Does the Dual-Sieve Attack on LWE even Work?

Léo Ducas\textsuperscript{1,2}, Ludo N. Pulles\textsuperscript{1}

22 August 2023

\textsuperscript{1}Cryptology Group, CWI, Amsterdam, \textsuperscript{2}Mathematical Institute, Leiden University
The security of lattice-based cryptoschemes, like Kyber and Dilithium, depends on the hardness of the Bounded Distance Decoding (BDD) problem.
The security of lattice-based cryptoschemes, like Kyber and Dilithium, depends on the hardness of the Bounded Distance Decoding (BDD) problem.

**BDD**: Given a “noisy” lattice vector, recover the lattice vector.
There are two types of lattice attacks against BDD:

<table>
<thead>
<tr>
<th>Primal attack</th>
<th>Dual attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Embed $\Lambda$ and $t$ into a lattice, where the shortest vector is shorter than expected.</td>
<td>I. Construct a function that distinguishes between BDD targets and uniform targets,</td>
</tr>
<tr>
<td>II. Solve unique-SVP instance by lattice reduction.</td>
<td>II. Using this distinguisher, guess and determine part of the secret.</td>
</tr>
</tbody>
</table>
Lattice attacks against BDD

There are two types of lattice attacks against BDD:

**Primal attack**

I. Embed $\Lambda$ and $t$ into a lattice, where the shortest vector is shorter than expected.

II. Solve unique-SVP instance by lattice reduction.

**Dual attack**

I. Construct a function that distinguishes between BDD targets and uniform targets.

II. Using this distinguisher, guess and determine part of the secret.

Shortest vector problem (SVP)
There are two types of lattice attacks against BDD:

**Primal attack**

1. Embed $\Lambda$ and $t$ into a lattice, where the shortest vector is shorter than expected.
2. Solve unique-SVP instance by lattice reduction.

**Dual attack**

1. Construct a function that distinguishes between BDD targets and uniform targets.
2. Using this distinguisher, guess and determine part of the secret.

**Shortest vector problem (SVP)**
Lattice attacks against BDD

There are two types of lattice attacks against BDD:

**Primal attack**

I. Embed $\Lambda$ and $t$ into a lattice, where the shortest vector is shorter than expected.

II. Solve unique-SVP instance by lattice reduction.

**Dual attack**

I. Construct a function that distinguishes between BDD targets and uniform targets,

II. Using this distinguisher, guess and determine part of the secret.

Theoretically and experimentally well-studied.
There are two types of lattice attacks against BDD:

**Primal attack**

1. Embed $\Lambda$ and $t$ into a lattice, where the shortest vector is shorter than expected.
2. Solve unique-SVP instance by lattice reduction.

Theoretically and experimentally well-studied.

**Dual attack**

1. Construct a function that distinguishes between BDD targets and uniform targets.
2. Using this distinguisher, guess and determine part of the secret.

Received little experimental attention so far.
Recent improvements to the dual attack

**Beginning of the dual attack**

[AR’05]: use short dual vectors for distinguishing.

**Recent developments**

- [ADPS’16]: A lattice sieve yields many short dual vectors. *
- [GJ’21]: Speed up evaluating distinguisher with a Fast Fourier Transform (FFT). *
- [MAT’22]: Improves dual attack with modulus switching technique. *

*: specific to LWE problem.

---

1. Aharonov & Regev. “Lattice problems in $\text{NP} \cap \text{coNP}$”. JACM ’05.
Recent improvements to the dual attack

**Beginning of the dual attack**

[AR’05]¹: use short dual vectors for distinguishing.

**Recent developments**

- [ADPS’16]²: A lattice sieve yields many short dual vectors.*
- [GJ’21]³: Speed up evaluating distinguisher with a Fast Fourier Transform (FFT).*
- [MAT’22]⁴: Improves dual attack with modulus switching technique.*

*: specific to LWE problem.

¹ Aharonov & Regev. “Lattice problems in NP ∩ coNP”. JACM ’05.
Recent improvements to the dual attack

Beginning of the dual attack

[AR’05]¹: use short dual vectors for distinguishing.

Recent developments

– [GJ’21]³: Speed up evaluating distinguisher with a Fast Fourier Transform (FFT).*
– [MAT’22]⁴: Improves dual attack with modulus switching technique.*

*: specific to LWE problem.

¹Aharonov & Regev. “Lattice problems in NP ∩ coNP”. JACM ’05.
Recent improvements to the dual attack

**Beginning of the dual attack**

[AR’05]$^1$: use short dual vectors for distinguishing.

**Recent developments**

- [ADPS’16]$^2$: A lattice sieve yields many short dual vectors.*
- [GJ’21]$^3$: Speed up evaluating distinguisher with a Fast Fourier Transform (FFT).*
- [MAT’22]$^4$: Improves dual attack with modulus switching technique.*

*: specific to LWE problem.

---

1 Aharonov & Regev. “Lattice problems in NP ∩ coNP”. JACM ’05.
Recent improvements to the dual attack

Beginning of the dual attack

[AR’05]: use short dual vectors for distinguishing.

Recent developments

– [ADPS’16]: A lattice sieve yields many short dual vectors.*
– [GJ’21]: Speed up evaluating distinguisher with a Fast Fourier Transform (FFT).*
– [MAT’22]: Improves dual attack with modulus switching technique.*

*: specific to LWE problem.

1 Aharonov & Regev. “Lattice problems in NP ∩ coNP”. JACM ’05.
Our contributions

<table>
<thead>
<tr>
<th>Generalization of FFT trick to BDD</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Provides geometric insight!</td>
</tr>
<tr>
<td>- Allows further improvements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A heuristic used in earlier works leads to two contradictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The distinguisher does not work as well as predicted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Experimental confirmation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derived cryptanalysis overestimates the success probability of attacks.</td>
</tr>
</tbody>
</table>
Our contributions

<table>
<thead>
<tr>
<th>Generalization of FFT trick to BDD</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Provides geometric insight!</td>
</tr>
<tr>
<td>– Allows further improvements.</td>
</tr>
</tbody>
</table>

A heuristic used in earlier works leads to two contradictions

The distinguisher does not work as well as predicted.

Experimental confirmation

Derived cryptanalysis overestimates the success probability of attacks.
## Our contributions

<table>
<thead>
<tr>
<th>Generalization of FFT trick to BDD</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Provides geometric insight!</td>
</tr>
<tr>
<td>– Allows further improvements.</td>
</tr>
</tbody>
</table>

**A heuristic used in earlier works leads to two contradictions**

The distinguisher does not work as well as predicted.

**Experimental confirmation**

Derived cryptanalysis overestimates the success probability of attacks.
Generalization of FFT trick to BDD
Generalization of FFT trick to BDD

$\alpha$-BDD search problem

Given: lattice $\Lambda$ and target $\mathbf{t} \in \mathbb{R}^n$, such that $\mathbf{t} = \mathbf{v} + \mathbf{e}$ with $\mathbf{v} \in \Lambda$ and $\|\mathbf{e}\| \approx \alpha \lambda_1$,

Problem: recover $\mathbf{v}$.

($\lambda_1$ is length of shortest vector)
Generalization of FFT trick to BDD

**α-BDD search problem**

Given: lattice $\Lambda$ and target $t \in \mathbb{R}^n$, such that $t = v + e$ with $v \in \Lambda$ and $\|e\| \approx \alpha \lambda_1$.

Problem: recover $v$.

$(\lambda_1$ is length of shortest vector)

Uniqueness:

- unique
- unique on average
- many solutions

Difficulty:

- easy
- statistically impossible

$Ludo$ Pulles (CWI)
The dual lattice $\Lambda^\lor$ consists of all points $w$ such that $\langle w, \Lambda \rangle \subseteq \mathbb{Z}$.

A dual vector $w$ corresponds to the character $\chi_w$. 
The dual lattice $\Lambda^\vee$ consists of all points $w$ such that $\langle w, \Lambda \rangle \subseteq \mathbb{Z}$.

A dual vector $w$ corresponds to the character $\chi_w$:
Distinguish based on score

Consider the score function:

\[ f_w(t) = \cos(2\pi \langle w, t \rangle), \]

- \( t \in \Lambda \implies \text{score} = 1, \)
- \( t \ close \ to \ \Lambda \ and \ w \ short \implies \text{score} \approx 1, \)
- \( t \ uniform \ from \ torus \ \mathbb{R}^n/\Lambda \implies \text{expected score is} \ 0. \)

⚠️ If score \( \approx 1, \) \( t \) can be uniform!
Consider the score function:

\[ f_w(t) = \cos(2\pi \langle w, t \rangle), \]

- \( t \in \Lambda \implies \text{score} = 1, \)
- \( t \) close to \( \Lambda \) and \( w \) short \( \implies \text{score} \approx 1, \)
- \( t \) uniform from torus \( \mathbb{R}^n/\Lambda \) \( \implies \text{expected score is 0}. \)

⚠️ If score \( \approx 1, t \) can be uniform!
Consider the score function:

$$f_w(t) = \cos(2\pi \langle w, t \rangle),$$

- $t \in \Lambda \implies$ score $= 1$,
- $t$ close to $\Lambda$ and $w$ short $\implies$ score $\approx 1$,
- $t$ uniform from torus $\mathbb{R}^n/\Lambda$ $\implies$ expected score is $0$.

⚠️ If score $\approx 1$, $t$ can be uniform!
Distinguish based on score

Consider the score function:

\[ f_w(t) = \cos(2\pi \langle w, t \rangle), \]

- \( t \in \Lambda \implies \text{score} = 1, \)
- \( t \text{ close to } \Lambda \text{ and } w \text{ short} \implies \text{score} \approx 1, \)
- \( t \text{ uniform from torus } \mathbb{R}^n/\Lambda \implies \text{expected score is 0.} \)

⚠️ If score \( \approx 1, t \) can be uniform!
Consider the score function:

\[ f_w(t) = \cos(2\pi \langle w, t \rangle), \]

- \( t \in \Lambda \Rightarrow \text{score} = 1, \)
- \( t \text{ close to } \Lambda \text{ and } w \text{ short} \Rightarrow \text{score} \approx 1, \)
- \( t \text{ uniform from torus } \mathbb{R}^n/\Lambda \) 
  \( \Rightarrow \text{expected score is 0.} \)

⚠️ If score \( \approx 1, t \) can be uniform!
To improve the distinguisher, we use all \((4/3)^{n/2}\) short dual vectors from a lattice sieve:

\[
f_{\mathcal{W}}(t) = \sum_{w \in \mathcal{W}} f_w(t) = \sum_{w \in \mathcal{W}} \cos\left(2\pi \langle w, t \rangle \right).
\]

Independence Heuristic used in [GJ’21], [MAT’22] and more

Given a set of dual vectors \(\mathcal{W}\) from a sieve, the scores \(\cos(2\pi \langle w, t \rangle)\) are mutually independent.
To improve the distinguisher, we use all \((4/3)^{n/2}\) short dual vectors from a lattice sieve:

\[
f_{\mathcal{W}}(t) = \sum_{w \in \mathcal{W}} f_w(t) = \sum_{w \in \mathcal{W}} \cos\left(2\pi \langle w, t \rangle \right).
\]

**Independence Heuristic used in [GJ’21], [MAT’22] and more**

Given a set of dual vectors \(\mathcal{W}\) from a sieve, the scores \(\cos(2\pi \langle w, t \rangle)\) are mutually independent.
Given a set of dual vectors $\mathcal{W}$ from a sieve, the scores $\cos(2\pi \langle \mathbf{w}, \mathbf{t} \rangle)$ are mutually independent.
Dual-Sieve distinguisher

Independence Heuristic used in [GJ’21], [MAT’22] and more

Given a set of dual vectors $\mathcal{W}$ from a sieve, the scores $\cos(2\pi \langle \mathbf{w}, \mathbf{t} \rangle)$ are mutually independent.

**Diagram:**
- PDF(score)
- Uniform distribution
- Threshold
- BDD distribution

$t$ uniform mod $\Lambda$ \quad $\xrightarrow{\text{w.h.p.}}$ \quad $f_{\mathcal{W}}(t) \approx 0$, $t$ BDD target \quad $\xrightarrow{\text{w.h.p.}}$ \quad $f_{\mathcal{W}}(t)$ large.
Take a sparsified sublattice $\Lambda' \subset \Lambda$,

- Use the distinguisher $f_{\Lambda'}$ for $\Lambda'$,

- For $t = v + e$ and a guess $g \in \Lambda$,

  \[ v \in g + \Lambda' \iff t \text{ close to } g + \Lambda' \]
  \[ \iff t - g \text{ close to } \Lambda' \text{ w.h.p.} \]

  distinguisher marks $t - g$ as BDD.
Search-BDD $\rightarrow$ Decision-BDD

- Take a sparsified sublattice $\Lambda' \subset \Lambda$,
- Use the distinguisher $f_W$ for $\Lambda'$,
- For $t = v + e$ and a guess $g \in \Lambda$,

\[ v \in g + \Lambda' \iff t \text{ close to } g + \Lambda' \]
\[ \iff t - g \text{ close to } \Lambda' \]
\[ \text{w.h.p} \iff \text{distinguisher marks } t - g \text{ as BDD.} \]
Search-BDD $\implies$ Decision-BDD

- Take a sparsified sublattice $\Lambda' \subset \Lambda$,
- Use the distinguisher $f_\mathcal{V}$ for $\Lambda'$,
- For $t = v + e$ and a guess $g \in \Lambda$,

$$v \in g + \Lambda' \iff t \text{ close to } g + \Lambda'$$
$$\iff t - g \text{ close to } \Lambda'$$
\[\text{w.h.p} \iff \text{distinguisher marks } t - g \text{ as BDD.}\]
Dual-Sieve attack

DualAttack(Λ, t):

1. Pick a sublattice Λ′ ⊂ Λ,
2. Run a lattice sieve on (Λ′)∨ to acquire dual vectors W,
3. Write Λ as union of Λ′-cosets:
   \[ Λ = \bigcup_{g} (Λ′ + g) \quad (g ∈ Λ), \]
4. Pick Λ′ + g that maximizes \( f_W(t - g) \).

- We recovered part of the secret: g.
- The new BDD instance is easier.
Dual-Sieve attack

**DualAttack(Λ, t):**

1. Pick a sublattice Λ' ⊂ Λ,
2. Run a lattice sieve on $(Λ')^\vee$ to acquire dual vectors $\mathcal{W}$,
3. Write Λ as union of Λ'-cosets:
   \[ Λ = \bigcup_{g} (Λ' + g) \quad (g ∈ Λ), \]
4. Pick Λ' + g that maximizes $f_\mathcal{W}(t - g)$.

- We recovered part of the secret: g.
- The new BDD instance is easier.
Dual-Sieve attack

**DualAttack(\(\Lambda, t\)):**

1. Pick a sublattice \(\Lambda' \subset \Lambda\),
2. Run a lattice sieve on \((\Lambda')^\vee\) to acquire dual vectors \(W\),
3. Write \(\Lambda\) as union of \(\Lambda'\)-cosets:
   \[
   \Lambda = \bigcup_{g}(\Lambda' + g) \quad (g \in \Lambda),
   \]
4. Pick \(\Lambda' + g\) that maximizes \(f_W(t - g)\).

- We recovered part of the secret: \(g\).
- The new BDD instance is easier.

Ludo Pulles (CWI)
Dual-Sieve attack

\textbf{DualAttack}(\Lambda, \mathbf{t}):\n
1. Pick a sublattice \( \Lambda' \subset \Lambda \),
2. Run a lattice sieve on \((\Lambda')^\vee\) to acquire dual vectors \( W \),
3. Write \( \Lambda \) as union of \( \Lambda' \)-cosets:
   \[ \Lambda = \bigcup_{g \in \Lambda} (\Lambda' + g), \]
4. Pick \( \Lambda' + g \) that maximizes \( \mathcal{f}_W(\mathbf{t} - g) \).

- We recovered part of the secret: \( g \).
- The new BDD instance is easier.
**Dual-Sieve attack**

**DualAttack(Λ, t):**

1. Pick a sublattice Λ′ ⊂ Λ,
2. Run a lattice sieve on (Λ′)∨ to acquire dual vectors \(W\),
3. Write Λ as union of Λ′-cosets:
   \[
   Λ = \bigcup_{g}(Λ′ + g) \quad (g \in Λ),
   \]
4. Pick Λ′ + g that maximizes \(f_W(t - g)\).

– We recovered part of the secret: \(g\).
– The new BDD instance is easier.
General Dual-Sieve-FFT attack

Naïvely, computing $f_{\mathcal{W}}(t - g)$, takes time $|\mathcal{W}|$ per guess.

**Fast Fourier Transform**

Computes scores for $T$ many guesses in amortized time $\log_2(T)$ per guess!

**Benefits of geometric insights**

- Attack works for any lattice $\Lambda$ and sparsification $\Lambda'$, not only $q$-ary lattices.
- Flexibility in sparsification $\Longrightarrow$ better attack.
General Dual-Sieve-FFT attack

Naïvely, computing $f_{W}(t - g)$, takes time $|W|$ per guess.

**Fast Fourier Transform**

Computes scores for $T$ many guesses in amortized time $\log_2(T)$ per guess!

**Benefits of geometric insights**

- Attack works for any lattice $\Lambda$ and sparsification $\Lambda'$, not only $q$-ary lattices.
- Flexibility in sparsification $\implies$ better attack.
General Dual-Sieve-FFT attack

Naïvely, computing $f_W(t - g)$, takes time $|\mathcal{W}|$ per guess.

**Fast Fourier Transform**

Computes scores for $T$ many guesses in amortized time $\log_2(T)$ per guess!

**Benefits of geometric insights**

- Attack works for any lattice $\Lambda$ and sparsification $\Lambda'$, not only $q$-ary lattices.
- Flexibility in sparsification $\implies$ better attack.
General Dual-Sieve-FFT attack

Naïvely, computing $f_W(t - g)$, takes time $|\mathcal{W}|$ per guess.

**Fast Fourier Transform**

Computes scores for $T$ many guesses in amortized time $\log_2(T)$ per guess!

**Benefits of geometric insights**

- Attack works for any lattice $\Lambda$ and sparsification $\Lambda'$, not only $q$-ary lattices.
- Flexibility in sparsification $\implies$ better attack.
Independence Heuristic leads to two contradictions
For any $\alpha > 0$, take $\beta > 1$ satisfying

$$\frac{\beta^2}{\ln(\beta)} = \frac{e^2}{\alpha^2}.$$ 

Given the shortest $\beta^n$ dual vectors, $f_{\mathcal{W}}(t)$ distinguishes between a uniform and a $\alpha$-BDD target with success probability 99%.

---


6 Recall: $t = v + e$ such that $v \in \Lambda$ and $\|e\| \approx \alpha \lambda_1$. 

Ludo Pulles (CWI)
For any \( \alpha > 0 \), take \( \beta > 1 \) satisfying
\[
\frac{\beta^2}{\ln(\beta)} = \frac{e^2}{\alpha^2}.
\]
Given the shortest \( \beta^n \) dual vectors, \( f_W(t) \) distinguishes between a uniform and a \( \alpha \)-BDD target\(^6\) with success probability 99%.

---


\(^6\)Recall: \( t = v + e \) such that \( v \in \Lambda \) and \( ||e|| \approx \alpha \lambda_1 \).
For any $\alpha > 0$, take $\beta > 1$ satisfying
\[
\frac{\beta^2}{\ln(\beta)} = \frac{e^2}{\alpha^2}.
\]

Given the shortest $\beta^n$ dual vectors, $f_W(t)$ distinguishes between a uniform and a $\alpha$-BDD target with success probability 99%.

---


6Recall: $t = v + e$ such that $v \in \Lambda$ and $\|e\| \approx \alpha \lambda_1$. 
Indistinguishability Theorem ("Smoothing bound")

[DDRT'22]⁷: In a random lattice, errors uniform from the ball of radius \( \alpha \lambda_1 \) become statistically indistinguishable from uniform errors in \( \mathbb{R}^n/\Lambda \) when \( \alpha > 1 \).

In particular, no adversary (having unbounded runtime) can ever succeed distinguishing with probability more than \( \frac{1}{2} + \alpha^{-n/2} \).

⁷Debris-Alazard, Ducas, Resch & Tillich. "Smoothing codes and lattices: Systematic Study and New Bounds".
Indistinguishability Theorem ("Smoothing bound")

[DDRT’22]⁷: In a random lattice, errors uniform from the ball of radius $\alpha \lambda_1$ become statistically indistinguishable from uniform errors in $\mathbb{R}^n/\Lambda$ when $\alpha > 1$.

In particular, no adversary (having unbounded runtime) can ever succeed distinguishing with probability more than $\frac{1}{2} + \alpha^{-n/2}$.

⁷Debris-Alazard, Ducas, Resch & Tillich. “Smoothing codes and lattices: Systematic Study and New Bounds”.
Distinguishing $\alpha$-BDD among many uniforms

**Given:** $T$ random uniform targets and a single $\alpha$-BDD target, shuffled.

**Return:** the BDD target.

Recall from Dual-Sieve attack ([GJ'21], [MAT'22] & more):

4. Pick $\Lambda' + g$ that maximizes $f_{\Lambda}(t - g)$.

**Limit on $T$**

**Question:** What is biggest $T$ for which Dual-Sieve attack works with 99% probability?
Distinguishing $\alpha$-BDD among many uniforms

**Given:** $T$ random uniform targets and a single $\alpha$-BDD target, shuffled.

**Return:** the BDD target.

Recall from Dual-Sieve attack ([GJ’21], [MAT’22] & more):

4. Pick $N' + g$ that maximizes $f_W(t - g)$.

**Limit on $T$**

**Question:** What is biggest $T$ for which Dual-Sieve attack works with 99% probability?
Given: $T$ random uniform targets and a single $\alpha$-BDD target, shuffled.

Return: the BDD target.

Recall from Dual-Sieve attack ([GJ’21], [MAT’22] & more):

4. Pick $\Lambda' + g$ that maximizes $f_W(t - g)$.

Limit on $T$

Question: What is biggest $T$ for which Dual-Sieve attack works with 99% probability?
Distinguishing failures

Failure $\implies$ a) $\alpha$-BDD target has low score, or
b) any of the $T$ uniform targets has high score.

Claim [GJ’21], [MAT’22] under Independence Heuristic:

Classic tail bound: $p \leq e^{-E^2_\alpha/|W|}$.

For $\alpha < 0.89$: $E^2_\alpha/|W| \sim e^{Cn}$, as $n \to \infty$.

$\implies$ Dual-Sieve attack works for $T = \frac{1}{p} = e^{Cn}?!$
Distinguishing failures

Failure \(\Rightarrow\) a) \(\alpha\)-BDD target has low score, or 
b) any of the \(T\) uniform targets has high score.

Claim [GJ’21], [MAT’22] under Independence Heuristic:

Classic tail bound: \(p \leq e^{-E_\alpha^2/|\mathcal{W}|}\).

For \(\alpha < 0.89\): \(E_\alpha^2/|\mathcal{W}| \sim e^{Cn}\), as \(n \to \infty\).

\(\Rightarrow\) Dual-Sieve attack works for \(T = \frac{1}{p} = e^{e^{Cn}}\) ?!
Distinguishing failures

Failure \implies a) \(\alpha\)-BDD target has low score, or
b) any of the \(T\) uniform targets has high score.

Claim [GJ’21], [MAT’22] under Independence Heuristic:

Classic tail bound: \(p \leq e^{-E^2_\alpha/|W|}\).

For \(\alpha < 0.89\): \(E^2_\alpha/|W| \sim e^{Cn}\), as \(n \to \infty\).

\(\implies\) Dual-Sieve attack works for \(T = \frac{1}{p} = e^{e^{Cn}}\) ?!
Distinguishing failures

Failure $\Rightarrow$ a) $\alpha$-BDD target has low score, or
b) any of the $T$ uniform targets has high score.

Claim [GJ’21], [MAT’22] under Independence Heuristic:

Classic tail bound: $p \leq e^{-E_\alpha^2/|\mathcal{W}|}$.

For $\alpha < 0.89$: $E_\alpha^2/|\mathcal{W}| \sim e^{Cn}$, as $n \to \infty$.

$\Rightarrow$ Dual-Sieve attack works for $T = \frac{1}{p} = e^{Cn}$?!

\[ E_\alpha = E[f_W(t)] \]

\[ \log_2 P[f_W(t) \geq x] \text{ for } t \sim \text{uniform}, \]
\[ \log_2 P[f_W(t) < x] \text{ for } t \sim \text{BDD}. \]
Distinguishing failures

Failure \iff

a) $\alpha$-BDD target has low score, or
b) any of the $T$ uniform targets has high score.

Claim [GJ’21], [MAT’22] under Independence Heuristic:

Classic tail bound: $p \leq e^{-E^2/|W|}$.

For $\alpha < 0.89$: $E^2_{\alpha}/|W| \sim e^{Cn}$, as $n \to \infty$.

$\implies$ Dual-Sieve attack works for $T = \frac{1}{p} = e^{Cn}$ ?!
Closeness Lemma

Given a random lattice $\Lambda$ and $r < \frac{1}{2}$, a uniform target

$$t \xleftarrow{\$} \mathbb{R}^n / \Lambda,$$

is at most $r\lambda_1$ away from a lattice point with probability $r^n$.  

Geometric contradiction

- Given $T \gg \alpha^{-n}$ uniform targets, there is one of them closer to $\Lambda$ than the $\alpha$-BDD target.
- This target has a higher score than the $\alpha$-BDD target!
**Closeness Lemma**

Given a random lattice $\Lambda$ and $r < \frac{1}{2}$, a uniform target

$$ t \leftarrow \mathbb{R}^n / \Lambda,$$

is at most $r\lambda_1$ away from a lattice point with probability $r^n$.

**Geometric contradiction**

- Given $T \gg \alpha^{-n}$ uniform targets, there is one of them closer to $\Lambda$ than the $\alpha$-BDD target.
- This target has a higher score than the $\alpha$-BDD target!
Closeness Lemma

Given a random lattice $\Lambda$ and $r < \frac{1}{2}$, a uniform target

$$t \xleftarrow{\$} \mathbb{R}^n / \Lambda,$$

is at most $r\lambda_1$ away from a lattice point with probability $r^n$.

Geometric contradiction

- Given $T \gg \alpha^{-n}$ uniform targets, there is one of them closer to $\Lambda$ than the $\alpha$-BDD target.
- This target has a higher score than the $\alpha$-BDD target!
What could be the cause?

Independence Heuristic:

“The scores \( \cos(2\pi \langle \mathbf{w}, \mathbf{t} \rangle) \) for \( \mathbf{w} \in \mathcal{W} \) are independent.”
Independence Heuristic:

“The scores $(\cos(2\pi \langle w, t \rangle))_{w \in \mathcal{W}}$ are independent.”
What could be the cause?

Independence Heuristic:

“The scores \( \cos(2\pi \langle w, t \rangle) \) for all \( w \in \mathcal{W} \) are independent.”

Ludo Pulles (CWI)
Experimental confirmation
Independence Heuristic overestimates success probability of attack.
Scores from uniform targets

Independence Heuristic overestimates success probability of attack.
Independence Heuristic overestimates success probability of attack.
Scores from uniform targets

Independence Heuristic overestimates success probability of attack.

**A Study of Error Floor Behavior in QC-MDPC Codes**

Sarah Apple1, Tyre Evans-Baignaire1, Darae Hwang2, Min Yo-Lan3, Luke T. Peterson1, and
Angela Antunes4

1 University of Colorado Boulder, Department of Mathematics
2 W. O. Colton Professor of Mathematics, Statistics, and Computer Science
3 Indiana University, Department of Mathematics & Statistics
4 University of California San Diego, Department of Mathematics
5 National Institute of Standards and Technology, Computer Security Division

Abstract. We present experimental findings and a theoretical analysis of the variance floor (VF) in QC-MDPC codes. To this end, we consider a number of QC-MDPC codes and compare their performance against a baseline of random linear codes. Our results show that the variance floor is not significantly higher than the floor of random linear codes, and that the variance floor is not significantly lower than the floor of random linear codes. We also show that the variance floor is not significantly different from the floor of random linear codes.

Keywords. QC-MDPC, variance floor, VR, QC-MDPC

Fig. 1. Distribution of uniform targets in dimension 60

Experiment

Prediction Independence

Heuristic

Log$_2$ $P[f_W(t) \geq \text{score}]$

Score distribution of uniform targets in dimension 60

Score distribution of uniform targets in dimension 80
Scores from BDD targets

Score distribution of 0.7-BDD targets in dimension 80

- Variance is much higher than predicted.
- Median is lower than predicted.

Again, Independence Heuristic overestimates success probability of attack.
Scores from BDD targets

Even prediction of BDD scores is off

- Variance is much higher than predicted.
- Median is lower than predicted.

Again, Independence Heuristic overestimates success probability of attack.
Aftermath
What is the impact?

Dual-Sieve analyses are invalidated

- Success probability of the Dual-Sieve attack is significantly overestimated.
- Hardness of BDD with respect to the Dual-Sieve attack is currently unknown.
What is the impact?

**Dual-Sieve analyses are invalidated**

- Success probability of the Dual-Sieve attack is significantly overestimated.
- Hardness of BDD with respect to the Dual-Sieve attack is currently unknown.
What is next?

**Ongoing research**

- Describing the score distribution of BDD targets using Bessel functions.
- New prediction for uniform targets that predicts “waterfall-floor phenomenon”.

A heuristic has to be *stress-tested* on small instances before being used in cryptographic attacks!
What is next?

Ongoing research

- Describing the score distribution of BDD targets using Bessel functions.
- New prediction for uniform targets that predicts “waterfall-floor phenomenon”.

A heuristic has to be stress-tested on small instances before being used in cryptographic attacks!
What is next?

**Ongoing research**

- Describing the score distribution of BDD targets using Bessel functions.
- New prediction for uniform targets that predicts “waterfall-floor phenomenon”.

A heuristic has to be *stress-tested* on small instances before being used in cryptographic attacks!
Thank you!

Questions?

**ePrint:**  https://ia.cr/2023/302

**code & data:**  https://github.com/ludopulles/DoesDualSieveWork

_Ludo Pulles (CWI)_