Provable Dual Attacks on Learning with Errors

Amaury Pouly and Yixin Shen

Centre National de la Recherche Scientifique (CNRS), Paris, France
King's College London, London, UK

30 May 2024

Learning with Error (LWE)

Fundamental problem for lattice-based cryptography

- n: dimension of secret
- m: number of samples
- χ_e: error distribution over $\mathbb{Z}_q$
- q: prime number
- $\mathbf{s} \in \mathbb{Z}_q^n$: secret

$\mathrm{LWE}(m, \mathbf{s}, \chi_e)$ distribution

Sample $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ *uniformly at random* and $\mathbf{e} \in \mathbb{Z}_q^m$ *according to* χ_e^m.
Output $(\mathbf{A}, \mathbf{b})$ where $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$.

Search LWE problem

Given $(\mathbf{A}, \mathbf{b})$ sampled from $\mathrm{LWE}(m, \mathbf{s}, \chi_e)$, recover (part of) $\mathbf{s}$.

In this paper:

- no assumption on $\mathbf{s}$ and χ_e
- $m \approx 2n$ (more on that at the end)

Dual attacks: brief history and controversy

Two main types of attacks: primal and dual.

[GJ21] dual attack with sieving, DFT, suggested modulus switching

[MAT22] formal analysis of dual attack with sieving + modulus switching

- $\rightsquigarrow$ claims comparable with best primal attacks (in some regime)
- $\rightsquigarrow$ correctness relies on statistical assumptions: do these really hold?

Dual attacks: brief history and controversy

Two main types of attacks: primal and dual.

[GJ21] dual attack with sieving, DFT, suggested modulus switching

[MAT22] formal analysis of dual attack with sieving + modulus switching

- $\rightsquigarrow$ claims comparable with best primal attacks (in some regime)
- $\rightsquigarrow$ correctness relies on statistical assumptions: do these really hold?

[DP23a]:

- Formalizes a simplified version of [MAT22]'s key assumption
- Shows that it does not hold for [MAT22]'s parameters
- Concludes that [MAT22]'s result is unsubstantiated

Dual attacks: brief history and controversy

Two main types of attacks: primal and dual.

[GJ21] dual attack with sieving, DFT, suggested modulus switching
[MAT22] formal analysis of dual attack with sieving + modulus switching

$\rightsquigarrow$ claims comparable with best primal attacks (in some regime)

$\rightsquigarrow$ correctness relies on statistical assumptions: do these really hold?

[DP23a]:

- Formalizes a simplified version of [MAT22]'s key assumption
- Shows that it does not hold for [MAT22]'s parameters
- Concludes that [MAT22]'s result is unsubstantiated

Open question: is [DP23a]'s simplified assumption really equivalent to [MAT22]'s key assumption? $\rightsquigarrow$ more on this later

Contributions

Main result

Completely formal, non-asymptotic analysis of a simplified dual attack.

- no assumptions $\rightsquigarrow$ no controversy
- makes it clear in which parameter regime the attack works
  $\rightsquigarrow$ almost complementary with [DP23a]'s contradictory regime in our simplified setting
- uses discrete Gaussian sampling (DGS) instead of sieving

Contributions

Main result

Completely formal, non-asymptotic analysis of a simplified dual attack.

- no assumptions $\rightsquigarrow$ no controversy
- makes it clear in which parameter regime the attack works
  $\rightsquigarrow$ almost complementary with [DP23a]'s contradictory regime in our simplified setting
- uses discrete Gaussian sampling (DGS) instead of sieving

Other contributions:

- Quantum version of the algorithm with non-trivial speed up based on ideas from [AS22]
- Improved analysis of DGS with BKZ reduced basis based on the Monte Carlo Markov Chain sampler [WL19]
- Complexity estimates for concrete parameters (Kyber)

Our dual attack on LWE: high-level

Given $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, split secret into two parts ($n = n_{\text{guess}} + n_{\text{dual}}$):

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{\text{guess}} & \mathbf{A}_{\text{dual}} \end{pmatrix}, \qquad \mathbf{s} = \begin{pmatrix} \mathbf{s}_{\text{guess}} \\ \mathbf{s}_{\text{dual}} \end{pmatrix}$$

Consider the lattice

$$L = \mathbf{A}_{\text{dual}} \mathbb{Z}_q^{n_{\text{dual}}} + q\mathbb{Z}^m$$

Our dual attack on LWE: high-level

Given $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, split secret into two parts ($n = n_{\text{guess}} + n_{\text{dual}}$):

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{\text{guess}} & \mathbf{A}_{\text{dual}} \end{pmatrix}, \qquad \mathbf{s} = \begin{pmatrix} \mathbf{s}_{\text{guess}} \\ \mathbf{s}_{\text{dual}} \end{pmatrix}$$

Consider the lattice

$$L = \mathbf{A}_{\text{dual}} \mathbb{Z}_q^{n_{\text{dual}}} + q\mathbb{Z}^m$$

Assume we have a function

$$f(\mathbf{t}) \approx g(\text{dist}(\mathbf{t}, L)), \qquad \mathbf{t} \in \mathbb{R}^m$$

for some decreasing function g.

Our dual attack on LWE: high-level

Given $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, split secret into two parts ($n = n_{\text{guess}} + n_{\text{dual}}$):

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{\text{guess}} & \mathbf{A}_{\text{dual}} \end{pmatrix}, \qquad \mathbf{s} = \begin{pmatrix} \mathbf{s}_{\text{guess}} \\ \mathbf{s}_{\text{dual}} \end{pmatrix}$$

Consider the lattice

$$L = \mathbf{A}_{\text{dual}} \mathbb{Z}_q^{n_{\text{dual}}} + q\mathbb{Z}^m$$

Assume we have a function

$$f(\mathbf{t}) \approx g(\text{dist}(\mathbf{t}, L)), \qquad \mathbf{t} \in \mathbb{R}^m$$

for some decreasing function g. Guess $\tilde{\mathbf{s}}_{\text{guess}}$ and compute

$$f(\mathbf{b} - \mathbf{A}_{\text{guess}}\tilde{\mathbf{s}}_{\text{guess}}) \approx g(\text{dist}(\mathbf{A}_{\text{guess}}(\mathbf{s}_{\text{guess}} - \tilde{\mathbf{s}}_{\text{guess}}) + \mathbf{e}, L))$$

Our dual attack on LWE: high-level

Given $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, split secret into two parts ($n = n_{\text{guess}} + n_{\text{dual}}$):

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{\text{guess}} & \mathbf{A}_{\text{dual}} \end{pmatrix}, \qquad \mathbf{s} = \begin{pmatrix} \mathbf{s}_{\text{guess}} \\ \mathbf{s}_{\text{dual}} \end{pmatrix}$$

Consider the lattice

$$L = \mathbf{A}_{\text{dual}} \mathbb{Z}_q^{n_{\text{dual}}} + q\mathbb{Z}^m$$

Assume we have a function

$$f(\mathbf{t}) \approx g(\text{dist}(\mathbf{t}, L)), \qquad \mathbf{t} \in \mathbb{R}^m$$

for some decreasing function g. Guess $\tilde{\mathbf{s}}_{\text{guess}}$ and compute

$$f(\mathbf{b} - \mathbf{A}_{\text{guess}}\tilde{\mathbf{s}}_{\text{guess}}) \approx g(\text{dist}(\mathbf{A}_{\text{guess}}(\mathbf{s}_{\text{guess}} - \tilde{\mathbf{s}}_{\text{guess}}) + \mathbf{e}, L))$$

Good guess: $\tilde{\mathbf{s}}_{\text{guess}} = \mathbf{s}_{\text{guess}}$

$f(\mathbf{b} - \mathbf{A}_{\text{guess}}\tilde{\mathbf{s}}_{\text{guess}}) \approx g(\text{dist}(\mathbf{e}, L)) = g(\|\mathbf{e}\|)$ if $\mathbf{e}$ is sufficiently small.

Our dual attack on LWE: high-level

Given $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, split secret into two parts ($n = n_{\text{guess}} + n_{\text{dual}}$):

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{\text{guess}} & \mathbf{A}_{\text{dual}} \end{pmatrix}, \qquad \mathbf{s} = \begin{pmatrix} \mathbf{s}_{\text{guess}} \\ \mathbf{s}_{\text{dual}} \end{pmatrix}$$

Consider the lattice

$$L = \mathbf{A}_{\text{dual}} \mathbb{Z}_q^{n_{\text{dual}}} + q\mathbb{Z}^m$$

Assume we have a function

$$f(\mathbf{t}) \approx g(\operatorname{dist}(\mathbf{t}, L)), \qquad \mathbf{t} \in \mathbb{R}^m$$

for some decreasing function g. Guess $\tilde{\mathbf{s}}_{\text{guess}}$ and compute

$$f(\mathbf{b} - \mathbf{A}_{\text{guess}}\tilde{\mathbf{s}}_{\text{guess}}) \approx g(\operatorname{dist}(\mathbf{A}_{\text{guess}}(\mathbf{s}_{\text{guess}} - \tilde{\mathbf{s}}_{\text{guess}}) + \mathbf{e}, L))$$

Bad guess: $\tilde{\mathbf{s}}_{\text{guess}} \neq \mathbf{s}_{\text{guess}}$

For most $\mathbf{A}$, $\operatorname{dist}(\mathbf{A}_{\text{guess}}(\mathbf{s}_{\text{guess}} - \tilde{\mathbf{s}}_{\text{guess}}) + \mathbf{e}, L) > \|\mathbf{e}\|$ if $\mathbf{e}$ is sufficiently small. So $f(\mathbf{b} - \mathbf{A}_{\text{guess}}\tilde{\mathbf{s}}_{\text{guess}}) \lessapprox g(\|\mathbf{e}\|)$.

Our dual attack on LWE: high-level

Given $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, split secret into two parts ($n = n_{\text{guess}} + n_{\text{dual}}$):

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{\text{guess}} & \mathbf{A}_{\text{dual}} \end{pmatrix}, \qquad \mathbf{s} = \begin{pmatrix} \mathbf{s}_{\text{guess}} \\ \mathbf{s}_{\text{dual}} \end{pmatrix}$$

Consider the lattice

$$L = \mathbf{A}_{\text{dual}} \mathbb{Z}_q^{n_{\text{dual}}} + q\mathbb{Z}^m$$

Assume we have a function

$$f(\mathbf{t}) \approx g(\operatorname{dist}(\mathbf{t}, L)), \qquad \mathbf{t} \in \mathbb{R}^m$$

for some decreasing function g. Guess $\tilde{\mathbf{s}}_{\text{guess}}$ and compute

$$f(\mathbf{b} - \mathbf{A}_{\text{guess}} \tilde{\mathbf{s}}_{\text{guess}}) \approx g(\operatorname{dist}(\mathbf{A}_{\text{guess}}(\mathbf{s}_{\text{guess}} - \tilde{\mathbf{s}}_{\text{guess}}) + \mathbf{e}, L))$$

Summary: If $\mathbf{e}$ is sufficiently small and for most $\mathbf{A}$,

$$\mathbf{s}_{\text{guess}} = \operatorname*{arg\,max}_{\tilde{\mathbf{s}}_{\text{guess}} \in \mathbb{Z}_q^{n_{\text{guess}}}} f(\mathbf{b} - \mathbf{A}_{\text{guess}} \tilde{\mathbf{s}}_{\text{guess}})$$

The score function f

Goal: given a lattice L, construct $f(\mathbf{t}) \approx g(\mathrm{dist}(\mathbf{t}, L))$ for all $\mathbf{t} \in \mathbb{R}^m$.

The score function f

Goal: given a lattice L, construct $f(\mathbf{t}) \approx g(\mathrm{dist}(\mathbf{t}, L))$ for all $\mathbf{t} \in \mathbb{R}^m$.

Find (exponentially) many short vectors $\mathbf{x}_1, \ldots, \mathbf{x}_N \in \widehat{L}$, define

$$f(\mathbf{t}) = \sum_{i=1}^{N} \cos(2\pi \langle \mathbf{x}_i, \mathbf{t} \rangle)$$

The score function f

Goal: given a lattice L, construct $f(\mathbf{t}) \approx g(\mathrm{dist}(\mathbf{t}, L))$ for all $\mathbf{t} \in \mathbb{R}^m$.

Find (exponentially) many short vectors $\mathbf{x}_1, \ldots, \mathbf{x}_N \in \widehat{L}$, define

$$f(\mathbf{t}) = \sum_{i=1}^{N} \cos(2\pi \langle \mathbf{x}_i, \mathbf{t} \rangle)$$

How to generate short vectors?

- BKZ + sieving in sublattice: used by all best attacks
  $\rightsquigarrow$ complicated to analyze, major source of problems in [MAT22] and leads to statistical assumptions

The score function f

Goal: given a lattice L, construct $f(\mathbf{t}) \approx g(\operatorname{dist}(\mathbf{t}, L))$ for all $\mathbf{t} \in \mathbb{R}^m$.

Find (exponentially) many short vectors $\mathbf{x}_1, \ldots, \mathbf{x}_N \in \widehat{L}$, define

$$f(\mathbf{t}) = \sum_{i=1}^{N} \cos(2\pi \langle \mathbf{x}_i, \mathbf{t} \rangle)$$

How to generate short vectors?

- BKZ + sieving in sublattice: used by all best attacks
  $\rightsquigarrow$ complicated to analyze, major source of problems in [MAT22] and leads to statistical assumptions

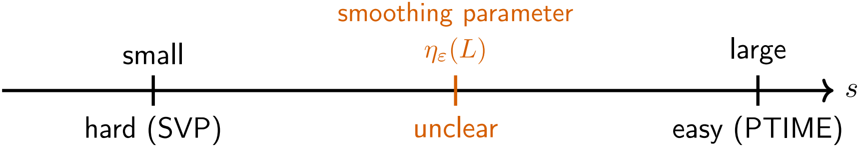
- BKZ + Gaussian sampler:
  $\rightsquigarrow$ well understood, $f(\mathbf{t}) \approx \rho_s(\operatorname{dist}(\mathbf{t}, L))$ [AR05]
  $\rightsquigarrow$ considered inefficient for dual attacks, maybe wrongly so!

Complexity of Discrete Gaussian Sampling

Sampling from the discrete Gaussian over L with parameter s:

Complexity of Discrete Gaussian Sampling

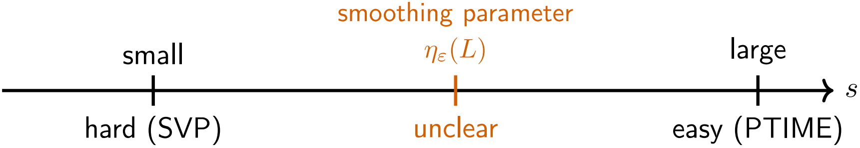
Sampling from the discrete Gaussian over L with parameter s:



For dual attack: smaller s is better, want $s < \eta_\varepsilon(L)$ if possible.

Complexity of Discrete Gaussian Sampling

Sampling from the discrete Gaussian over L with parameter s:



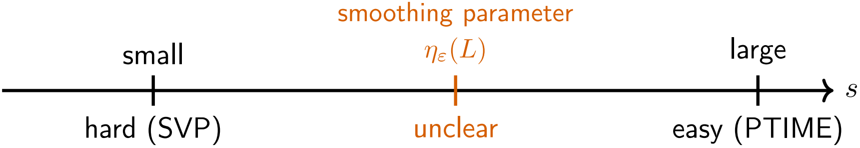
For dual attack: smaller s is better, want $s < \eta_\varepsilon(L)$ if possible.

Run BKZ to reduce the basis, then

1. Klein sampler: PTIME, s depends on basis but $s \geqslant \eta_\varepsilon(L)$ by construction $\rightsquigarrow$ not good enough

Complexity of Discrete Gaussian Sampling

Sampling from the discrete Gaussian over L with parameter s:



For dual attack: smaller s is better, want $s < \eta_\varepsilon(L)$ if possible.

Run BKZ to reduce the basis, then

1. Klein sampler: PTIME, s depends on basis but $s \geqslant \eta_\varepsilon(L)$ by construction $\rightsquigarrow$ not good enough
2. Monte Carlo Markov Chain (MCMC) sampler [WL19]: complexity and s depend on basis, no constraint on s
   - regime where $s < \eta_\varepsilon(L)$ and the sampler runs in exponential time
   - the generic complexity bound in [WL19] is not good enough
   - we improved it specifically for BKZ-reduced basis under GSA

Main result and working/contradictory regime

Main result (very informal)

Our dual attack works for most $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$ as long as $\|\mathbf{e}\| \leqslant \frac{1}{2}\lambda_1(L_q(\mathbf{A}))$.

Main result and working/contradictory regime

Main result (very informal)

Our dual attack works for most $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$ as long as $\|\mathbf{e}\| \leqslant \frac{1}{2}\lambda_1(L_q(\mathbf{A}))$.

In [DP23a], the authors introduced a "contradictory regime" where dual attacks provably do not work. In our setting (simplified attack), this regime is roughly

$$\|\mathbf{e}\| > \lambda_1(L_q(\mathbf{A})).$$

Main result and working/contradictory regime

Main result (very informal)

Our dual attack works for most $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$ as long as $\|\mathbf{e}\| \leqslant \frac{1}{2}\lambda_1(L_q(\mathbf{A}))$.

In [DP23a], the authors introduced a "contradictory regime" where dual attacks provably do not work. In our setting (simplified attack), this regime is roughly

$$\|\mathbf{e}\| > \lambda_1(L_q(\mathbf{A})).$$

Take away (for simplified attack):

- [DP23a] + our work covers most of the parameter range
- Open question: what happens for $\frac{1}{2} \leqslant \frac{\|\mathbf{e}\|}{\lambda_1(L_q(\mathbf{A}))} \leqslant 1$?

Complexity estimates

Our attack does not have modulus switching $\rightsquigarrow$ not competitive

Scheme	attack	m	n_{guess}	n_{dual}	β
Kyber512	185	1013	15	497	550
Kyber768	273	1469	23	745	870
Kyber1024	376	2025	31	993	1230

Complexity estimates

Our attack does not have modulus switching $\rightsquigarrow$ not competitive

Scheme	attack	m	n_{guess}	n_{dual}	β
Kyber512	185	1013	15	497	550
Kyber768	273	1469	23	745	870
Kyber1024	376	2025	31	993	1230

We estimated the complexity of a hypothetical extension of our attack with modulus switching (MS):

Scheme	Our attack	MS	MATZOV
Kyber512	185	141	143
Kyber768	273	202	200
Kyber1024	376	279	264

- promising but unproven, most likely too optimistic
- validates the approach of BKZ + MCMC DGS sampling

Targets and related works

Given $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$,

$$\mathbf{s}_{\text{guess}} = \mathop{\arg\max}_{\tilde{\mathbf{s}}_{\text{guess}} \in \mathbb{Z}_q^{n_{\text{guess}}}} f(\underbrace{\mathbf{b} - \mathbf{A}_{\text{guess}}\tilde{\mathbf{s}}_{\text{guess}}}_{\text{target}})$$

where $f = f_{\mathcal{X}}$ for some (sampled) dual vectors $\mathcal{X} \subseteq \widehat{L}$.

Targets and related works

Given $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$,

$$\mathbf{s}_{\text{guess}} = \underset{\tilde{\mathbf{s}}_{\text{guess}} \in \mathbb{Z}_q^{n_{\text{guess}}}}{\arg\max}\; f(\underbrace{\mathbf{b} - \mathbf{A}_{\text{guess}}\tilde{\mathbf{s}}_{\text{guess}}}_{\text{target}})$$

where $f = f_{\mathcal{X}}$ for some (sampled) dual vectors $\mathcal{X} \subseteq \widehat{L}$. Study

$$\Pr_{\mathcal{X}}\left[\underbrace{f(\mathbf{e})}_{\text{good guess}} > \underbrace{f(\mathbf{e} + \mathbf{A}_{\text{guess}}\mathbf{u})}_{\text{bad guess}}, \forall \mathbf{u} \in \mathbb{Z}_q^{n_{\text{guess}}} \setminus \{0\}\right]. \tag{1}$$

Difficult because it depends on $\mathbf{A}_{\text{guess}}$ and $\mathbf{e}$.

Targets and related works

Given $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$,

$$\mathbf{s}_{\text{guess}} = \underset{\tilde{\mathbf{s}}_{\text{guess}} \in \mathbb{Z}_q^{n_{\text{guess}}}}{\arg\max} f(\underbrace{\mathbf{b} - \mathbf{A}_{\text{guess}}\tilde{\mathbf{s}}_{\text{guess}}}_{\text{target}})$$

where $f = f_{\mathcal{X}}$ for some (sampled) dual vectors $\mathcal{X} \subseteq \widehat{L}$. Study

$$\Pr_{\mathcal{X}}\left[\underbrace{f(\mathbf{e})}_{\text{good guess}} > \underbrace{f(\mathbf{e} + \mathbf{A}_{\text{guess}}\mathbf{u})}_{\text{bad guess}}, \forall \mathbf{u} \in \mathbb{Z}_q^{n_{\text{guess}}} \setminus \{0\}\right]. \quad (1)$$

Difficult because it depends on $\mathbf{A}_{\text{guess}}$ and $\mathbf{e}$. [DP23a] "simplifies" this to

$$\Pr_{\mathcal{X}, \mathbf{t}^{(i)} \sim \mathcal{U}(\mathbb{Z}^m/L)}\left[f(\mathbf{e}) > f(\mathbf{t}^{(i)}), i = 1, \ldots, q^{n_{\text{guess}}}\right]. \quad (2)$$

Targets and related works

Given $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$,

$$\mathbf{s}_{\text{guess}} = \underset{\tilde{\mathbf{s}}_{\text{guess}} \in \mathbb{Z}_q^{n_{\text{guess}}}}{\arg\max} f(\underbrace{\mathbf{b} - \mathbf{A}_{\text{guess}}\tilde{\mathbf{s}}_{\text{guess}}}_{\text{target}})$$

where $f = f_{\mathcal{X}}$ for some (sampled) dual vectors $\mathcal{X} \subseteq \widehat{L}$. Study

$$\Pr_{\mathcal{X}}\left[\underbrace{f(\mathbf{e})}_{\text{good guess}} > \underbrace{f(\mathbf{e} + \mathbf{A}_{\text{guess}}\mathbf{u})}_{\text{bad guess}}, \forall \mathbf{u} \in \mathbb{Z}_q^{n_{\text{guess}}} \setminus \{0\}\right]. \qquad (1)$$

Difficult because it depends on $\mathbf{A}_{\text{guess}}$ and $\mathbf{e}$. [DP23a] "simplifies" this to

$$\Pr_{\mathcal{X}, \mathbf{t}^{(i)} \sim \mathcal{U}(\mathbb{Z}^m/L)}\left[f(\mathbf{e}) > f(\mathbf{t}^{(i)}), i = 1, \ldots, q^{n_{\text{guess}}}\right]. \qquad (2)$$

Later [CDMT24] and [DP23b] analyzed the distribution of $f(\mathbf{t})$ when $\mathbf{t} \sim \mathcal{U}(\mathbb{Z}^m/L)$ and $\mathcal{X}$ comes from sieving in $\widehat{L}$.

Open question: (1) is NOT equivalent to (2), how do they compare?

Conclusion and future work

- strong foundation for provable dual attacks with no assumptions
- BKZ + MCMC DGS sampling seems competitive with BKZ + sieving but simpler to analyze
- promising complexity estimates
- quantum algorithm with non-trivial speed up

Open questions:

- analyze modulus switching or coding theory-based dimension reduction from [CST22]
- close the gap between working and contradictory regime
- make the attack work with $m = n$ samples by using

$$\{(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}^m \times \mathbb{Z}^{n_{\text{dual}}} : \mathbf{x}^T \mathbf{A}_{\text{dual}} = \mathbf{y} \bmod q\}$$

instead of dual lattice

Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe.
Post-quantum key exchange: A new hope.
USENIX Association, 2016.

Martin R. Albrecht.
On dual lattice attacks against small-secret lwe and parameter choices in HElib and SEAL.
In *EUROCRYPT*, 2017.

Dorit Aharonov and Oded Regev.
Lattice problems in NP $\cap$ CoNP.
J. ACM, 2005.

Martin R. Albrecht and Yixin Shen.
Quantum augmented dual attack.
Cryptology ePrint Archive, Paper 2022/656, 2022.

Kévin Carrier, Thomas Debris-Alazard, Charles Meyer-Hilfiger, and Jean-Pierre Tillich.
Reduction from sparse LPN to LPN, dual attack 3.0.
In *EUROCRYPT*, 2024.

Kevin Carrier, Yixin Shen, and Jean-Pierre Tillich.
Faster dual lattice attacks by using coding theory.
2022.

Léo Ducas and Ludo N. Pulles.
Does the dual-sieve attack on learning with errors even work?
In *CRYPTO*, 2023.

Léo Ducas and Ludo N. Pulles.
Accurate score prediction for dual-sieve attacks.
Cryptology ePrint Archive, Paper 2023/1850, 2023.
https://eprint.iacr.org/2023/1850.

Thomas Espitau, Antoine Joux, and Natalia Kharchenko.
On a Dual/Hybrid Approach to Small Secret LWE.
In *INDOCRYPT*. 2020.

Qian Guo and Thomas Johansson.
Faster dual lattice attacks for solving LWE – with applications to crystals.
Springer-Verlag, 2021.

MATZOV.
Report on the Security of LWE: Improved Dual Lattice Attack, 2022.

Zheng Wang and Cong Ling.
Lattice gaussian sampling by markov chain monte carlo: Bounded distance decoding and trapdoor sampling.
IEEE Transactions on Information Theory, 2019.