Quantum Key Search for Ternary LWE

ia.cr/2021/865

Iggy van Hoof, Elena Kirshanova, and Alexander May

2021, July 20th

Introduction

- We Modified “Meet-LWE” [May2021] to the quantum setting.
- This algorithm attacks ternary LWE, including NTRU.
- Classical algorithm solves LWE in $\mathcal{S}^{0.24}$.

Introduction

- We Modified "Meet-LWE" [May2021] to the quantum setting.
- This algorithm attacks ternary LWE, including NTRU.
- Classical algorithm solves LWE in $\mathcal{S}^{0.24}$.
- Quantum algorithm solves LWE in $\mathcal{S}^{0.19}$.

Introduction

- We Modified “Meet-LWE” [May2021] to the quantum setting.
- This algorithm attacks ternary LWE, including NTRU.
- Classical algorithm solves LWE in $\mathcal{S}^{0.24}$.
- Quantum algorithm solves LWE in $\mathcal{S}^{0.19}$.
- Different approach than the current best attacks.
- NTRU still quantum secure.

LWE

- Public $A \in \mathbb{Z}_q^{n \times n}, b \in \mathbb{Z}_q^n$.
- Solve $As = b + e \mod q$ where $s \in \mathbb{Z}_q^n, e \in \mathbb{Z}_q^n$ are the secret key.
- NTRU: $n = 509, q = 2048$.

LWE

- Public $A \in \mathbb{Z}_q^{n \times n}, b \in \mathbb{Z}_q^n$.
- Solve $As = b + e \mod q$ where $s \in \mathbb{Z}_q^n, e \in \mathbb{Z}_q^n$ are the secret key.
- NTRU: $n = 509, q = 2048$.
- Ternary if $s, e \in \{-1, 0, 1\}^n$.
- We also know the *weight* w of s.
- NTRU: $w = 254$.

LWE

- Public $A \in \mathbb{Z}_q^{n \times n}, b \in \mathbb{Z}_q^n$.
- Solve $As = b + e \mod q$ where $s \in \mathbb{Z}_q^n, e \in \mathbb{Z}_q^n$ are the secret key.
- NTRU: $n = 509, q = 2048$.
- Ternary if $s, e \in \{-1, 0, 1\}^n$.
- We also know the *weight* w of s.
- NTRU: $w = 254$.
- We assume s has an equal number of 1 and -1 entries.
- NTRU: 127 1s, 127 -1s, 255 0s.

LWE

- Public $A \in \mathbb{Z}_q^{n \times n}, b \in \mathbb{Z}_q^n$.
- Solve $As = b + e \mod q$ where $s \in \mathbb{Z}_q^n, e \in \mathbb{Z}_q^n$ are the secret key.
- NTRU: $n = 509, q = 2048$.
- Ternary if $s, e \in \{-1, 0, 1\}^n$.
- We also know the *weight* w of s.
- NTRU: $w = 254$.
- We assume s has an equal number of 1 and -1 entries.
- NTRU: 127 1s, 127 -1s, 255 0s.
- Number of possible s: $\mathcal{S} = \binom{n}{w/2}\binom{n-w/2}{w/2}$.
- NTRU: $\mathcal{S} \approx 2^{754}$.

Odlyzko's MitM attack

- Meet in the middle [HPS98]: split $s = (s_1, s_2)$.

Odlyzko's MitM attack

- Meet in the middle [HPS98]: split $s = (s_1, s_2)$.
- Where $s_1, s_2 \in \mathbb{Z}_q^{n/2}$.
- Weight $\frac{w}{2}$ each, balanced.

Odlyzko's MitM attack

- Meet in the middle [HPS98]: split $s = (s_1, s_2)$.
- Where $s_1, s_2 \in \mathbb{Z}_q^{n/2}$.
- Weight $\frac{w}{2}$ each, balanced.
- Permutations poly(n).

Odlyzko's MitM attack

- Meet in the middle [HPS98]: split $s = (s_1, s_2)$.
- Where $s_1, s_2 \in \mathbb{Z}_q^{n/2}$.
- Weight $\frac{w}{2}$ each, balanced.
- Permutations poly(n).
- Try to find solutions to $A_1 s_1 \approx b - A_2 s_2$ using locality sensitive hashing.

Odlyzko's MitM attack

- Meet in the middle [HPS98]: split $s = (s_1, s_2)$.
- Where $s_1, s_2 \in \mathbb{Z}_q^{n/2}$.
- Weight $\frac{w}{2}$ each, balanced.
- Permutations poly(n).
- Try to find solutions to $A_1 s_1 \approx b - A_2 s_2$ using locality sensitive hashing.
- Time & space complexity for NTRU with $n = 509, q = 2048, w = 254$:

$$2^{377} = \mathcal{S}^{\frac{1}{2}}.$$

Quantum Odlyzko

- How do we turn this quantum?

Quantum Odlyzko

- How do we turn this quantum?
- Idea: quantum random walk.

Quantum Odlyzko

- How do we turn this quantum?
- Idea: quantum random walk.
  - What do we walk over?

Quantum Odlyzko

- How do we turn this quantum?
- Idea: quantum random walk.
  - What do we walk over?
  - What do we want to find?

Quantum Odlyzko

- How do we turn this quantum?
- Idea: quantum random walk.
    - What do we walk over?
    - What do we want to find?
    - What is the speedup?

Quantum random walks

- We have a graph $G = (V, E)$.

Quantum random walks

- We have a graph $G = (V, E)$.
- Vertices $v \in V$: subsets of all s_1, s_2.
- L is the size of all s_1.

Quantum random walks

- We have a graph $G = (V, E)$.
- Vertices $v \in V$: subsets of all s_1, s_2.
- L is the size of all s_1.
- We make the subsets all size L^γ.

Quantum random walks

- We have a graph $G = (V, E)$.
- Vertices $v \in V$: subsets of all s_1, s_2.
- L is the size of all s_1.
- We make the subsets all size L^γ.
- Edge $(u, v) \in E$ iff $|\Delta(u, v)| = 1$.

Quantum random walks

- We have a graph $G = (V, E)$.
- Vertices $v \in V$: subsets of all s_1, s_2.
- L is the size of all s_1.
- We make the subsets all size L^γ.
- Edge $(u, v) \in E$ iff $|\Delta(u, v)| = 1$.
- Try to find u containing (s_1, s_2) as the secret key.

Quantum random walks

- We have a graph $G = (V, E)$.
- Vertices $v \in V$: subsets of all s_1, s_2.
- L is the size of all s_1.
- We make the subsets all size L^γ.
- Edge $(u, v) \in E$ iff $|\Delta(u, v)| = 1$.
- Try to find u containing (s_1, s_2) as the secret key.
- Random walk: keep a single subset in memory.

Quantum random walks

- We have a graph $G = (V, E)$.
- Vertices $v \in V$: subsets of all s_1, s_2.
- L is the size of all s_1.
- We make the subsets all size L^γ.
- Edge $(u, v) \in E$ iff $|\Delta(u, v)| = 1$.
- Try to find u containing (s_1, s_2) as the secret key.
- Random walk: keep a single subset in memory.
- Quantum random walk: create a superposition over all subsets.
- Use Johnson graph: $\gamma = 2/3$ optimal for quantum.

Quantum random walks

- We have a graph $G = (V, E)$.
- Vertices $v \in V$: subsets of all s_1, s_2.
- L is the size of all s_1.
- We make the subsets all size L^γ.
- Edge $(u, v) \in E$ iff $|\Delta(u, v)| = 1$.
- Try to find u containing (s_1, s_2) as the secret key.
- Random walk: keep a single subset in memory.
- Quantum random walk: create a superposition over all subsets.
- Use Johnson graph: $\gamma = 2/3$ optimal for quantum.
- For our NTRU example: $2^{252} = \mathcal{S}^{1/3}$.

Meet-LWE

Big picture idea

- Split $s = s_1 + s_2$ with $s_1, s_2 \in \mathbb{Z}_q^n$, weight $\frac{w}{2}$.

Meet-LWE

Big picture idea

- Split $s = s_1 + s_2$ with $s_1, s_2 \in \mathbb{Z}_q^n$, weight $\frac{w}{2}$.
- Guess r entries of e.
- Example: guess 23/509.

Meet-LWE

Big picture idea

- Split $s = s_1 + s_2$ with $s_1, s_2 \in \mathbb{Z}_q^n$, weight $\frac{w}{2}$.
- Guess r entries of e.
- Example: guess 23/509.
- Set $t \in \mathbb{Z}_q^r$.

Meet-LWE

Big picture idea

- Split $s = s_1 + s_2$ with $s_1, s_2 \in \mathbb{Z}_q^n$, weight $\frac{w}{2}$.
- Guess r entries of e.
- Example: guess 23/509.
- Set $t \in \mathbb{Z}_q^r$.
- Try to find s_1, s_2 s.t.

$$\pi_r \left(As_1^{(1)} + e_1 \right) \mod q = t = \pi_r \left(b - As_2^{(1)} + e_2 \right) \mod q.$$

Meet-LWE

Big picture idea

- Split $s = s_1 + s_2$ with $s_1, s_2 \in \mathbb{Z}_q^n$, weight $\frac{w}{2}$.
- Guess r entries of e.
- Example: guess $23/509$.
- Set $t \in \mathbb{Z}_q^r$.
- Try to find s_1, s_2 s.t.

$$\pi_r\left(As_1^{(1)} + e_1\right) \mod q = t = \pi_r\left(b - As_2^{(1)} + e_2\right) \mod q.$$

- Do this recursively.

Meet-LWE

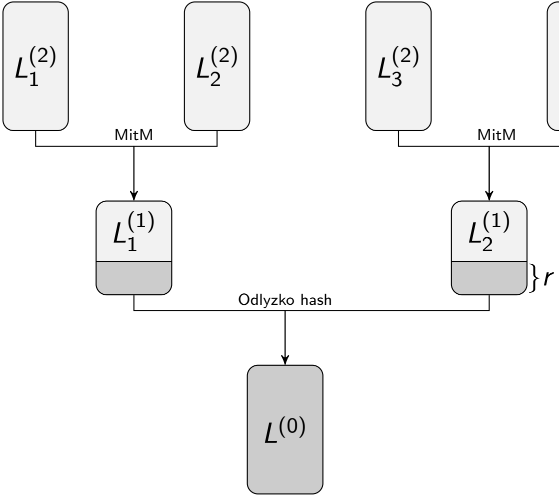
Big picture idea

- Split $s = s_1 + s_2$ with $s_1, s_2 \in \mathbb{Z}_q^n$, weight $\frac{w}{2}$.
- Guess r entries of e.
- Example: guess 23/509.
- Set $t \in \mathbb{Z}_q^r$.
- Try to find s_1, s_2 s.t.

$$\pi_r\left(As_1^{(1)} + e_1\right) \mod q = t = \pi_r\left(b - As_2^{(1)} + e_2\right) \mod q.$$

- Do this recursively.
- At highest level do MitM.
- At lowest level check solution using LSH.

Figure



$s_i^{(2)} \in \mathbb{Z}_q^{n/2}$, weight $\frac{w}{4}$

$s_1^{(1)}, s_2^{(1)} \in \mathbb{Z}_q^n$, weight $\frac{w}{2}$

Meet-LWE

Runtime

- Time complexity $T = T_g \times T_\ell$.

Meet-LWE

Runtime

- Time complexity $T = T_g \times T_\ell$.
- $T_g = 3^r$.
- Example: $3^{23} \approx 2^{36}$.

Meet-LWE

Runtime

- Time complexity $T = T_g \times T_\ell$.
- $T_g = 3^r$.
- Example: $3^{23} \approx 2^{36}$.
- T_ℓ is the size of the largest list.
- Example: 2^{282}

Meet-LWE

Runtime

- Time complexity $T = T_g \times T_\ell$.
- $T_g = 3^r$.
- Example: $3^{23} \approx 2^{36}$.
- T_ℓ is the size of the largest list.
- Example: 2^{282}
- Final runtime: $2^{282+36} = 2^{318} < 2^{377}$.

QMeet-LWE

- Apply Grover & quantum walk.

QMeet-LWE

- Apply Grover & quantum walk.
- $T_{qg} = \sqrt{T_g}$ using Grover.
- Example: $2^{36 \cdot \frac{1}{2}} = 2^{18}$.

QMeet-LWE

- Apply Grover & quantum walk.
- $T_{qg} = \sqrt{T_g}$ using Grover.
- Example: $2^{36 \cdot \frac{1}{2}} = 2^{18}$.
- Inner loop: subsets of highest level lists.

QMeet-LWE

- Apply Grover & quantum walk.
- $T_{qg} = \sqrt{T_g}$ using Grover.
- Example: $2^{36 \cdot \frac{1}{2}} = 2^{18}$.
- Inner loop: subsets of highest level lists.
- Number of levels $d + 1$.
- $\gamma = \frac{2^d}{2^d + 1}$.

QMeet-LWE

- Apply Grover & quantum walk.
- $T_{qg} = \sqrt{T_g}$ using Grover.
- Example: $2^{36 \cdot \frac{1}{2}} = 2^{18}$.
- Inner loop: subsets of highest level lists.
- Number of levels $d + 1$.
- $\gamma = \frac{2^d}{2^d+1}$.
- Example: 2 levels optimal, $2^{212+18} = 2^{230} < 2^{318}$.

QMeet-LWE

- Apply Grover & quantum walk.
- $T_{qg} = \sqrt{T_g}$ using Grover.
- Example: $2^{36 \cdot \frac{1}{2}} = 2^{18}$.
- Inner loop: subsets of highest level lists.
- Number of levels $d + 1$.
- $\gamma = \frac{2^d}{2^d+1}$.
- Example: 2 levels optimal, $2^{212+18} = 2^{230} < 2^{318}$.
- Further improvement: $1 - 1 = 0$.

QMeet-LWE

- Apply Grover & quantum walk.
- $T_{qg} = \sqrt{T_g}$ using Grover.
- Example: $2^{36 \cdot \frac{1}{2}} = 2^{18}$.
- Inner loop: subsets of highest level lists.
- Number of levels $d + 1$.
- $\gamma = \frac{2^d}{2^d+1}$.
- Example: 2 levels optimal, $2^{212+18} = 2^{230} < 2^{318}$.
- Further improvement: $1 - 1 = 0$.
- Classically now 2^{267}.

QMeet-LWE

- Apply Grover & quantum walk.
- $T_{qg} = \sqrt{T_g}$ using Grover.
- Example: $2^{36 \cdot \frac{1}{2}} = 2^{18}$.
- Inner loop: subsets of highest level lists.
- Number of levels $d + 1$.
- $\gamma = \frac{2^d}{2^d+1}$.
- Example: 2 levels optimal, $2^{212+18} = 2^{230} < 2^{318}$.
- Further improvement: $1 - 1 = 0$.
- Classically now 2^{267}.
- Example: 4 levels optimal, $2^{155+33} = 2^{188}$.

Results

Cryptosystem		Meet-LWE	QMeet-LWE	cSVP		
name	(n, q, w)	bit complexity	qbit complexity	β	bit	qbit
NTRU-Enc	$(509, 2048, 254)$	$267 = 193 + 74$	$188 = 155 + 33$	369	108	98
	$(677, 2048, 254)$	$313 = 235 + 78$	$223 = 191 + 32$	517	151	137
	$(821, 4096, 510)$	$449 = 336 + 113$	$320 = 268 + 52$	619	181	164
	$(701, 8192, 468)$	$387 = 295 + 92$	$278 = 235 + 43$	474	139	126
NTRU-Prime	$(653, 4621, 288)$	$309 = 236 + 73$	$225 = 190 + 35$	449	131	119
	$(761, 4591, 286)$	$344 = 265 + 79$	$245 = 206 + 39$	539	157	143
	$(857, 5167, 322)$	$383 = 294 + 89$	$274 = 236 + 38$	615	180	163
BLISS I+II	$(512, 12289, 154)$	$206 = 168 + 38$	$149 = 133 + 16$	292	85	77

Table: cSVP numbers from ia.cr/2020/292

Conclusions

- Significant quantum speedup.

Conclusions

- Significant quantum speedup.
- Results are worse than lattice results.
- Core SVP classic: 2^{108} quantum: 2^{98}.
- Different heuristic.

Conclusions

- Significant quantum speedup.
- Results are worse than lattice results.
- Core SVP classic: 2^{108} quantum: 2^{98}.
- Different heuristic.
- γ for time-memory trade-off.