A Refined Hardness Estimation of LWE in Two-step Mode

eprint: 2024/067

PKC2024

Wenwen Xia[1,2,5], Leizhang Wang[3], Geng Wang[4,5], Dawu Gu[4,1,*], Baocang Wang[3]

1 School of Cyber Engineering, Xidian University, Xi'an, 710071, China xiawenwen@stu.xidian.edu.cn

2 Lab of Cryptology and Computer Security, Shanghai Jiao Tong University, Shanghai, 200240, China

3 State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, China {lzwang_2, bcwang}@stu.xidian.edu.cn

4 School of Electronic, Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, 200240, China {wanggxx, dwgu}@sjtu.edu.cn

5 State Key Laboratory of Cryptology, P.O.Box 5159, Beijing, 100878, China

* Corresponding author

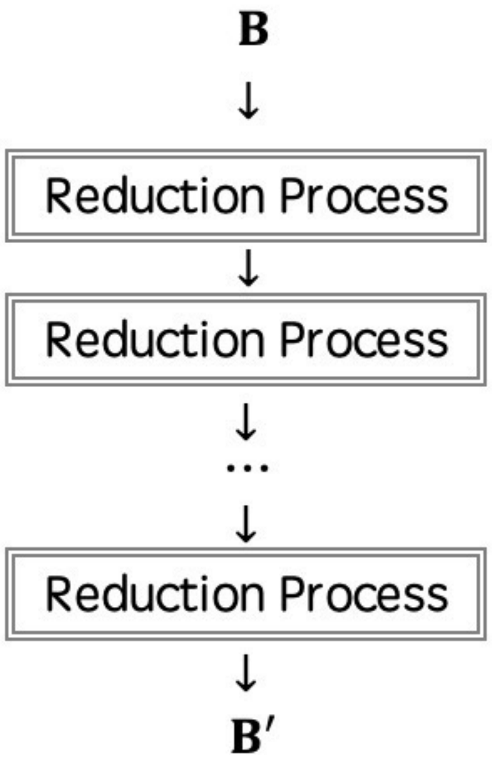
2024.4.16

CONTENTS

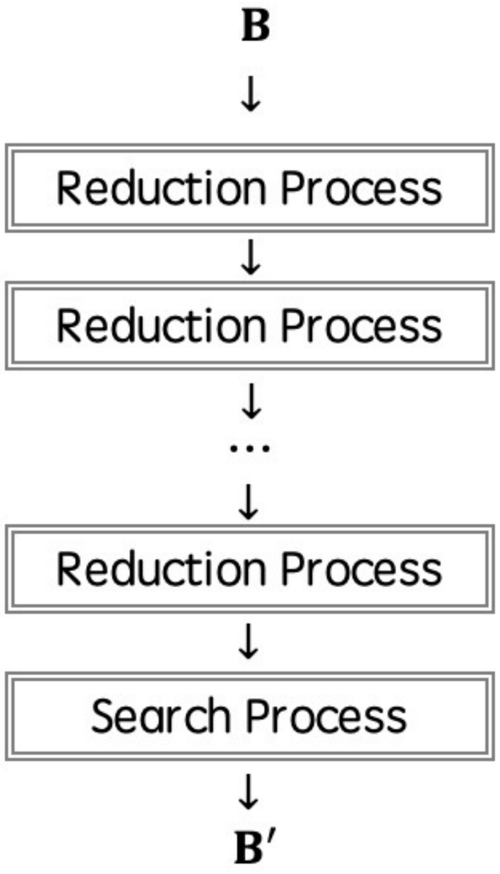
01

Introduction of LWE Estimator

Introduction of LWE Estimator



BKZ-only Mode



Two-step Mode

Introduction of LWE Estimators

Two-step mode

2013
BDD Estimator[1]
BKZ+Enum+Suc Prob of Enum

2016
core-SVP[2]
BKZ+GSA+expected norm

2017
lattice-estimator[3]
BKZ+Sieve+GSA+expected norm

2020
leaky-LWE-Estimator[4]
BKZ+distribution of target norm

2021
Improved leaky-LWE-Estimator[5]
Delete p_{lift}

2024
Our Work
(Refined) PnjBKZ+Sieve+distribution of target norm
(Lower bound) BKZ+Sieve+GSA+expected norm

BKZ-only mode

Introduction of LWE Estimators

Comparison among different LWE Estimators

Estimator	Mode	Reduction Process	Search Process	Terminal Condition	Cost
BDD Estimator	Two-step	BKZ	Enumeration	**Success Probability** of last **Enumeration**	$\frac{T_{redu} + T_{Enum}}{p_{succ}}$
core-SVP	BKZ-only	BKZ	/	Minimize β by **GSA** and **expected target norm**	$T_{sieve}(\beta)$
lattice-estimator	Two-step	BKZ	Sieve	Minimize β and d_{svp} by **GSA** and **expected target norm**	$T_{BKZ}(\beta) + T_{sieve}(d_{svp})$
(Improved) leaky-LWE-Estimator	BKZ-only	BKZ	/	Estimate $\bar{\beta}$ by **distribution of target norm**	$T_{BKZ}(\bar{\beta})$
Our work(Refined)	Two-step	PnjBKZ with jump>1	Sieve	Minimize d_{svp} by **distribution of target norm**	$\overline{T_{PnjBKZ}(\beta, J) + T_{sieve}(d_{svp})}$
Our work(Lower Bound)	Two-step	BKZ	Sieve	Estimate d_{svp} by **GSA** and **expected target norm**	$T_{sieve}(d_{svp})$

02

Our Contribution

Our Contribution

1. Prove in theory that the Two-step mode is faster in solving uSVP than the BKZ-only mode under Geometric Series Assumption.
2. Construct a Refined LWE Hardness Estimator in Two-step mode. Give Experiments:
   (1) Accuracy verification of Success Probability used in Refined LWE Hardness Estimator;
   (2) Verification Experiments for Efficiency of Two-step Mode by Refined LWE Hardness Estimator.
3. Give a Lower Bound Estimation for LWE in Two-step mode.
4. Re-evaluate the security bit of NIST PQC schemes both by the Refined LWE Hardness Estimator and Lower Bound Estimation .

03

Efficiency of Two-step Mode

Efficiency of Two-step Mode

Heuristic 1 (Gaussian Heuristic) *The expected first minimum of a lattice* $\mathcal{L}$ *(denoted as* $\lambda_1(\mathcal{L}(\boldsymbol{B}))$*) according to the Gaussian Heuristic denoted by* $GH(\mathcal{L})$ *is given by* $\lambda_1\left(\mathcal{L}(\boldsymbol{B})\right) \approx GH(\mathcal{L}) = \frac{\left(\Gamma\left(\frac{d}{2}+1\right)\cdot \mathrm{Vol}(\mathcal{L})\right)^{\frac{1}{d}}}{\sqrt{\pi}} \approx \sqrt{\frac{d}{2\pi e}} \cdot \mathrm{Vol}(\mathcal{L})^{\frac{1}{d}}$.

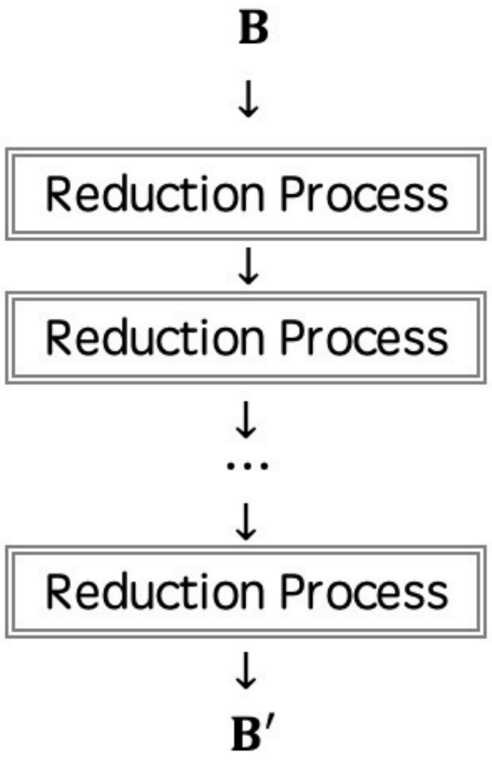
We also write $GH(\boldsymbol{B}) = GH(\mathcal{L}(\boldsymbol{B}))$ *and* $GH(\mathrm{rr}_{[i:j]}) = GH(\boldsymbol{B}_{\pi[i:j]})$.

Heuristic 2 (Geometric Series Assumption (GSA)) *Let* $\boldsymbol{B}$ *be a lattice basis after lattice reduction, then Geometric Series Assumption states that* $\|\boldsymbol{b}_i^*\| \approx \alpha \cdot \|\boldsymbol{b}_{i-1}^*\|$, $0 < \alpha < 1$. *Combine the GSA with root-Hermite factor and* $Vol\left(L(B)\right) = \prod_{i=0}^{d-1}\|\boldsymbol{b}_i^*\|$, *it infers that* $\alpha = \delta^{-\frac{2d}{d-1}} \approx \delta^{-2}$.

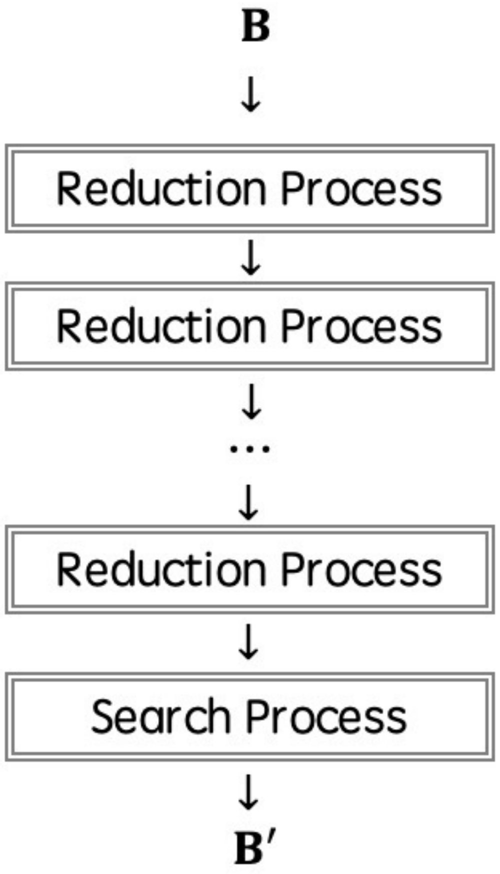
Heuristic 4 in [7]

Let $\boldsymbol{B}$ *be a lattice basis after reduction of several PnjBKZ-*(β_i, J_i) *tours,* $J_i \leq \frac{\mathrm{d4f}(\beta_i)}{2}$. *If* $\boldsymbol{B}$ *has same quality with a BKZ-*β *reduced basis, then the basis cannot be further improved by a PnjBKZ-*(β, J) *tour for any* $J \geq 1$.

Efficiency of Two-step Mode

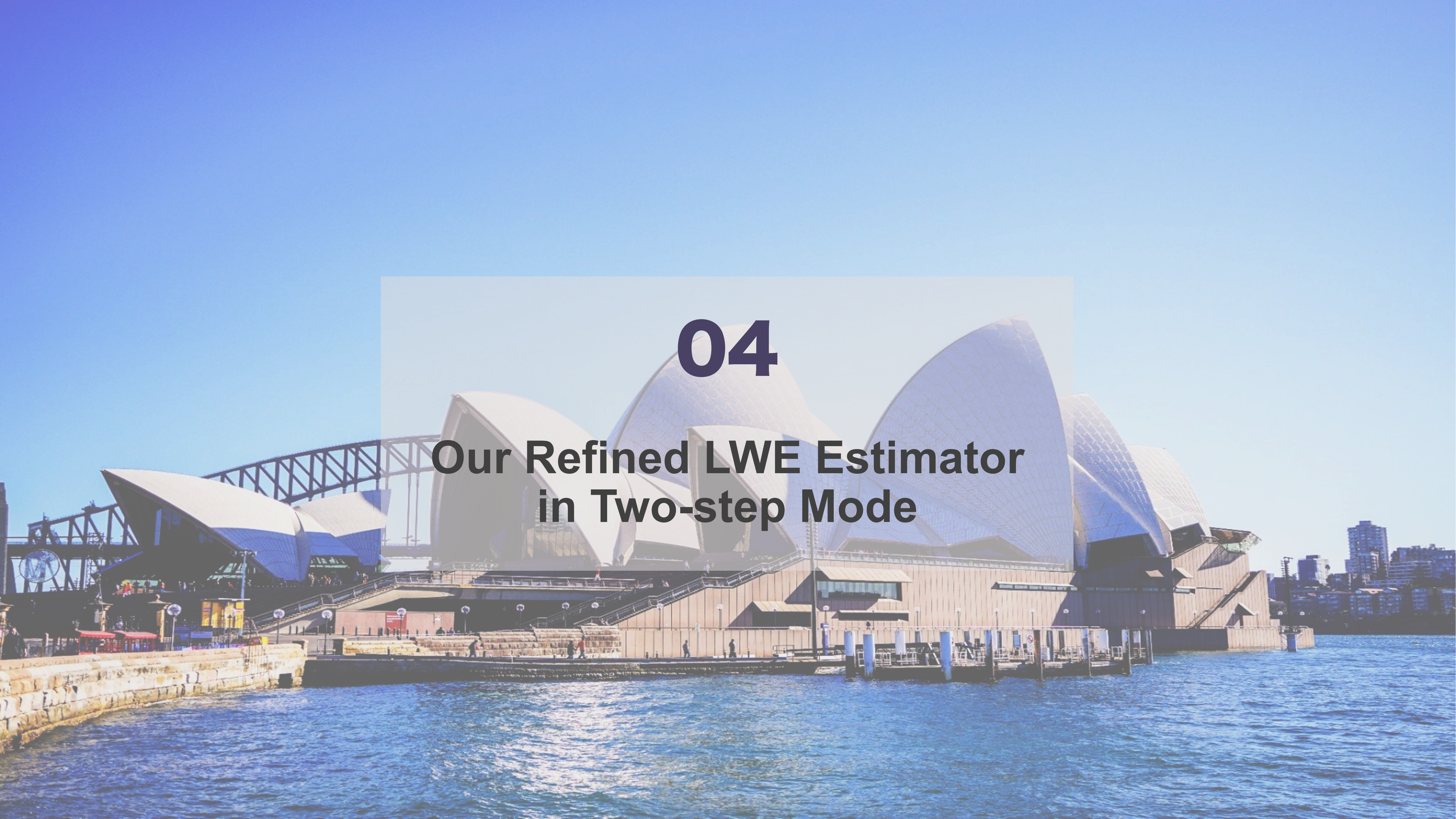


BKZ-only Mode



Two-step Mode

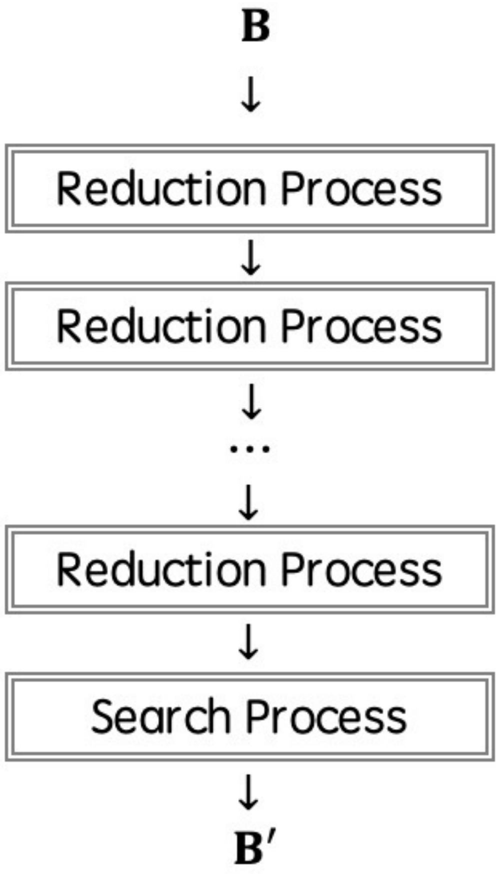
Theorem 1. *Assume Gaussian Heuristic (Heuristic 1), GSA(Heuristic 2) and Heuristic 4 in [7] hold. Let d be the dimension of lattice, $d \geq 100$, we assume that uSVP$_\gamma$ instance can be solved by BKZ-only mode through a BKZ-β reduced basis with $\frac{d+16}{9} \leq \beta \leq \frac{d}{2}$, and let the time cost for sieving on d-dimensional lattice be $2^{c \cdot d + c_0}$ where $c \leq 0.35$. Then, there exists a parameter choice for the two-step mode which solves the uSVP$_\gamma$ instance in less time than BKZ-only mode.*



04

Our Refined LWE Estimator in Two-step Mode

Our Refined LWE Estimator in Two-step Mode



Two-step Mode

1. How to estimate the success probability of finding the target vector ?
2. How to estimate the time cost and memory cost?

1. Propose the success probability computation model combining BKZ and Sieve.
2. Compute the expected time cost and memory cost through success probability.

Our Refined LWE Estimator in Two-step Mode

- W: The event of solving LWE successfully during running Progressive BKZ or the final high-dimension progressive sieve of Two-step mode.
- $\mathrm{W}_{\beta}^{(1)}$: The event of solving LWE by BKZ-β successfully, $\mathrm{F}_{\beta}^{(1)} = \neg \mathrm{W}_{\beta}^{(1)}$.
- $\mathrm{E}_{\beta_i}^{(1)}$: The event of solving LWE successfully during the process of running Progressive BKZ: from BKZ-β_1 to BKZ-β_i .
- $\mathrm{W}_{d_{\mathrm{svp}}}^{(2)}$: The event of solving LWE by d_{svp}-dimensional progressive sieve successfully, $\mathrm{F}_{d_{\mathrm{svp}}}^{(2)} = \neg \mathrm{W}_{d_{\mathrm{svp}}}^{(2)}$.
- $\mathrm{E}_{d_{\mathrm{svp}}}^{(2)}$: The event of finding the projection of the target vector exactly after a d_{svp}-dimensional sieve during progressive sieving .

Our Refined LWE Estimator in Two-step Mode

Heuristic 3. *The lattice basis is randomized each time by a reduction of BKZ-β with larger β. Then, events $W_{\beta_i}^{(1)}$ and $F_{\beta_j}^{(1)}$ are independent for $i \neq j$.*

Success event of each BKZ is independently.

Based on **Heuristic 3**, $\Pr\left[\mathrm{E}_{\beta_k}^{(1)}\right] = \sum_{i=1}^{k} \Pr\left[\mathrm{W}_{\beta_i}^{(1)} \wedge \bigwedge_{i>1,j=1}^{i-1} \mathrm{F}_{\beta_j}^{(1)}\right] = \Pr\left[\mathrm{E}_{\beta_{k-1}}^{(1)}\right] + \Pr\left[\mathrm{W}_{\beta_k}^{(1)}\right] \cdot \left(1 - \Pr\left[\mathrm{E}_{\beta_{k-1}}^{(1)}\right]\right)$. (2)

Heuristic 4. For $i \in \{2, \ldots, d_{\text{svp}}\}$, $\mathrm{W}_i^{(2)} \supseteq \mathrm{W}_{i-1}^{(2)} \supseteq \mathrm{W}_{i-2}^{(2)} \supseteq \cdots \supseteq \mathrm{W}_2^{(2)}$. Then $\mathrm{E}_i^{(2)} = \mathrm{W}_i^{(2)} - \mathrm{W}_{i-1}^{(2)}$.

Success event of each sieve in a Progressive sieve is dependently.

Let $\Pr[\mathrm{W}_{d_{\text{start}}-1}^{(2)}] = 0$. Based on **Heuristic 4**, $\Pr\left[\mathrm{E}_{d_{\text{svp}}}^{(2)}\right] = \Pr\left[W_{d_{\text{svp}}}^{(2)}\right] - \Pr\left[W_{d_{\text{svp}}-1}^{(2)}\right]$. (3)

The cumulative probability of solving LWE in our refined LWE estimator in Two-step mode:

$$\Pr[\mathrm{W}] = \Pr\left[\mathrm{W}_{\beta_1}^{(1)}\right] + \Pr\left[\mathrm{W}_{\beta_2}^{(1)} \wedge \mathrm{F}_{\beta_1}^{(1)}\right] + \Pr\left[\mathrm{W}_{\beta_2}^{(1)} \wedge \mathrm{F}_{\beta_2}^{(1)} \wedge \mathrm{F}_{\beta_1}^{(1)}\right] + \cdots + \Pr\left[\mathrm{W}_{\beta_2}^{(1)} \wedge \bigwedge_{j=1}^{\text{end}-1} \mathrm{F}_{\beta_j}^{(1)}\right] + \Pr\left[\mathrm{W}_{d_{\text{svp}}}^{(2)} \wedge \bigwedge_{j=1}^{\text{end}} \mathrm{F}_{\beta_j}^{(1)}\right]$$

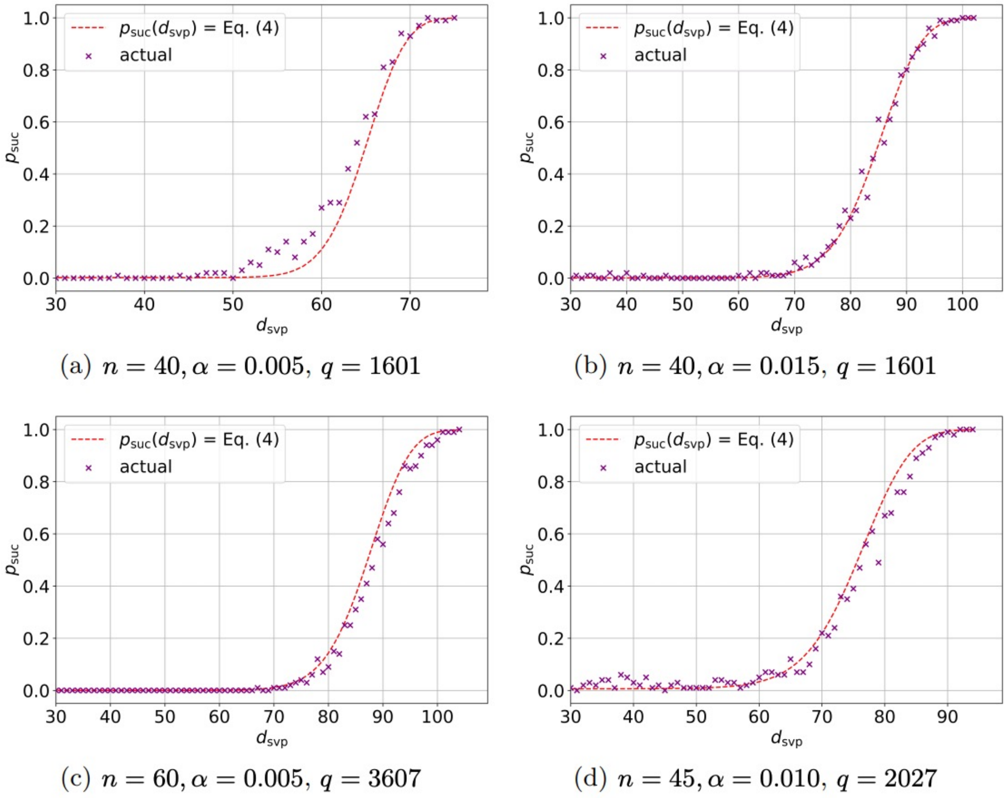
$$= \left(\sum_{i=1}^{\text{end}} \Pr\left[\mathrm{W}_{\beta_i}^{(1)} \wedge \bigwedge_{i>1,j=1}^{i-1} \mathrm{F}_{\beta_j}^{(1)}\right]\right) + \Pr\left[\mathrm{W}_{d_{\text{svp}}}^{(2)} \wedge \bigwedge_{j=1}^{\text{end}} \mathrm{F}_{\beta_j}^{(1)}\right] \quad (1)$$

$$= \Pr\left[\mathrm{E}_{\beta_{\text{end}}}^{(1)}\right] + \left(1 - \Pr\left[E_{\beta_{\text{end}}}^{(1)}\right]\right) \cdot \sum_{i=d_{\text{start}}}^{d_{\text{svp}}} \Pr[\mathrm{E}_i^{(2)}]$$

$$= \Pr\left[\mathrm{E}_{\beta_{\text{end}}}^{(1)}\right] + \left(1 - \Pr\left[E_{\beta_{\text{end}}}^{(1)}\right]\right) \cdot \Pr\left[\mathrm{W}_{d_{\text{svp}}}^{(2)}\right]. \quad (4)$$

If $\Pr[\mathrm{W}] = 1$, then it implies all the LWE instance with specific average value and variance could be solved, time to terminate estimator.

Our Refined LWE Estimator in Two-step Mode



(a) $n = 40, \alpha = 0.005,\ q = 1601$ (b) $n = 40, \alpha = 0.015,\ q = 1601$

(c) $n = 60, \alpha = 0.005,\ q = 3607$ (d) $n = 45, \alpha = 0.010,\ q = 2027$

Success Probability Verification Experiments

The cumulative probability of solving LWE in our refined LWE estimator in Two-step mode:

$$\Pr[\mathrm{W}] = \Pr\left[\mathrm{W}_{\beta_1}^{(1)}\right] + \Pr\left[\mathrm{W}_{\beta_2}^{(1)} \wedge \mathrm{F}_{\beta_1}^{(1)}\right] + \Pr\left[\mathrm{W}_{\beta_2}^{(1)} \wedge \mathrm{F}_{\beta_2}^{(1)} \wedge \mathrm{F}_{\beta_1}^{(1)}\right] + \cdots$$

$$+\Pr\left[\mathrm{W}_{\beta_2}^{(1)} \wedge \bigwedge_{j=1}^{\mathrm{end}-1} \mathrm{F}_{\beta_j}^{(1)}\right] + \Pr\left[\mathrm{W}_{d_{\mathrm{svp}}}^{(2)} \wedge \bigwedge_{j=1}^{\mathrm{end}} \mathrm{F}_{\beta_j}^{(1)}\right]$$

$$= \left(\sum_{i=1}^{\mathrm{end}} \Pr\left[\mathrm{W}_{\beta_i}^{(1)} \wedge \bigwedge_{i>1, j=1}^{i-1} \mathrm{F}_{\beta_j}^{(1)}\right]\right) + \Pr\left[\mathrm{W}_{d_{\mathrm{svp}}}^{(2)} \wedge \bigwedge_{j=1}^{\mathrm{end}} \mathrm{F}_{\beta_j}^{(1)}\right] \quad (1)$$

$$= \Pr\left[\mathrm{E}_{\beta_{\mathrm{end}}}^{(1)}\right] + \left(1 - \Pr\left[E_{\beta_{\mathrm{end}}}^{(1)}\right]\right) \cdot \sum_{i=d_{\mathrm{start}}}^{d_{\mathrm{svp}}} \Pr[\mathrm{E}_i^{(2)}]$$

$$= \Pr\left[\mathrm{E}_{\beta_{\mathrm{end}}}^{(1)}\right] + \left(1 - \Pr\left[E_{\beta_{\mathrm{end}}}^{(1)}\right]\right) \cdot \Pr\left[\mathrm{W}_{d_{\mathrm{svp}}}^{(2)}\right]. \quad (4)$$

$\Pr\left[\mathrm{E}_{\beta_{\mathrm{end}}}^{(1)}\right] \approx 0$, $\quad 1 - \Pr\left[E_{\beta_{\mathrm{end}}}^{(1)}\right] \approx 1$

- The predication of the success rate of solving LWE given by Eq. (4) is consistent with the experimental results.

Our Refined LWE Estimator in Two-step Mode

$\mathrm{gate}(\beta)$: The gate count of a sieve algorithm with dimension β.

$\mathrm{pgate}(\beta) = C \cdot \mathrm{gate}(\beta)$: The gate count of a progressive sieve algorithm with dimension β.

$\mathrm{pbgate}(\beta) = (d - \beta + 1) \cdot \mathrm{pgate}(\beta)$: The gate count of BKZ-$\beta$.

$\mathrm{pbgate}(\beta, J) = \frac{d-\beta+1}{J} \cdot \mathrm{pgate}(\beta)$: The gate count of PnjBKZ-(β, J).

Gate Count of reduction step: $G_1 = \sum_{i=1}^{\mathrm{end}} \Pr\left[\mathrm{W}_{\beta_i}^{(1)}\right] \cdot \left(1 - \Pr\left[\mathrm{E}_{\beta_{i-1}}^{(1)}\right]\right) \cdot \left[\sum_{j=0}^{i} \mathrm{pbgate}\left(\beta_j - \mathrm{d4f}(\beta_j)\right)\right]$

Gate Count of search step: $G_2 = \sum_{i=d_{\mathrm{start}}}^{d_{\mathrm{svp}}} \Pr\left[\mathrm{E}_i^{(2)}\right] \cdot \left(1 - \Pr\left[\mathrm{E}_{\beta_{\mathrm{end}}}^{(1)}\right]\right) \cdot \left[\left(\sum_{j=0}^{\mathrm{end}} \mathrm{pbgate}\left(\beta_j - \mathrm{d4f}(\beta_j)\right)\right) + \mathrm{pgate}\left(i - \mathrm{d4f}(i)\right)\right]$

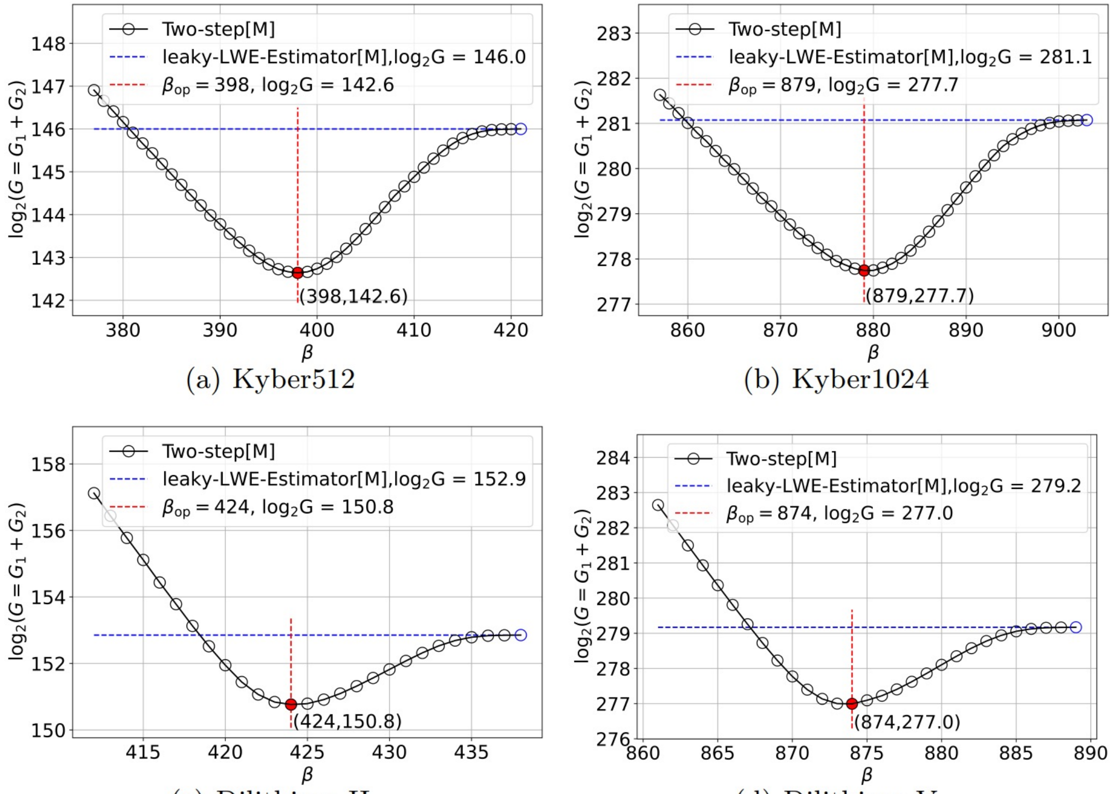
Total Gate Count: $G = G_1 + G_2$

Memory Count of reduction step: $B_1 = \sum_{i=1}^{\mathrm{end}} \Pr\left[\mathrm{W}_{\beta_i}^{(1)}\right] \cdot \left(1 - \Pr\left[\mathrm{E}_{\beta_{i-1}}^{(1)}\right]\right) \cdot \mathrm{bit}\left(\beta_j - \mathrm{d4f}(\beta_j)\right)$

Memory Count of search step: $B_2 = \sum_{i=d_{\mathrm{start}}}^{d_{\mathrm{svp}}} \Pr\left[\mathrm{E}_i^{(2)}\right] \cdot \left(1 - \Pr\left[\mathrm{E}_{\beta_{\mathrm{end}}}^{(1)}\right]\right) \cdot \max\left\{\mathrm{bit}\left(\beta_j - \mathrm{d4f}(\beta_j)\right), \mathrm{bit}\left(i - \mathrm{d4f}(i)\right)\right\}$

Total Memory Count: $B = B_1 + B_2$

Our Refined LWE Estimator in Two-step Mode



(a) Kyber512 (b) Kyber1024 (c) Dilithium-II (d) Dilithium-V

Estimation Comparison with leaky-LWE-Estimator

- The Two-step mode is faster than that of using BKZ reduction only.

input : n, m, q, χ, S;
output: $\mathsf{GB}_{\min}$;
Function TwoStepLWEEsimator(n, m, q, χ, S):
  $\mathsf{GB}_{\min} \leftarrow (+\infty, +\infty)$; $\mathsf{GB} \leftarrow (0, 0)$; $\mathsf{GB}_{\mathrm{pre}} \leftarrow (0, 0)$; $p_{\mathrm{tot}} \leftarrow 0$;
  rr $\leftarrow$ expected length of GS-basis of an LLL reduced $\mathrm{LWE}_{n,m,q,\chi}$ instance
  for $\beta \in$ S *or* $(\beta, J) \in$ S **do**
    rr $\leftarrow$ BKZSim(rr, β); // PnjBKZSim(rr, β, J) if $J > 1$;
    $P(\beta) \leftarrow \Pr\left[x \leftarrow \chi^2_\beta \middle| x \leq (\mathrm{rr}[d-\beta])^2\right]$;
    $\mathsf{GB}_{\mathrm{cum}} \leftarrow (\sum_{b=\beta_0}^{\beta} \mathtt{pbgate}(b - \mathtt{d4f}(b)), \mathtt{bit}(\beta - \mathtt{d4f}(\beta)))$;
    $\mathsf{GB}_{\mathrm{pre}} \leftarrow \mathsf{GB}_{\mathrm{pre}} + \mathsf{GB}_{\mathrm{cum}} \cdot (1 - p_{\mathrm{tot}}) \cdot P(\beta)$;
    $p_{\mathrm{tot}} \leftarrow p_{\mathrm{tot}} + (1 - p_{\mathrm{tot}}) \cdot P(\beta)$; $\mathsf{GB}_{\mathrm{csieve}} \leftarrow (0, 0)$; $P(d_{\mathrm{start}} - 1) \leftarrow 0$;
    for $d_{\mathrm{svp}} \leftarrow d_{\mathrm{start}}$ **to** d **do**
      $P(d_{\mathrm{svp}}) \leftarrow \Pr\left[x \leftarrow \chi^2_{d_{\mathrm{svp}}} \middle| x \leq (\mathrm{GH}(\mathrm{rr}_{[d-d_{\mathrm{svp}}:d]}))^2\right]$;
      $\mathsf{GB}_{\mathrm{cum}}[0] \leftarrow \mathsf{GB}_{\mathrm{cum}}[0] + \mathtt{pgate}(d_{\mathrm{svp}} - \mathtt{d4f}(d_{\mathrm{svp}}))$;
      $\mathsf{GB}_{\mathrm{cum}}[1] \leftarrow \max\{\mathsf{GB}_{\mathrm{cum}}[1], \mathtt{bit}(d_{\mathrm{svp}} - \mathtt{d4f}(d_{\mathrm{svp}}))\}$;
      $\mathsf{GB}_{\mathrm{csieve}} \leftarrow \mathsf{GB}_{\mathrm{csieve}} + \mathsf{GB}_{\mathrm{cum}} \cdot (1 - p_{\mathrm{tot}}) \cdot (P(d_{\mathrm{svp}}) - P(d_{\mathrm{svp}} - 1))$;
      if $p_{\mathrm{tot}} + (1 - p_{\mathrm{tot}}) \cdot P(d_{\mathrm{svp}}) \geq 0.999$ **then**
        break;
    $\mathsf{GB} \leftarrow \mathsf{GB}_{\mathrm{pre}} + \mathsf{GB}_{\mathrm{csieve}}$;
    if $\mathsf{GB}[0] < \mathsf{GB}_{\min}[0]$ **then**
      $\mathsf{GB}_{\min} \leftarrow \mathsf{GB}$;
  return $\mathsf{GB}_{\min}$;

Algorithm 2: Two-step LWE Estimator

05

Improved Conservative Estimation for LWE

Improved Conservative Estimation for LWE

Notation

V: Lattice Volume.

$\delta(\beta)$: The root Hermite factor of a BKZ-β reduced lattice basis.

$\mathrm{rhf}(\delta,\beta)$: A new root Hermite factor of lattice basis after one BKZ-β tour under GSA.

$\mathrm{md}(\delta,M)$: Minimum dimension for sieving to find the target vector with norm M.

Heuristic 5

BKZ is the optimal algorithm for lattice reduction, i.e. generating a lattice basis satisfying GSA.

Heuristic 6

The best way of solving $uSVP_\gamma$ or LWE is by performing lattice sieving on a projected sublattice of a reduced lattice basis satisfying GSA.

Improved Conservative Estimation for LWE

How to compute $\mathrm{rhf}(\delta, \beta)$?

basis quality δ
lattice Volume V

GS-lengths under GSA
$\left(\delta^d V^{\frac{1}{d}}, \alpha\delta^d V^{\frac{1}{d}}, \dots, \alpha^{d-1}\delta^d V^{\frac{1}{d}}\right)$,
$\alpha = \delta^{-\frac{d-1}{2d}}$

Case 1: $\delta > \delta(\beta)$

(Lattice basis could be further reduced by BKZ-β)

1. Compute $\|\boldsymbol{b}_0\|$ after a BKZ-β by $\mathrm{GH}\left(\mathcal{L}_{\pi[0:\beta]}\right)$
2. Expand the remain GS-lengths by GSA.

new RHF

$$\mathrm{rhf}(\delta, \beta) \approx \left(\sqrt{\frac{\beta}{2\pi e} \cdot \delta^{\frac{d(d-\beta)}{d-1}}}\right)^{\frac{1}{d}} = \delta^{\frac{d-\beta}{d-1}} \cdot \left(\frac{\beta}{2\pi e}\right)^{\frac{1}{2d}}$$

Case 2: $\delta \leq \delta(\beta)$

(Lattice basis cannot be further reduced by BKZ-β)

$$\mathrm{rhf}(\delta, \beta) = \delta$$

Improved Conservative Estimation for LWE

input : M, $V \leftarrow \mathrm{Vol}(\mathcal{L})$;
output: T;
Function LowerBoundEst(M, $V \leftarrow \mathrm{Vol}(\mathcal{L})$):
  for $\beta \leftarrow \beta_0$ **to** d **do**
    con $\leftarrow$ true;
    $d_{\mathrm{svp}} \leftarrow \mathsf{md}(\delta(\beta), M)$;
    for $\beta' \leftarrow \beta + 1$ **to** d **do**
      $\delta' \leftarrow \mathsf{rhf}(\delta(\beta), \beta')$;
      if $T_{\mathrm{sieve}}(d_{\mathrm{svp}}) > T_{\mathrm{BKZ}}(\beta') + T_{\mathrm{sieve}}(\mathsf{md}(\delta', M))$ **then**
        con $\leftarrow$ false; break;
    if con **then**
      $\beta_{\mathrm{optimal}} \leftarrow \beta$;
      return β_{optimal}, d_{svp}, $T_{\mathrm{sieve}}(d_{\mathrm{svp}})$;

Algorithm 4: Lower Bound Estimation

Find a β and $d_{\mathrm{svp}} = \mathrm{md}(\delta(\beta), M)$ such that

$$T_{\mathrm{sieve}}(d_{\mathrm{svp}}) \le T_{\mathrm{BKZ}}(\beta') + T_{\mathrm{sieve}}(\mathrm{md}(\delta', M))$$

holds for all $\beta' \ge \beta + 1$, where $\delta' = \mathrm{rhf}(\delta(\beta), \beta')$. Then, output $T_{\mathrm{sieve}}(d_{\mathrm{svp}})$ as the Lower Bound Estimation of LWE(or uSVP).

Find a β and d_{svp} such that one more BKZ-β' before last sieve cannot shorten the total cost for solving LWE(or uSVP).

Theorem 2. *Assume that Gaussian Heuristic (Heuristic 1), GSA(Heuristic 2), Heuristic 5, 6, and Heuristic 4 in [7] hold, then the estimated cost of our lower bound estimation is strictly lower than the actual cost for solving uSVP$_\gamma$ in almost all lattices.*

Improved Conservative Estimation for LWE

input : $m_{\max}$, n, σ, q;
output: β_{optimal}, d_{svp}, $T_{\text{sieve}}(d_{\text{svp}})$;

Function `LowerBoundEstWithOptimalM`($m_{\max}$, n, σ, q):
    $d^*_{\text{svp}} \leftarrow m_{\max} + n + 1$; $m_{\text{optimal}} \leftarrow m_{\max}$; $\beta_{\text{optimal}} \leftarrow m_{\max} + n + 1$;
    for $m \leftarrow m_{\max}$ **to** 1 **do**
        $d \leftarrow n + m + 1$; $M \leftarrow \sigma \cdot \sqrt{d}$; $V \leftarrow q^m$;
        $\beta_{\text{current}}, d_{\text{svp}}, T_{\text{sieve}}(d_{\text{svp}}) \leftarrow$ `LowerBoundEst`(M, V);
        if $d^*_{\text{svp}} > d_{\text{svp}}$ **then**
            $d^*_{\text{svp}} \leftarrow d_{\text{svp}}$; $m_{\text{optimal}} \leftarrow m$; $\beta_{\text{optimal}} \leftarrow \beta_{\text{current}}$;
    $d_{\text{optimal}} \leftarrow m_{\text{optimal}} + n + 1$;
    return d_{optimal}, β_{optimal}, d^*_{svp}, $T_{\text{sieve}}(d^*_{\text{svp}})$;

Algorithm 5: Lower Bound Estimation with Optimal m

- Numerically optimize the number of LWE samples m to minimize the lower-bound security estimation by Alg. 5.

06

Estimated Results

Estimated Results

NIST standards	$\log_2 G/\log_2(\text{gates})^*$			$\log_2 B/\log_2(\text{bits})$			$\Delta\log_2 G$	
	Previous	Our Refined LWE Estimator		Previous	Our Refined LWE Estimator			
		S_0	S_{op}		S_0	S_{op}	S_0	S_{op}
Kyber512	146.0	142.6	141.4	94.0	99.1	98.1	3.4	4.6
Kyber768	208.9	205.5	204.4	138.7	144	143.2	3.4	4.5
Kyber1024	281.1	277.7	276.9	189.78	195.4	194.6	3.3	4.2
Dilithium-II	152.9	150.8	150.6	98.0	104.3	104.4	2.1	2.3
Dilithium-III	210.2	207.9	207.9	138.8	145.3	145.3	2.3	2.3
Dilithium-V	279.2	277.0	277.0	187.5	194.1	194.1	2.2	2.2

Estimation of NIST standards by Our Refined LWE Estimator

- S_0: Trivial Progressive BKZ in Two-step mode
- S_{op}: Progressive BKZ in Two-step mode with strategy generated by EnumBS[7]
- * : Gate Count of all estimations in this Table uses the improved list-decoding technique proposed by MATZOV[6]
- The security bit drops by 2.2~4.6 bits.

Estimated Results

NIST standards	Kyber512	Kyber768	Kyber1024	DilithiumII	DilithiumIII	DilithiumV
Lattice Dim d	1003	1424	1885	2049	2561	3582
BKZ β	406	625	877	423	624	863
CoreSVP	118	182	256	123	182	252
Lattice Dim d	1025	1477	1954	2039	2672	3461
β_{optimal}	392	608	857	415	614	853
d_{svp}	423	641	891	449	649	889
LBE	123.52	187.17	260.17	131.11	189.51	259.59
LBE(d4f)	112.44	172.32	241.24	119.57	174.52	240.69
ΔHardness	5.52	5.17	4.17	8.11	7.51	7.59
ΔHardness(d4f)	-5.56	-9.68	-14.76	-3.43	-7.48	-11.31

Estimation of NIST standards by Our Lower Bound LWE Estimator

- Our lower bound estimation is 4.17~8.11 bits higher than the Core-SVP estimation.
- If considering d4f technique, lower bound estimation will decrease by 3.42 ~ 14.76 bits, which declares that Core-SVP model is not conservative enough to offset the influence of the d4f technique.

PKC2024

Thanks

Article Access: https://eprint.iacr.org/2024/067.pdf

Open Source Code for Estimator: https://github.com/Summwer/lwe-estimator-with-pnjbkz/tree/refined-lwe-estimator

Open Source Code for Verfication Experiments: https://github.com/Summwer/test-for-refined-lwe-estimator

Reference

[1] Mingjie Liu, and Phong Q. Nguyen. "Solving BDD by Enumeration: An Update." In *Topics in Cryptology – CT-RSA 2013*, edited by Ed Dawson, 293 – 309. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2013.
[2] Alkim, Erdem, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. "Post-Quantum Key Exchange—A New Hope," 327 – 43, 2016.
[3] https://github.com/malb/lattice-estimator
[4] Dachman-Soled, Dana, Léo Ducas, Huijing Gong, and Mélissa Rossi. "LWE with Side Information: Attacks and Concrete Security Estimation." In Advances in Cryptology – CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17 – 21, 2020, Proceedings, Part II, 329 – 58. Berlin, Heidelberg: Springer-Verlag, 2020. https://doi.org/10.1007/978-3-030-56880-1_12.
[5] Postlethwaite, Eamonn W., and Fernando Virdia. "On the Success Probability of Solving Unique SVP via BKZ." In *Public-Key Cryptography – PKC 2021*, edited by Juan A. Garay, 12710:68 – 98. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2021.
[6] MATZOV, "Report on the Security of LWE: Improved Dual Lattice Attack." Accessed April 12, 2022.
[7] W. Xia, L. Wang, GengWang, D. Gu, and B. Wang, "Improved progressive bkz with lattice sieving." Cryptology ePrint Archive, Paper 2022/1343, 2022. https: //eprint.iacr.org/archive/2022/1343/1697360937.pdf.