phi(n)-1} a_i X^{\phi(n)-i}$ for $a = \sum_{i=0}^{\phi(n)-1} a_i X^i$
- $N_{\mathbb{K}/\mathbb{L}}(a) = a\bar{a} \in \mathbb{L}$
- More generally, if $\mathbb{L}$ subfield of $\mathbb{K}$ of dim. m and $r = n/m$, $N_{\mathbb{K}/\mathbb{L}}(a) = \Pi_{\sigma \in H} \sigma(a)$ for H fixing $\mathbb{L}$

- Ring of integers: $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\omega_n] = \{a \in \mathbb{K} : f_{\mathbb{Q}}^a \in \mathbb{Z}[X]\}$ where $f_{\mathbb{Q}}^a$ is the monic irreducible minimal polynomial of a over $\mathbb{Q}$
- Ideal $g\mathcal{O}_{\mathbb{K}}$ can be represented by a lattice: multiplication matrix by g in $\mathcal{O}_{\mathbb{K}}$

Cyclotomic Number Field

- $\mathbb{K} = \mathbb{Q}[\omega_n] \simeq \mathbb{Q}[X]/(\Phi_n(X))$ where $\omega_n = \exp(2i\pi/n)$
- $\mathbb{L} = \mathbb{Q}(\omega_n + \bar{\omega_n})$: maximal real subfield of $\mathbb{K}$ of dim. $(n-1)/2$

- Conjugate: $\bar{a} = a_0 + \sum_{i=1}^{\phi(n)-1} a_i X^{\phi(n)-i}$ for $a = \sum_{i=0}^{\phi(n)-1} a_i X^i$
- $N_{\mathbb{K}/\mathbb{L}}(a) = a\bar{a} \in \mathbb{L}$
- More generally, if $\mathbb{L}$ subfield of $\mathbb{K}$ of dim. m and $r = n/m$, $N_{\mathbb{K}/\mathbb{L}}(a) = \Pi_{\sigma \in H} \sigma(a)$ for H fixing $\mathbb{L}$

- Ring of integers: $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\omega_n] = \{a \in \mathbb{K} : f_{\mathbb{Q}}^a \in \mathbb{Z}[X]\}$ where $f_{\mathbb{Q}}^a$ is the monic irreducible minimal polynomial of a over $\mathbb{Q}$
- Ideal $g\mathcal{O}_{\mathbb{K}}$ can be represented by a lattice: multiplication matrix by g in $\mathcal{O}_{\mathbb{K}}$

Cyclotomic Number Field

- $\mathbb{K} = \mathbb{Q}[\omega_n] \simeq \mathbb{Q}[X]/(\Phi_n(X))$ where $\omega_n = \exp(2i\pi/n)$
- $\mathbb{L} = \mathbb{Q}(\omega_n + \bar{\omega_n})$: maximal real subfield of $\mathbb{K}$ of dim. $(n-1)/2$

- Conjugate: $\bar{a} = a_0 + \sum_{i=1}^{\phi(n)-1} a_i X^{\phi(n)-i}$ for $a = \sum_{i=0}^{\phi(n)-1} a_i X^i$
- $N_{\mathbb{K}/\mathbb{L}}(a) = a\bar{a} \in \mathbb{L}$
- More generally, if $\mathbb{L}$ subfield of $\mathbb{K}$ of dim. m and $r = n/m$, $N_{\mathbb{K}/\mathbb{L}}(a) = \Pi_{\sigma \in H} \sigma(a)$ for H fixing $\mathbb{L}$

- Ring of integers: $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\omega_n] = \{a \in \mathbb{K} : f_{\mathbb{Q}}^a \in \mathbb{Z}[X]\}$ where $f_{\mathbb{Q}}^a$ is the monic irreducible minimal polynomial of a over $\mathbb{Q}$
- Ideal $g\mathcal{O}_{\mathbb{K}}$ can be represented by a lattice: multiplication matrix by g in $\mathcal{O}_{\mathbb{K}}$

Analysis

Consider the lattice generated by this matrix

$$\mathbf{A}_{norm} = \begin{pmatrix} q I_{n/r} & M^{\mathcal{O}_{\mathbb{L}}}_{N_{\mathbb{K}/\mathbb{L}}(h)} \\ 0 & I_{n/r} \end{pmatrix} \text{ where } N_{\mathbb{K}/\mathbb{L}}(h) \in \mathcal{O}_{\mathbb{L}}.$$

- $(N_{\mathbb{K}/\mathbb{L}}(f), N_{\mathbb{K}/\mathbb{L}}(g))$ is contained in this lattice.
- expect short vector $\approx q^{n/(2n)}\sqrt{2n/(2\pi re)} = \sqrt{qn/(\pi re)}$
- For $\mathbb{L}$ real subfield of $\mathbb{K}$, if $\|f\| > \sqrt{n}$ and as $f\bar{f} \geqslant \|f\|^2 = n$, but since $n \geqslant q/2$, the attack does not work on NTRU parameters

But with very large modulus q, $N_{\mathbb{K}/\mathbb{L}}(f) = f\bar{f}$ is smaller than the expected short vector !

Analysis

Consider the lattice generated by this matrix

$$\mathbf{A}_{norm} = \begin{pmatrix} q I_{n/r} & M^{\mathcal{O}_{\mathbb{L}}}_{N_{\mathbb{K}/\mathbb{L}}(h)} \\ 0 & I_{n/r} \end{pmatrix} \text{ where } N_{\mathbb{K}/\mathbb{L}}(h) \in \mathcal{O}_{\mathbb{L}}.$$

- $(N_{\mathbb{K}/\mathbb{L}}(f), N_{\mathbb{K}/\mathbb{L}}(g))$ is contained in this lattice.
- expect short vector $\approx q^{n/(2n)}\sqrt{2n/(2\pi re)} = \sqrt{qn/(\pi re)}$
- For $\mathbb{L}$ real subfield of $\mathbb{K}$, if $\|f\| > \sqrt{n}$ and as $f\bar{f} \geqslant \|f\|^2 = n$, but since $n \geqslant q/2$, the attack does not work on NTRU parameters

But with very large modulus q, $N_{\mathbb{K}/\mathbb{L}}(f) = f\bar{f}$ is smaller than the expected short vector !

Analysis

Consider the lattice generated by this matrix

$$\mathbf{A}_{norm} = \begin{pmatrix} qI_{n/r} & M^{\mathcal{O}_{\mathbb{L}}}_{N_{\mathbb{K}/\mathbb{L}}(h)} \\ 0 & I_{n/r} \end{pmatrix} \text{ where } N_{\mathbb{K}/\mathbb{L}}(h) \in \mathcal{O}_{\mathbb{L}}.$$

- $(N_{\mathbb{K}/\mathbb{L}}(f), N_{\mathbb{K}/\mathbb{L}}(g))$ is contained in this lattice.
- expect short vector $\approx q^{n/(2n)}\sqrt{2n/(2\pi re)} = \sqrt{qn/(\pi re)}$
- For $\mathbb{L}$ real subfield of $\mathbb{K}$, if $\|f\| > \sqrt{n}$ and as $f\bar{f} \geqslant \|f\|^2 = n$, but since $n \geqslant q/2$, the attack does not work on NTRU parameters

But with very large modulus q, $N_{\mathbb{K}/\mathbb{L}}(f) = f\bar{f}$ is smaller than the expected short vector !

Subfield attack

Consider the lattice generated by this matrix

$$\mathbf{A}_{norm} = \begin{pmatrix} qI_{n/r} & M^{\mathcal{O}_{\mathbb{L}}}_{N_{\mathbb{K}/\mathbb{L}}(h)} \\ 0 & I_{n/r} \end{pmatrix} \text{ where } N_{\mathbb{K}/\mathbb{L}}(h) \in \mathcal{O}_{\mathbb{L}}.$$

- $(f' = N_{\mathbb{K}/\mathbb{L}}(f), g' = N_{\mathbb{K}/\mathbb{L}}(g)) \in \Lambda(\mathbf{A}_{norm})$
- $\|f'\| \approx (\sigma n)^r$ where $r = [\mathbb{K} : \mathbb{L}]$
- solution returned by BKZ: $\|(x', y')\| \leqslant \beta^{\Theta(n/\beta r)} \cdot (n\sigma)^{\Theta(r)}$
- if $\|(x', y')\| < q/\|(f', g')\|$, $(x', y') = v(f', g')$ for $v \in \mathcal{O}_{\mathbb{L}}$

Efficient: small dimension $(2n/r)$ and lifting the solution to $\mathbb{K}$

Subfield attack

Consider the lattice generated by this matrix

$$\mathbf{A}_{norm} = \begin{pmatrix} qI_{n/r} & M^{\mathcal{O}_{\mathbb{L}}}_{N_{\mathbb{K}/\mathbb{L}}(h)} \\ 0 & I_{n/r} \end{pmatrix} \text{ where } N_{\mathbb{K}/\mathbb{L}}(h) \in \mathcal{O}_{\mathbb{L}}.$$

- $(f' = N_{\mathbb{K}/\mathbb{L}}(f), g' = N_{\mathbb{K}/\mathbb{L}}(g)) \in \Lambda(\mathbf{A}_{norm})$
- $\|f'\| \approx (\sigma n)^r$ where $r = [\mathbb{K} : \mathbb{L}]$
- solution returned by BKZ: $\|(x', y')\| \leqslant \beta^{\Theta(n/\beta r)} \cdot (n\sigma)^{\Theta(r)}$
- if $\|(x', y')\| < q/\|(f', g')\|$, $(x', y') = v(f', g')$ for $v \in \mathcal{O}_{\mathbb{L}}$

Efficient: small dimension $(2n/r)$ and lifting the solution to $\mathbb{K}$

Subfield attack

- Condition to work: $\sqrt{q} = \beta^{\Theta(2n/(r\beta))} \cdot n^{\Theta(r)}$ when $\sigma = poly(n)$
  1. Faster than the direct attack with dim. $2n$ when q super-polynomial:
     - Subfield: $\beta / \log \beta = \Theta(n \log n / \log^2 q)$ for $r = \Theta(\log q / \log n)$
     - Direct: $\beta / \log \beta = \Theta(n / \log q)$
  2. Quasi-polynomial time when q is exponential in n

Reparations

- $\mathcal{R} = \mathbb{Z}[X]/(X^p - X - 1)$ as suggested by Bernstein *et al.*: NTRUprime
- $\mathbb{K} = \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ with safe prime p: Galois with no subfield

Subfield attack

- Condition to work: $\sqrt{q} = \beta^{\Theta(2n/(r\beta))} \cdot n^{\Theta(r)}$ when $\sigma = poly(n)$
  1. Faster than the direct attack with dim. $2n$ when q super-polynomial:
     - Subfield: $\beta / \log \beta = \Theta(n \log n / \log^2 q)$ for $r = \Theta(\log q / \log n)$
     - Direct: $\beta / \log \beta = \Theta(n / \log q)$
  2. Quasi-polynomial time when q is exponential in n

Reparations

- $\mathcal{R} = \mathbb{Z}[X]/(X^p - X - 1)$ as suggested by Bernstein *et al.*: NTRUprime
- $\mathbb{K} = \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ with safe prime p: Galois with no subfield

New Subring Attack

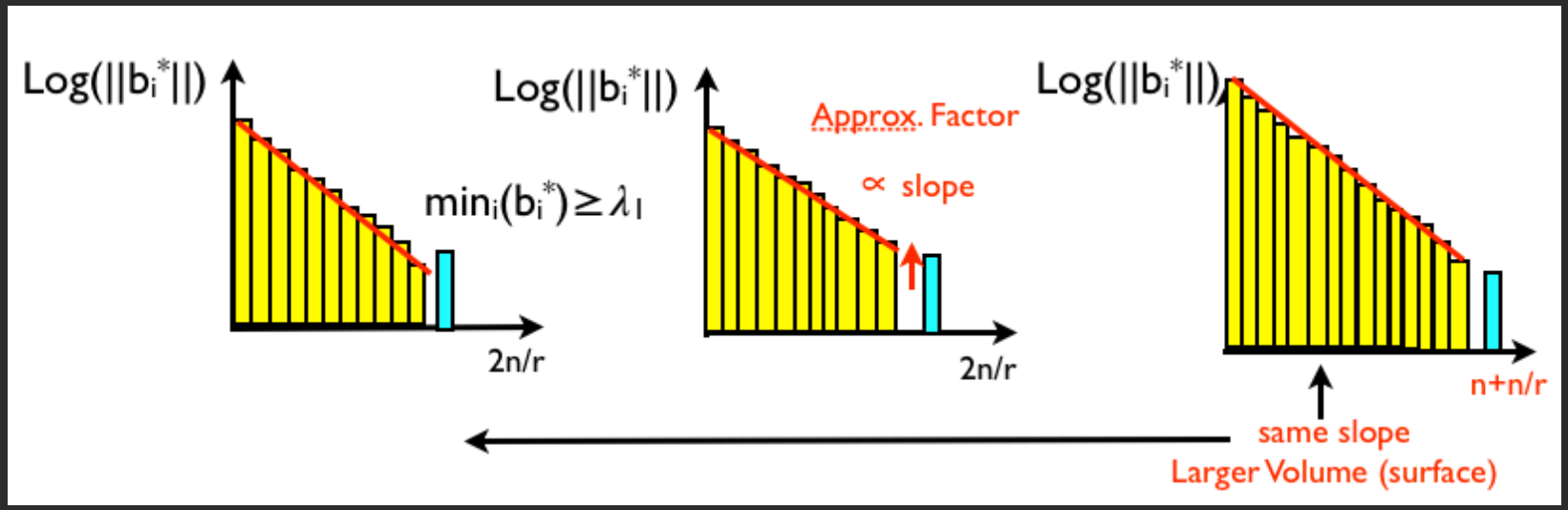
$$\mathbf{A} = \begin{pmatrix} q I_n & M_h^{\mathcal{O}_{\mathbb{L}}} \\ 0 & I_{n/r} \end{pmatrix}$$

- Original lattice but we put $M_h^{\mathcal{O}_{\mathbb{L}}}$ in a subring of $\mathcal{O}_{\mathbb{K}}$
- For any $g \in \mathcal{O}$, $N_{\mathbb{K}/\mathbb{L}}(g) \in g\mathcal{O} \cap \mathcal{O}_{\mathbb{L}}$
- We show that $(fN_{\mathbb{K}/\mathbb{L}}(g)/g, N_{\mathbb{K}/\mathbb{L}}(g)) \in \Lambda(\mathbf{A})$ and is short

Efficiency ? Subfield attack dim. is $2n/r$ instead $n + n/r$?

New Subring Attack

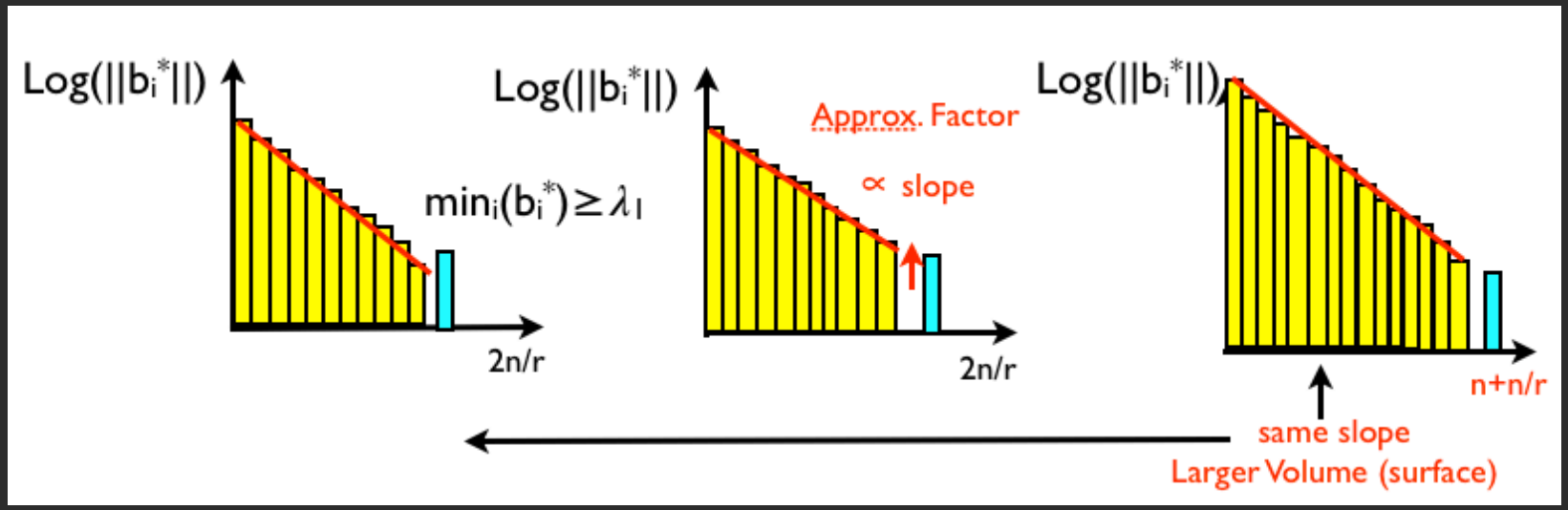
Runtime of lattice reduction depends on the dimension and approx. factor (slope of the line)



- Increase the volume of the lattice
- Use a projected lattice to reduce the dimension !

New Subring Attack

Runtime of lattice reduction depends on the dimension and approx. factor (slope of the line)



- Increase the volume of the lattice
- Use a projected lattice to reduce the dimension !

New Subring Attack

$$\mathbf{A} = \begin{pmatrix} q I_n & M_h^{\mathcal{O}_{\mathbb{L}}} \\ 0 & I_{n/r} \end{pmatrix}$$

- This approach is more flexible: it allows to reduce the dimension and the number of coordinates !
- Projected Lattice: extract the last d rows and columns
- Heuristic: If the algorithm finds a vector shorter than the Minkowski bound, it is a multiple of the key
- if $\log \sigma = \Theta(\log n)$, poly-time algo when $q = 2^{\Omega(\sqrt{n \log \log n})}$
- if $\sigma = \Theta(\sqrt{n})$, faster algo. as soon as $q \geqslant n^{\Theta(\sqrt{\log \log n})}$
- $\beta / \log \beta = \Theta(n \log \sigma / \log^2 q)$ and $d \geqslant 2n/r$

New Subring Attack

$$\mathbf{A} = \begin{pmatrix} q I_n & M_h^{\mathcal{O}_{\mathbb{L}}} \\ 0 & I_{n/r} \end{pmatrix}$$

- This approach is more flexible: it allows to reduce the dimension and the number of coordinates !
- Projected Lattice: extract the last d rows and columns
- Heuristic: If the algorithm finds a vector shorter than the Minkowski bound, it is a multiple of the key
- if $\log \sigma = \Theta(\log n)$, poly-time algo when $q = 2^{\Omega(\sqrt{n \log \log n})}$
- if $\sigma = \Theta(\sqrt{n})$, faster algo. as soon as $q \geqslant n^{\Theta(\sqrt{\log \log n})}$
- $\beta / \log \beta = \Theta(n \log \sigma / \log^2 q)$ and $d \geqslant 2n/r$

Simplification and Generalization

Are these attacks better than other practical attacks NTRU: the lattice reduction step of the hybrid attack ?

$$\mathbf{A} = \begin{pmatrix} qI_n & M_h^{\mathcal{O}_{\mathbb{K}}} \\ 0 & I_n \end{pmatrix}$$

There are n short vectors rotated of (f, g), $(x^i f, x^i g)$.

- Finding a vector in a sublattice of low volume for lattice reduction algo. depends on the rank of the sublattice
- Previous analysis restrict to the special case of rank one
- Pataki & Tural: the volume of the sublattice generated by r vectors is larger than the product of the r smallest GS norms

Simplification and Generalization

Are these attacks better than other practical attacks NTRU: the lattice reduction step of the hybrid attack ?

$$\mathbf{A} = \begin{pmatrix} qI_n & M_h^{\mathcal{O}_{\mathbb{K}}} \\ 0 & I_n \end{pmatrix}$$

There are n short vectors rotated of (f, g), $(x^i f, x^i g)$.

- Finding a vector in a sublattice of low volume for lattice reduction algo. depends on the rank of the sublattice
- Previous analysis restrict to the special case of rank one
- Pataki & Tural: the volume of the sublattice generated by r vectors is larger than the product of the r smallest GS norms

Simplification and Generalization

Are these attacks better than other practical attacks NTRU: the lattice reduction step of the hybrid attack ?

$$\mathbf{A} = \begin{pmatrix} qI_n & M_h^{\mathcal{O}_{\mathbb{K}}} \\ 0 & I_n \end{pmatrix}$$

There are n short vectors rotated of (f, g), $(x^i f, x^i g)$.

- Finding a vector in a sublattice of low volume for lattice reduction algo. depends on the rank of the sublattice
- Previous analysis restrict to the special case of rank one
- Pataki & Tural: the volume of the sublattice generated by r vectors is larger than the product of the r smallest GS norms

Simplification and Generalization

Are these attacks better than other practical attacks NTRU: the lattice reduction step of the hybrid attack ?

$$\mathbf{A} = \begin{pmatrix} qI_n & M_h^{\mathcal{O}_{\mathbb{K}}} \\ 0 & I_n \end{pmatrix}$$

1. We reduce the middle of the matrix $\mathbf{A}$
2. Same efficiency w/o subfield with an orthogonal basis of $\mathcal{O}$

Recovery: half of $f\mathcal{O}$ and $g\mathcal{O}$ and heuristically the middle matrix is a basis of $(f, g)\mathcal{O}$

Experiments on NTRU

$\log n$	$\log q$	$\log r$	Success	Method	Coordinates	Origin
11	165	4	Yes	ABD16	128	-
11	115	4	Yes	Ours	510	-
11	114	4	No	Ours	630	-
11	95	3	Yes	ABD16	256	-
11	81	3	Yes	Ours	600	-
11	80	3	No	Ours	600	-
11	79	3	No	Ours	860	YASHE
11	70	2	Yes	Ours	600	-
11	69	2	No	Ours	600	-
12	190	4	Yes	ABD16	256	-
12	157	4	Yes	Ours	430	YASHE
12	144	4	Yes	Ours	850	-
12	143	4	No	Ours	850	-
13	383	4	Yes	Ours	512	Dowlin
13	312	5	Yes	Ours	470	YASHE

Experiments and Prediction

$\log n$	$\log q$	$\log r$	Success	Method	Coordinates	Origin
14	622	5	Yes	Ours	470	YASHE
15	1271	5	Yes	Ours	512	Doroz
15	1243	6	Yes	Ours	660	YASHE
16	2485	7	Yes	Ours	820	YASHE

$\log n$	Prediction	$\log r$
11	116	4
11	82	3
11	71	2
12	146	4

Experiments on NTRUprime with Large Moduli

$\log n$	$\log q$	ℓ	Success
11	72	1116	Yes
11	70	1200	Yes
11	69	1200	No
12	118	1024	Yes
12	117	1024	No
12	105	1700	Yes
12	104	1700	No
13	230	1024	Yes
14	450	1024	Yes
15	930	1024	Yes

$\log n$	ℓ	Prediction
11	1033	71
12	1472	106
13	2275	156
14	3357	230
15	5127	337
16	7124	477

Conclusion

Provable Security and Attack

- The property that we use is present until $\sigma \approx \sqrt{nq}$
- Stehlé and Steinfeld prove security for $\sigma \approx \sqrt{n^3 q}$
- Attack: more efficient on NTRU than Ring-LWE $\sigma \lesssim \sqrt{q}/n$
- Standard cryptography (signature, key exchange and IBE) use modulus $q \leqslant n^2$ and attack doesn't apply

Conclusion

- Subfield attack and our subring attack are slower than the direct attack with projection
- We broke many instantiations of FHE schemes in practice
- First time: n rotated small vectors are useful to analyze the security of NTRU !