Cool + Cruel = Dual

and New Benchmarks for Sparse LWE

Alexander Karenin
Technology Innovation Institute
Elena Kirshanova
Technology Innovation Institute
Julian Nowakowski
Ruhr University Bochum → Centrum Wiskunde & Informatica
Eamonn W. Postlethwaite
King's College London
Ludo N. Pulles
Centrum Wiskunde & Informatica → Institut de Mathématiques de Bordeaux
Fernando Virdia
University of Surrey
Paul Vié
Télécom Paris

(Sparse) LWE

LWE:

Given:

- $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$,
- $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$, where $\|\mathbf{e}\|$ is small

Find:

- $\mathbf{s} \in \mathbb{Z}_q^n$

Sparse LWE:

- $\mathbf{s}$ has low Hamming weight (and small entries)
- relevant for FHE, but not for ML-KEM/Kyber

(Sparse) LWE

LWE:

Given:

- $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$,
- $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$, where $\|\mathbf{e}\|$ is small

Find:

- $\mathbf{s} \in \mathbb{Z}_q^n$

Sparse LWE:

- $\mathbf{s}$ has low Hamming weight (and small entries)
- relevant for FHE, but not for ML-KEM/Kyber

Wenger, Saxena, Malhou, Thieu, Lauter

Benchmarking Attacks on Learning with Errors

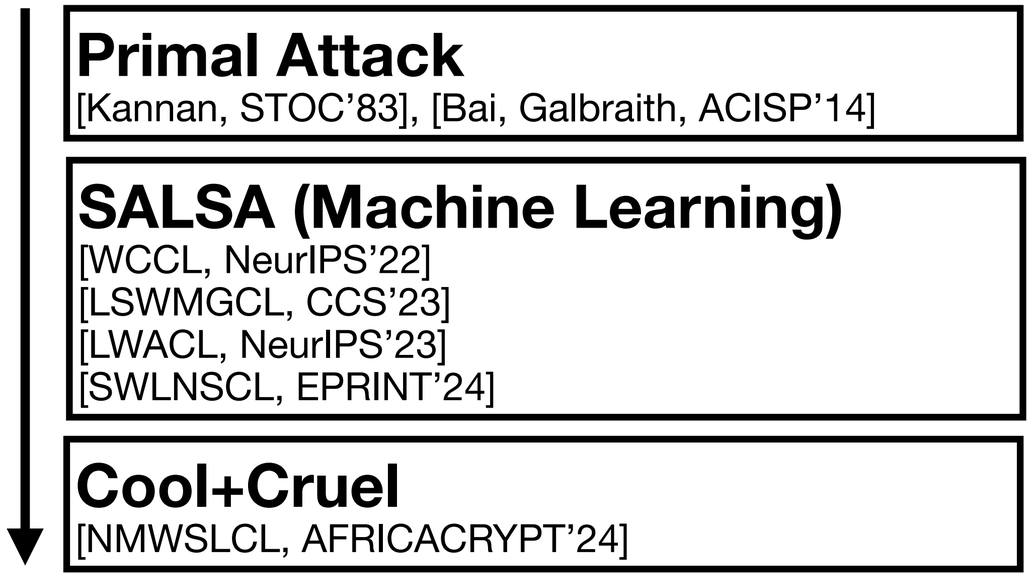
S&P'25

- benchmarks of Sparse LWE attacks on an industrial-scale cluster
- did not consider all relevant attacks

Attacks on Sparse LWE

[WSMTL, S&P'25] benchmarks suggest:

worst



best

Attacks on Sparse LWE

[WSMTL, S&P'25] benchmarks suggest:

worst

Primal Attack
[Kannan, STOC'83], [Bai, Galbraith, ACISP'14]

SALSA (Machine Learning)
[WCCL, NeurIPS'22]
[LSWMGCL, CCS'23]
[LWACL, NeurIPS'23]
[SWLNSCL, EPRINT'24]

Cool+Cruel
[NMWSLCL, AFRICACRYPT'24]

best

We show:

=

Dual Attack
[Aharonov, Regev, FOCS'05]
[Albrecht, EC'17]

Attacks on Sparse LWE

[WSMTL, S&P'25] benchmarks suggest:

worst

Primal Attack
[Kannan, STOC'83], [Bai, Galbraith, ACISP'14]

SALSA (Machine Learning)
[WCCL, NeurIPS'22]
[LSWMGCL, CCS'23]
[LWACL, NeurIPS'23]
[SWLNSCL, EPRINT'24]

Cool+Cruel
[NMWSLCL, AFRICACRYPT'24]

best

We show:

=

Dual Attack
[Aharonov, Regev, FOCS'05]
[Albrecht, EC'17]

<

Primal Attack
Drop+Solve [May, Silverman, CaLC'01]
Guess+Verify [Albrecht, Curtis, Wunderer, SAC'19]

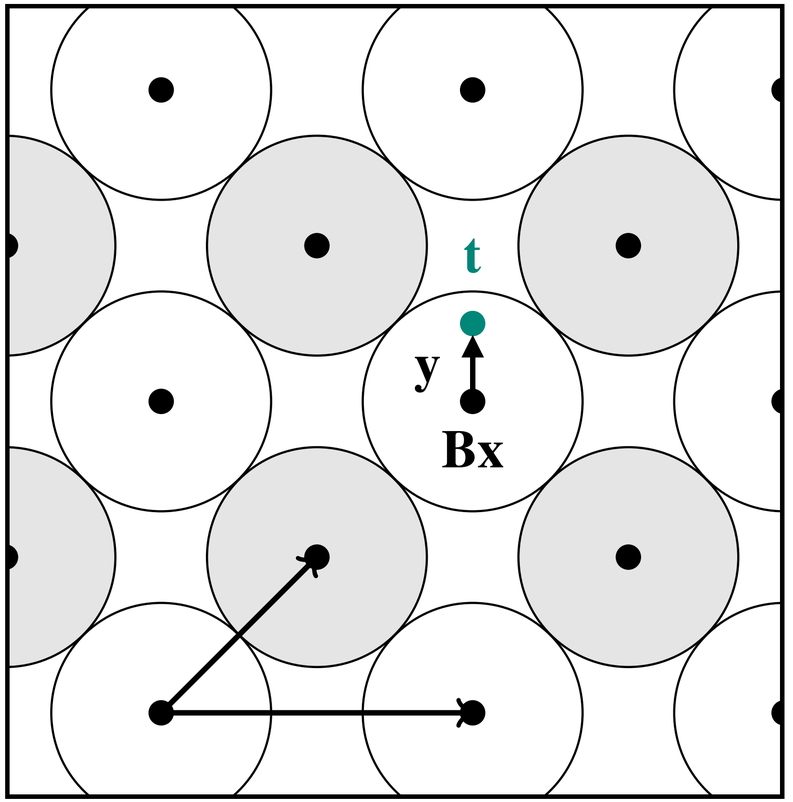
Bounded Distance Decoding (BDD)

Given:

- basis $\mathbf{B}$ of a lattice $\mathscr{L}(\mathbf{B}) := \mathbf{B} \cdot \mathbb{Z}^d$,
- $\mathbf{t} = \mathbf{B}\mathbf{x} + \mathbf{y}$, where $\mathbf{x} \in \mathbb{Z}^d$, and $\|\mathbf{y}\|$ is small

Find:

- $\mathbf{x} \in \mathbb{Z}^d$ minimizing $\|\mathbf{t} - \mathbf{B}\mathbf{x}\|$ (promised to be unique)



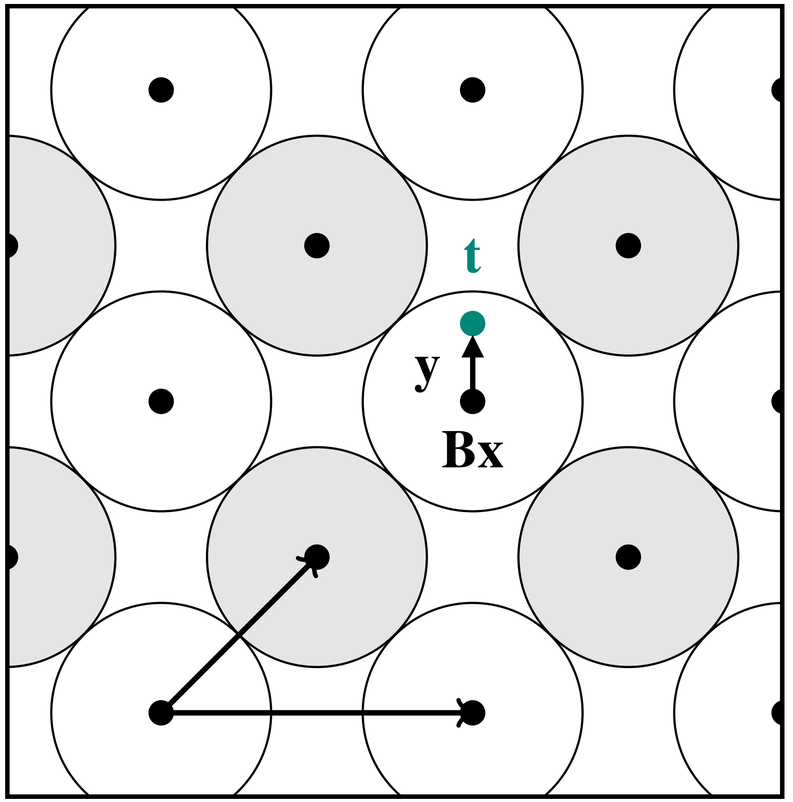
Bounded Distance Decoding (BDD)

Given:

- basis $\mathbf{B}$ of a lattice $\mathcal{L}(\mathbf{B}) := \mathbf{B} \cdot \mathbb{Z}^d$,
- $\mathbf{t} = \mathbf{Bx} + \mathbf{y}$, where $\mathbf{x} \in \mathbb{Z}^d$, and $\|\mathbf{y}\|$ is small

Find:

- $\mathbf{x} \in \mathbb{Z}^d$ minimizing $\|\mathbf{t} - \mathbf{Bx}\|$ (promised to be unique)



Sparse LWE $\mathbf{b} \equiv \mathbf{As} + \mathbf{e} \mod q$:

$$\mathcal{L}(\mathbf{B}) = \left\{(\mathbf{v}_1, \mathbf{v}_2) \in \mathbb{Z}^n \times \mathbb{Z}^m \mid \mathbf{v}_2 \equiv -\mathbf{A}\mathbf{v}_1 \mod q\right\}$$

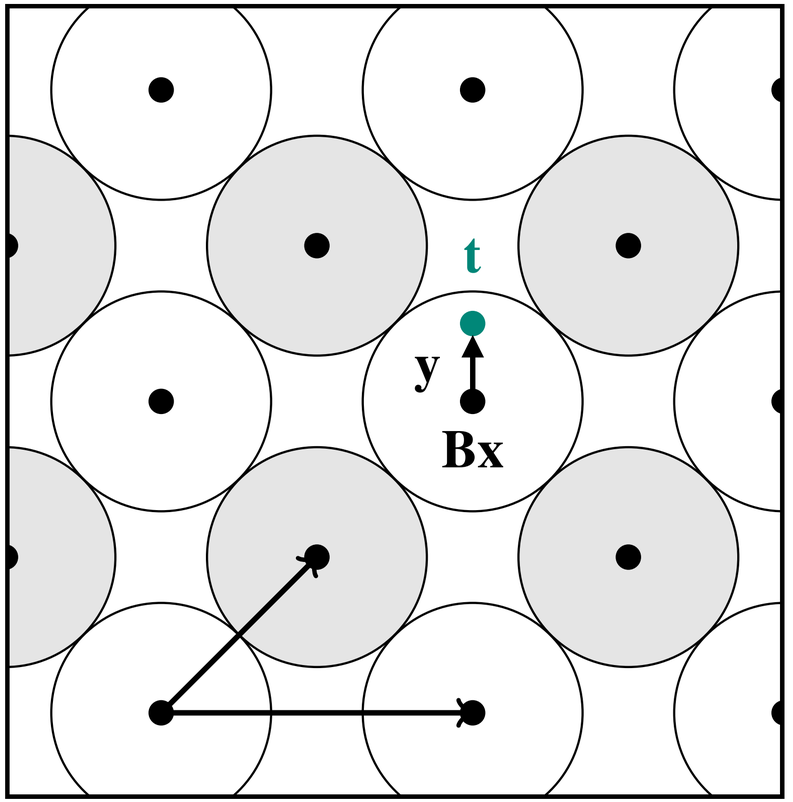
Bounded Distance Decoding (BDD)

Given:

- basis $\mathbf{B}$ of a lattice $\mathcal{L}(\mathbf{B}) := \mathbf{B} \cdot \mathbb{Z}^d$,
- $\mathbf{t} = \mathbf{Bx} + \mathbf{y}$, where $\mathbf{x} \in \mathbb{Z}^d$, and $\|\mathbf{y}\|$ is small

Find:

- $\mathbf{x} \in \mathbb{Z}^d$ minimizing $\|\mathbf{t} - \mathbf{Bx}\|$ (promised to be unique)



Sparse LWE $\mathbf{b} \equiv \mathbf{As} + \mathbf{e} \mod q$**:**

$$\mathcal{L}(\mathbf{B}) = \left\{(\mathbf{v}_1, \mathbf{v}_2) \in \mathbb{Z}^n \times \mathbb{Z}^m \mid \mathbf{v}_2 \equiv -\mathbf{A}\mathbf{v}_1 \mod q\right\}$$

$$\mathbf{Bx} = (-\mathbf{s}, \mathbf{b} - \mathbf{e}), \qquad \mathbf{y} = (\mathbf{s}, \mathbf{e}), \qquad \mathbf{t} = (0^n, \mathbf{b})$$

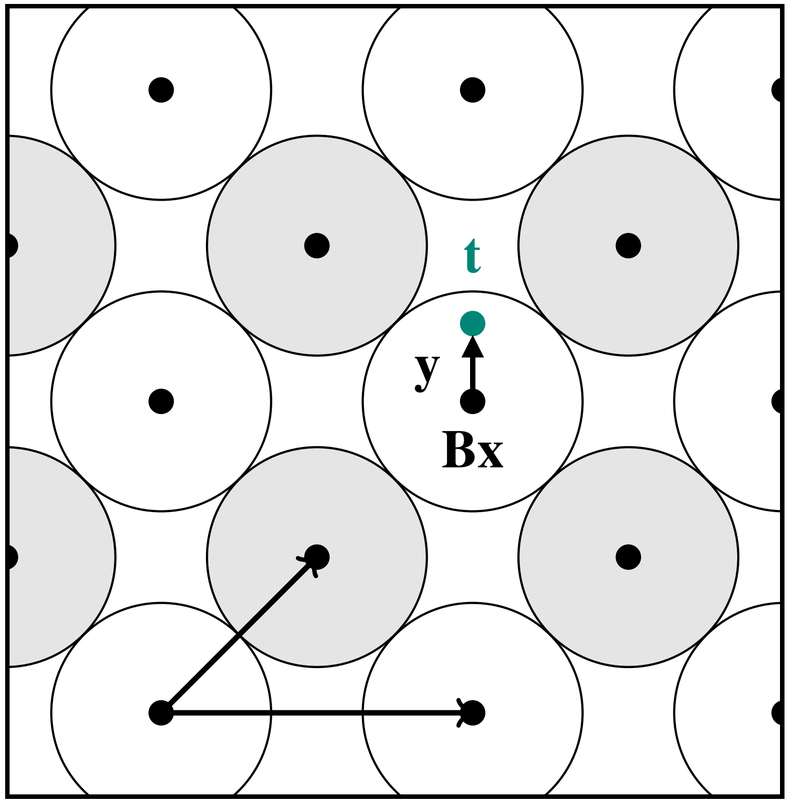
Bounded Distance Decoding (BDD)

Given:

- basis $\mathbf{B}$ of a lattice $\mathcal{L}(\mathbf{B}) := \mathbf{B} \cdot \mathbb{Z}^d$,
- $\mathbf{t} = \mathbf{Bx} + \mathbf{y}$, where $\mathbf{x} \in \mathbb{Z}^d$, and $\|\mathbf{y}\|$ is small

Find:

- $\mathbf{x} \in \mathbb{Z}^d$ minimizing $\|\mathbf{t} - \mathbf{Bx}\|$ (promised to be unique)



Sparse LWE $\mathbf{b} \equiv \mathbf{As} + \mathbf{e} \mod q$**:**

$$\mathcal{L}(\mathbf{B}) = \left\{(\mathbf{v}_1, \mathbf{v}_2) \in \mathbb{Z}^n \times \mathbb{Z}^m \mid \mathbf{v}_2 \equiv -\mathbf{A}\mathbf{v}_1 \mod q\right\}$$

$$\mathbf{Bx} = (-\mathbf{s}, \mathbf{b} - \mathbf{e}), \qquad \mathbf{y} = (\mathbf{s}, \mathbf{e}), \qquad \mathbf{t} = (0^n, \mathbf{b})$$

→ relatively few candidates for $\mathbf{Bx}$

☞ hybrid attacks: lattice reduction + enumeration

Hybrid Attacks

Step 1:

- Split BDD instance $\mathbf{t} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{B}_1\mathbf{x}_1 + \mathbf{y}$
- Enumerate list of $\mathbf{t}^{(i)} := \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$

$$\mathbf{B} = [\mathbf{B}_0, \mathbf{B}_1], \quad \mathbf{x} = \begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_1 \end{pmatrix}$$

Step 2:

- Identify i^* with $\mathbf{t}^{(i^*)} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{y}$
- Solve lower-dim. BDD instance on $\mathscr{L}(\mathbf{B}_0)$

Hybrid Attacks

Step 1:

- Split BDD instance $\mathbf{t} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{B}_1\mathbf{x}_1 + \mathbf{y}$
- Enumerate list of $\mathbf{t}^{(i)} := \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$

$$\mathbf{B} = [\mathbf{B}_0, \mathbf{B}_1], \quad \mathbf{x} = \begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_1 \end{pmatrix}$$

Step 2:

- Identify i^* with $\mathbf{t}^{(i^*)} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{y}$
- Solve lower-dim. BDD instance on $\mathscr{L}(\mathbf{B}_0)$

Primal attacks:

- Apply BDD solver to every $\mathbf{t}^{(i)}$
- Yields candidates $\mathbf{x}_0^{(i)}$ for $\mathbf{x}_0$
- Take the index i that minimizes

$$\|\mathbf{t} - \mathbf{B}(\mathbf{x}_0^{(i)}, \mathbf{x}_1^{(i)})^T\|$$

Hybrid Attacks

Step 1:

- Split BDD instance $\mathbf{t} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{B}_1\mathbf{x}_1 + \mathbf{y}$
- Enumerate list of $\mathbf{t}^{(i)} := \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$

$$\mathbf{B} = [\mathbf{B}_0, \mathbf{B}_1], \quad \mathbf{x} = \begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_1 \end{pmatrix}$$

Step 2:

- Identify i^* with $\mathbf{t}^{(i^*)} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{y}$
- Solve lower-dim. BDD instance on $\mathscr{L}(\mathbf{B}_0)$

Primal attacks:

- Apply BDD solver to every $\mathbf{t}^{(i)}$
- Yields candidates $\mathbf{x}_0^{(i)}$ for $\mathbf{x}_0$
- Take the index i that minimizes

$$\|\mathbf{t} - \mathbf{B}(\mathbf{x}_0^{(i)}, \mathbf{x}_1^{(i)})^T\|$$

Dual attacks:

- Compute many short vectors $\mathbf{w} \in \mathscr{L}(\mathbf{B}_0)^*$
- Apply test to all $\langle \mathbf{t}^{(i)}, \mathbf{w} \rangle$

Hybrid Attacks

Step 1:

- Split BDD instance $\mathbf{t} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{B}_1\mathbf{x}_1 + \mathbf{y}$
- Enumerate list of $\mathbf{t}^{(i)} := \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$

$$\mathbf{B} = [\mathbf{B}_0, \mathbf{B}_1], \quad \mathbf{x} = \begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_1 \end{pmatrix}$$

Step 2:

- Identify i^* with $\mathbf{t}^{(i^*)} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{y}$
- Solve lower-dim. BDD instance on $\mathscr{L}(\mathbf{B}_0)$

Primal attacks:

- Apply BDD solver to every $\mathbf{t}^{(i)}$
- Yields candidates $\mathbf{x}_0^{(i)}$ for $\mathbf{x}_0$
- Take the index i that minimizes

$$\|\mathbf{t} - \mathbf{B}(\mathbf{x}_0^{(i)}, \mathbf{x}_1^{(i)})^T\|$$

Dual attacks:

- Compute many short vectors $\mathbf{w} \in \mathscr{L}(\mathbf{B}_0)^*$
- Apply test to all $\langle \mathbf{t}^{(i)}, \mathbf{w} \rangle$
- Idea:
  - $\langle \mathbf{t}^{(i)}, \mathbf{w} \rangle$ reveals information on $\mathrm{dist}(\mathbf{t}^{(i)}, \mathscr{L}(\mathbf{B}_0))$
  - $\mathrm{dist}(\mathbf{t}^{(i^*)}, \mathscr{L}(\mathbf{B}_0)) < \mathrm{dist}(\mathbf{t}^{(i)}, \mathscr{L}(\mathbf{B}_0)), \ i \neq i^*$

Hybrid Attacks

Guess+Verify

Cool+Cruel

+ information set decoding

Primal attacks:

- Apply BDD solver to every $\mathbf{t}^{(i)}$
- Yields candidates $\mathbf{x}_0^{(i)}$ for $\mathbf{x}_0$
- Take the index i that minimizes

$$\|\mathbf{t} - \mathbf{B}(\mathbf{x}_0^{(i)}, \mathbf{x}_1^{(i)})^T\|$$

Dual attacks:

- Compute many short vectors $\mathbf{w} \in \mathscr{L}(\mathbf{B}_0)^*$
- Apply test to all $\langle \mathbf{t}^{(i)}, \mathbf{w} \rangle$
- Idea:
  - $\langle \mathbf{t}^{(i)}, \mathbf{w} \rangle$ reveals information on $\mathrm{dist}(\mathbf{t}^{(i)}, \mathscr{L}(\mathbf{B}_0))$
  - $\mathrm{dist}(\mathbf{t}^{(i^*)}, \mathscr{L}(\mathbf{B}_0)) < \mathrm{dist}(\mathbf{t}^{(i)}, \mathscr{L}(\mathbf{B}_0)),\ i \neq i^*$

Cool+Cruel < Guess+Verify

Sparse LWE with $n = 512$, $q \approx 2^{28}$

Cool+Cruel < Guess+Verify

Sparse LWE with $n = 512, q \approx 2^{28}$

[WSMTL, S&P'25]

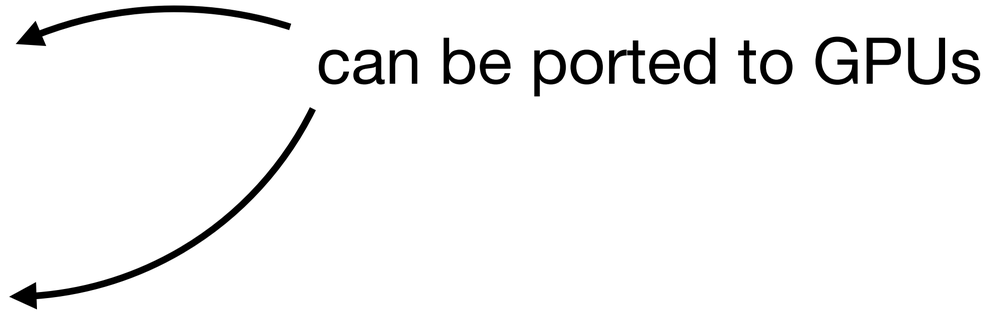
Primal Attack 1 CPU
Cool+Cruel **lattice reduction** 151 CPUs
Cool+Cruel **enumeration** 256 GPUs

Cool+Cruel < Guess+Verify

Sparse LWE with $n = 512, q \approx 2^{28}$

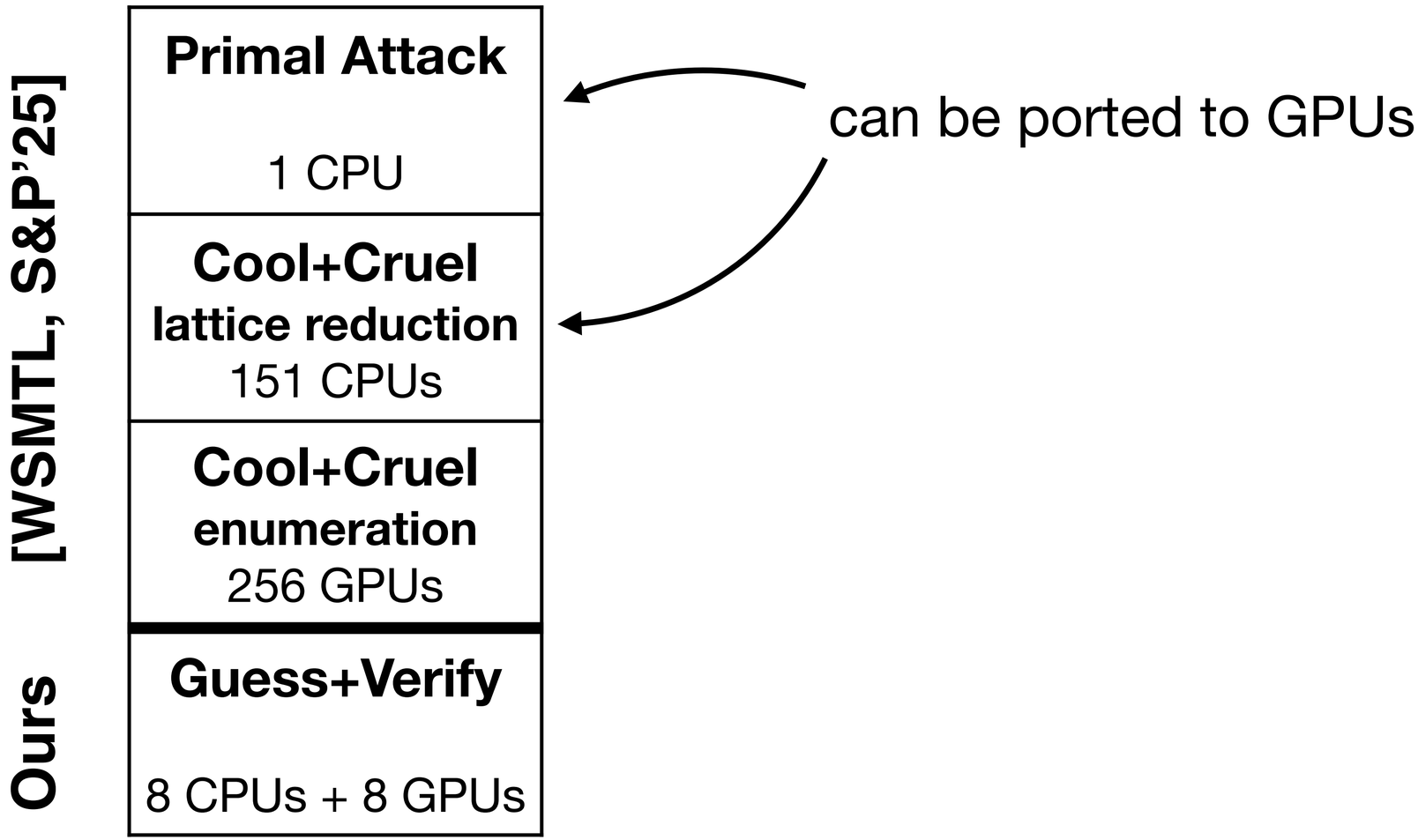
[WSMTL, S&P'25]

Primal Attack 1 CPU
Cool+Cruel **lattice reduction** 151 CPUs
Cool+Cruel **enumeration** 256 GPUs



Cool+Cruel < Guess+Verify

Sparse LWE with $n = 512, q \approx 2^{28}$



Cool+Cruel < Guess+Verify

Sparse LWE with $n = 512, q \approx 2^{28}$

[WSMTL, S&P'25]

Primal Attack

1 CPU

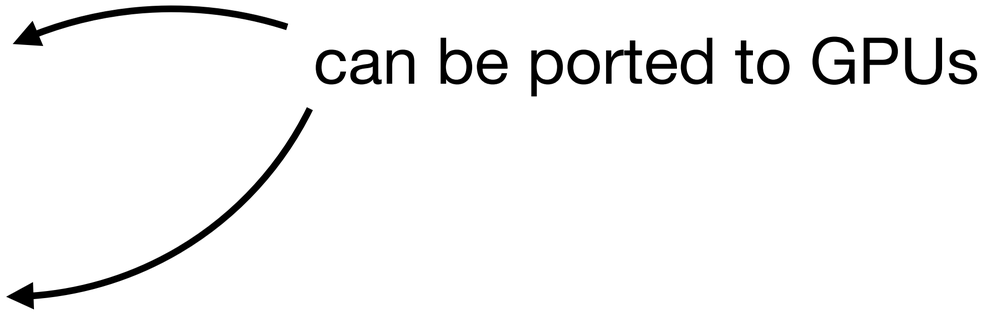
Cool+Cruel
lattice reduction
151 CPUs

Cool+Cruel
enumeration
256 GPUs

Ours

Guess+Verify

8 CPUs + 8 GPUs



Hamming weight	**20**	**21**	**25**
Cool+Cruel enumeration min. GPU-hours	**38**	**141**	**10642**
Guess+Verify avg. GPU-hours	**23**	**38**	**164**

Conclusion

Summary:

- Drop+Solve/Guess+Verify Primal > Cool+Cruel = Dual

Conclusion

Summary:

- Drop+Solve/Guess+Verify Primal > Cool+Cruel = Dual

Lessons learned:

- LWE view can obfuscate important details.
- BDD view often yields a simpler analysis, and can prevent reinventing known attacks.

Conclusion

Summary:

- Drop+Solve/Guess+Verify Primal > Cool+Cruel = Dual

Lessons learned:

- LWE view can obfuscate important details.
- BDD view often yields a simpler analysis, and can prevent reinventing known attacks.

Food for thought:

- Are there BDD/LWE regimes where dual outperforms primal?

Conclusion

Summary:

- Drop+Solve/Guess+Verify Primal > Cool+Cruel = Dual

Lessons learned:

- LWE view can obfuscate important details.
- BDD view often yields a simpler analysis, and can prevent reinventing known attacks.

Food for thought:

- Are there BDD/LWE regimes where dual outperforms primal?
- More generally, is there a more efficient way to identify $\mathbf{t}^{(i^*)} = \mathbf{B}\mathbf{x}_0 + \mathbf{y}$ among all $\mathbf{t}^{(i)} = \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$ than applying a BDD solver to every $\mathbf{t}^{(i)}$?

Conclusion

Summary:

- Drop+Solve/Guess+Verify Primal > Cool+Cruel = Dual

Lessons learned:

- LWE view can obfuscate important details.
- BDD view often yields a simpler analysis, and can prevent reinventing known attacks.

Food for thought:

- Are there BDD/LWE regimes where dual outperforms primal?
- More generally, is there a more efficient way to identify $\mathbf{t}^{(i^*)} = \mathbf{B}\mathbf{x}_0 + \mathbf{y}$ among all $\mathbf{t}^{(i)} = \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$ than applying a BDD solver to every $\mathbf{t}^{(i)}$?

ia.cr/2025/1002

github.com/ludopulles/eprint-2025-1002

Appendix

Cool+Cruel

Input: LWE instance $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$

Output: First n_u coordinates of $\mathbf{s}^T = (\mathbf{s}_u, \mathbf{s}_r)^T \in \mathbb{Z}^{n_u} \times \mathbb{Z}^{n_r}$

Cool+Cruel

Input: LWE instance $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$

Output: First n_u coordinates of $\mathbf{s}^T = (\mathbf{s}_u, \mathbf{s}_r)^T \in \mathbb{Z}^{n_u} \times \mathbb{Z}^{n_r}$

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \xrightarrow[\text{on submatrices of } \mathbf{D}]{\text{lattice reduction}} \text{many shortish vectors } \mathbf{w} \in \mathscr{L}(\mathbf{D})$$

Cool+Cruel

Input: LWE instance $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$

Output: First n_u coordinates of $\mathbf{s}^T = (\mathbf{s}_u, \mathbf{s}_r)^T \in \mathbb{Z}^{n_u} \times \mathbb{Z}^{n_r}$

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \xrightarrow[\text{on submatrices of } \mathbf{D}]{\text{lattice reduction}} \text{many shortish vectors } \mathbf{w} \in \mathscr{L}(\mathbf{D}) \xrightarrow[\text{has special shape}]{\text{observe that } \mathbf{w}} \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

Cool+Cruel

Input: LWE instance $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$

Output: First n_u coordinates of $\mathbf{s}^T = (\mathbf{s}_u, \mathbf{s}_r)^T \in \mathbb{Z}^{n_u} \times \mathbb{Z}^{n_r}$

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \xrightarrow[\text{on submatrices of } \mathbf{D}]{\text{lattice reduction}} \text{many shortish vectors } \mathbf{w} \in \mathscr{L}(\mathbf{D}) \xrightarrow[\text{has special shape}]{\text{observe that } \mathbf{w}} \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

Already observed and used in [Howgrave-Graham C'07], [Ducas, Espitau, Postlethwaite C'23].
Z-shape of q-ary lattices.

Cool+Cruel

Input: LWE instance $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$

Output: First n_u coordinates of $\mathbf{s}^T = (\mathbf{s}_u, \mathbf{s}_r)^T \in \mathbb{Z}^{n_u} \times \mathbb{Z}^{n_r}$

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \xrightarrow[\text{on submatrices of } \mathbf{D}]{\text{lattice reduction}} \text{many shortish vectors } \mathbf{w} \in \mathscr{L}(\mathbf{D}) \xrightarrow[\text{has special shape}]{\text{observe that } \mathbf{w}} \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

Already observed and used in [Howgrave-Graham C'07], [Ducas, Espitau, Postlethwaite C'23]. **Z-shape of q-ary lattices.**

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{A}_r^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_1^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix}$$

Cool+Cruel

Input: LWE instance $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$

Output: First n_u coordinates of $\mathbf{s}^T = (\mathbf{s}_u, \mathbf{s}_r)^T \in \mathbb{Z}^{n_u} \times \mathbb{Z}^{n_r}$

Already observed and used in [Howgrave-Graham C'07], [Ducas, Espitau, Postlethwaite C'23]. **Z-shape of q-ary lattices.**

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \xrightarrow[\text{on submatrices of } \mathbf{D}]{\text{lattice reduction}} \text{many shortish vectors } \mathbf{w} \in \mathscr{L}(\mathbf{D}) \xrightarrow[\text{has special shape}]{\text{observe that } \mathbf{w}} \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{A}_r^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_1^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix}$$

Enumerate candidates $\mathbf{s}_u^{(i)}$ for $\mathbf{s}_u$. Take the one that makes $\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}}\mathbf{s}_u^{(i)}$ short (mod q).

Cool+Cruel

Input: LWE instance $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$

Output: First n_u coordinates of $\mathbf{s}^T = (\mathbf{s}_u, \mathbf{s}_r)^T \in \mathbb{Z}^{n_u} \times \mathbb{Z}^{n_r}$

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \xrightarrow[\text{on submatrices of } \mathbf{D}]{\text{lattice reduction}} \text{many shortish vectors } \mathbf{w} \in \mathscr{L}(\mathbf{D}) \xrightarrow[\text{has special shape}]{\text{observe that } \mathbf{w}} \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

Already observed and used in [Howgrave-Graham C'07], [Ducas, Espitau, Postlethwaite C'23]. **Z-shape of q-ary lattices.**

short

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{A}_r^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_1^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix} \equiv \begin{pmatrix} \vdots \\ \mathbf{w}_2^T(\mathbf{A}\mathbf{s} + \mathbf{e}) \\ \vdots \end{pmatrix}$$

Enumerate candidates $\mathbf{s}_u^{(i)}$ for $\mathbf{s}_u$. Take the one that makes $\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}}\mathbf{s}_u^{(i)}$ short (mod q).

Cool+Cruel

Input: LWE instance $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$

Output: First n_u coordinates of $\mathbf{s}^T = (\mathbf{s}_u, \mathbf{s}_r)^T \in \mathbb{Z}^{n_u} \times \mathbb{Z}^{n_r}$

Already observed and used in [Howgrave-Graham C'07], [Ducas, Espitau, Postlethwaite C'23]. **Z-shape of q-ary lattices.**

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \xrightarrow[\text{on submatrices of } \mathbf{D}]{\text{lattice reduction}} \text{many shortish vectors } \mathbf{w} \in \mathscr{L}(\mathbf{D}) \xrightarrow[\text{has special shape}]{\text{observe that } \mathbf{w}} \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{A}_r^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_1^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix} \equiv \begin{pmatrix} \vdots \\ \mathbf{w}_2^T(\mathbf{A}\mathbf{s} + \mathbf{e}) \\ \vdots \end{pmatrix} \equiv \mathbf{A}_u^{\text{red}}\mathbf{s}_u + \mathbf{A}_r^{\text{red}}\mathbf{s}_r + \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{e} \rangle \\ \vdots \end{pmatrix} \mod q$$

$$\mathbf{w}_2^T\mathbf{A} \equiv (\mathbf{w}_0, \mathbf{w}_1)^T \mod q$$

Enumerate candidates $\mathbf{s}_u^{(i)}$ for $\mathbf{s}_u$. Take the one that makes $\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}}\mathbf{s}_u^{(i)}$ short (mod q).

Cool+Cruel

Input: LWE instance $\mathbf{b} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \mod q$

Output: First n_u coordinates of $\mathbf{s}^T = (\mathbf{s}_u, \mathbf{s}_r)^T \in \mathbb{Z}^{n_u} \times \mathbb{Z}^{n_r}$

Already observed and used in [Howgrave-Graham C'07], [Ducas, Espitau, Postlethwaite C'23]. **Z-shape of q-ary lattices.**

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \xrightarrow[\text{on submatrices of } \mathbf{D}]{\text{lattice reduction}} \text{many shortish vectors } \mathbf{w} \in \mathscr{L}(\mathbf{D}) \xrightarrow[\text{has special shape}]{\text{observe that } \mathbf{w}} \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{A}_r^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_1^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix} \equiv \begin{pmatrix} \vdots \\ \mathbf{w}_2^T(\mathbf{A}\mathbf{s} + \mathbf{e}) \\ \vdots \end{pmatrix} \equiv \mathbf{A}_u^{\text{red}}\mathbf{s}_u + \mathbf{A}_r^{\text{red}}\mathbf{s}_r + \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{e} \rangle \\ \vdots \end{pmatrix} \mod q$$

$$\mathbf{w}_2^T\mathbf{A} \equiv (\mathbf{w}_0, \mathbf{w}_1)^T \mod q$$

short

Enumerate candidates $\mathbf{s}_u^{(i)}$ for $\mathbf{s}_u$. Take the one that makes $\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}}\mathbf{s}_u^{(i)}$ short (mod q).

Cool+Cruel = Dual

Cool+Cruel:

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \longrightarrow \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix}$$

Enumerate candidates $\mathbf{s}_u^{(i)}$ for $\mathbf{s}_u$.
Take the one that makes
$\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}} \mathbf{s}_u^{(i)}$ short (mod q).

Cool+Cruel = Dual

Cool+Cruel:

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \longrightarrow \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix}$$

Enumerate candidates $\mathbf{s}_u^{(i)}$ for $\mathbf{s}_u$.
Take the one that makes
$\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}} \mathbf{s}_u^{(i)}$ short (mod q).

Dual Attack:

- Split BDD instance $\mathbf{t} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{B}_1\mathbf{x}_1 + \mathbf{y}$
- Compute short vectors $\mathbf{w}' \in \mathscr{L}(\mathbf{B}_0)^*$
- Enumerate $\mathbf{t}^{(i)} := \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$
- Apply test to all $\langle \mathbf{t}^{(i)}, \mathbf{w}' \rangle$

Cool+Cruel = Dual

Cool+Cruel:

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \longrightarrow \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix}$$

Enumerate candidates $\mathbf{s}_u^{(i)}$ for $\mathbf{s}_u$.
Take the one that makes
$\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}} \mathbf{s}_u^{(i)}$ short (mod q).

Dual Attack:

- Split BDD instance $\mathbf{t} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{B}_1\mathbf{x}_1 + \mathbf{y}$
- Compute short vectors $\mathbf{w}' \in \mathscr{L}(\mathbf{B}_0)^*$
- Enumerate $\mathbf{t}^{(i)} := \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$
- Apply test to all $\langle \mathbf{t}^{(i)}, \mathbf{w}' \rangle$

LWE:

- $\mathscr{L}(\mathbf{B}_0)^* \simeq \mathscr{L}(\mathbf{D})$ with first n_u coord. removed

Cool+Cruel = Dual

Cool+Cruel:

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \longrightarrow \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix}$$

Enumerate candidates $\mathbf{s}_u^{(i)}$ for $\mathbf{s}_u$.
Take the one that makes
$\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}} \mathbf{s}_u^{(i)}$ short (mod q).

Dual Attack:

- Split BDD instance $\mathbf{t} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{B}_1\mathbf{x}_1 + \mathbf{y}$
- Compute short vectors $\mathbf{w}' \in \mathscr{L}(\mathbf{B}_0)^*$ ✓
- Enumerate $\mathbf{t}^{(i)} := \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$
- Apply test to all $\langle \mathbf{t}^{(i)}, \mathbf{w}' \rangle$

LWE:

- $\mathscr{L}(\mathbf{B}_0)^* \simeq \mathscr{L}(\mathbf{D})$ with first n_u coord. removed

Cool+Cruel = Dual

Cool+Cruel:

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \longrightarrow \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix}$$

Enumerate candidates $\mathbf{s}_u^{(i)}$ for $\mathbf{s}_u$.
Take the one that makes
$\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}} \mathbf{s}_u^{(i)}$ short (mod q).

Dual Attack:

- Split BDD instance $\mathbf{t} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{B}_1\mathbf{x}_1 + \mathbf{y}$
- Compute short vectors $\mathbf{w}' \in \mathscr{L}(\mathbf{B}_0)^*$ ✓
- Enumerate $\mathbf{t}^{(i)} := \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$
- Apply test to all $\langle \mathbf{t}^{(i)}, \mathbf{w}' \rangle$

LWE:

- $\mathscr{L}(\mathbf{B}_0)^* \simeq \mathscr{L}(\mathbf{D})$ with first n_u coord. removed
- $$\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}} \mathbf{s}_u^{(i)} \equiv \begin{pmatrix} \vdots \\ \left\langle \mathbf{t}^{(i)}, \begin{pmatrix} \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \right\rangle \\ \vdots \end{pmatrix} \mod q$$

Cool+Cruel = Dual

Cool+Cruel:

$$\mathbf{D} := \begin{bmatrix} q\mathbf{I}_n & \mathbf{A}^T \\ & \mathbf{I}_m \end{bmatrix} \longrightarrow \mathbf{w} = \begin{pmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \begin{matrix} \} n_u \\ \} n_r \\ \} m \end{matrix}$$

short

$$\mathbf{A}_u^{\text{red}} := \begin{bmatrix} \vdots \\ \mathbf{w}_0^T \\ \vdots \end{bmatrix} \qquad \mathbf{b}^{\text{red}} := \begin{pmatrix} \vdots \\ \langle \mathbf{w}_2, \mathbf{b} \rangle \\ \vdots \end{pmatrix}$$

Enumerate candidates $\mathbf{s}_u^{(i)}$ for $\mathbf{s}_u$.
Take the one that makes
$\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}} \mathbf{s}_u^{(i)}$ short (mod q).

Dual Attack:

- Split BDD instance $\mathbf{t} = \mathbf{B}_0\mathbf{x}_0 + \mathbf{B}_1\mathbf{x}_1 + \mathbf{y}$
- Compute short vectors $\mathbf{w}' \in \mathscr{L}(\mathbf{B}_0)^*$ ✓
- Enumerate $\mathbf{t}^{(i)} := \mathbf{t} - \mathbf{B}_1\mathbf{x}_1^{(i)}$ ✓
- Apply test to all $\langle \mathbf{t}^{(i)}, \mathbf{w}' \rangle$ ✓

LWE:

- $\mathscr{L}(\mathbf{B}_0)^* \simeq \mathscr{L}(\mathbf{D})$ with first n_u coord. removed
- $\mathbf{b}^{\text{red}} - \mathbf{A}_u^{\text{red}} \mathbf{s}_u^{(i)} \equiv \begin{pmatrix} \vdots \\ \left\langle \mathbf{t}^{(i)}, \begin{pmatrix} \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \right\rangle \\ \vdots \end{pmatrix} \mod q$