Improved Hardness of BDD and SVP under Gap-(S)ETH

Huck Bennett, Chris Peikert, Yi Tang

ITCS 2022
Preliminaries: Lattices

Lattice: regular grid of points in space. Formally, lattice $\mathcal{L}$ of rank $n$: set of all integer linear combinations of a basis $B = (b_1, \ldots, b_n)$. 
Preliminaries: Lattice-Based Cryptography

**Problem:** Attacker with quantum computation can break number theoretical cryptography.

**Solution:** Use lattice-based cryptography!

**Fact:** State-of-the-art attacks are based on solving exact or low-approximation-factor lattice problems (e.g. SVP).

**Problem:** Whether attacker can solve these problems in $2^n$ vs. $2^{n/10}$ vs. $2^{\sqrt{n}}$ time has a huge impact on security.

**Our work:** Address this by showing *fine-grained* hardness results for lattice problems.
Preliminaries: Lattice-Based Cryptography

**Problem**: Attacker with quantum computation can break number theoretical cryptography.

**Solution**: Use lattice-based cryptography!

**Fact**: State-of-the-art attacks are based on solving exact or low-approximation-factor lattice problems (e.g. SVP).

**Problem**: Whether attacker can solve these problems in $2^n$ vs. $2^{n/10}$ vs. $2^{\sqrt{n}}$ time has a huge impact on security.

**Our work**: Address this by showing *fine-grained* hardness results for lattice problems.
Preliminaries: Lattice-Based Cryptography

**Problem:** Attacker with quantum computation can break number theoretical cryptography.

**Solution:** Use lattice-based cryptography!

**Fact:** State-of-the-art attacks are based on solving exact or low-approximation-factor lattice problems (e.g. SVP).

**Problem:** Whether attacker can solve these problems in $2^n$ vs. $2^{n/10}$ vs. $2^{\sqrt{n}}$ time has a huge impact on security.

**Our work:** Address this by showing *fine-grained* hardness results for lattice problems.
Preliminaries: Lattice-Based Cryptography

**Problem:** Attacker with quantum computation can break number theoretical cryptography.

**Solution:** Use lattice-based cryptography!

**Fact:** State-of-the-art attacks are based on solving exact or low-approximation-factor lattice problems (e.g. $SVP$).

**Problem:** Whether attacker can solve these problems in $2^n$ vs. $2^{n/10}$ vs. $2^{\sqrt{n}}$ time has a huge impact on security.

**Our work:** Address this by showing fine-grained hardness results for lattice problems.
Preliminaries: Lattice-Based Cryptography

**Problem**: Attacker with quantum computation can break number theoretical cryptography.

**Solution**: Use lattice-based cryptography!

**Fact**: State-of-the-art attacks are based on solving exact or low-approximation-factor lattice problems (e.g. SVP).

**Problem**: Whether attacker can solve these problems in $2^n$ vs. $2^{n/10}$ vs. $2^{\sqrt{n}}$ time has a huge impact on security.

**Our work**: Address this by showing *fine-grained* hardness results for lattice problems.
Preliminaries: Shortest Vector Problem (SVP)

Shortest $\ell_p$ norm of nonzero vector in lattice $\mathcal{L}$: $\lambda_1^{(p)}(\mathcal{L})$.

$\gamma$-approximate SVP in $\ell_p$ (SVP$_{p,\gamma}$)

Instance: Basis $B$ of lattice $\mathcal{L}$.
Goal: Decide whether $\lambda_1^{(p)}(\mathcal{L}) \leq 1$ or $\lambda_1^{(p)}(\mathcal{L}) > \gamma$. 
Preliminaries: Shortest Vector Problem (SVP)

Shortest $\ell_p$ norm of nonzero vector in lattice $\mathcal{L}$: $\lambda_1^{(p)}(\mathcal{L})$.

$\gamma$-approximate SVP in $\ell_p$ ($\text{SVP}_{p,\gamma}$)

**Instance:** Basis $B$ of lattice $\mathcal{L}$.

**Goal:** Decide whether $\lambda_1^{(p)}(\mathcal{L}) \leq 1$ or $\lambda_1^{(p)}(\mathcal{L}) > \gamma$. 
Preliminaries: Bounded Distance Decoding (BDD)

BDD in $\ell_p$ with relative distance $\alpha$ ($\text{BDD}_{p,\alpha}$)

**Instance:** Lattice $\mathcal{L}$ and target $\mathbf{t}$ with $\text{dist}_p(\mathbf{t}, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$.

**Goal:** Find closest lattice vector to $\mathbf{t}$ in $\mathcal{L}$.

Smaller $\alpha$ corresponds to stronger promise and easier problem.

($p = 2$, $\alpha = 0.6$)
Preliminaries: Bounded Distance Decoding (BDD)

BDD in $\ell_p$ with relative distance $\alpha$ ($\text{BDD}_{p,\alpha}$)

**Instance:** Lattice $\mathcal{L}$ and target $t$ with $\text{dist}_p(t, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$.

**Goal:** Find closest lattice vector to $t$ in $\mathcal{L}$.

Smaller $\alpha$ corresponds to stronger promise and easier problem.

($p = 2$, $\alpha = 0.6$)
Preliminaries: Exponential Time Hypothesis (ETH)

ETH variants:
- ETH: 3-SAT cannot be solved in $2^{o(n)}$ time.
- Strong ETH (SETH): $k$-SAT cannot be solved in $2^{(1-\varepsilon)n}$ time.
- Gap-(S)ETH: Gap-3-SAT$_{1-\delta,1}$ & Gap-$k$-SAT$_{1-\delta(k),1}$.
- Randomized/non-uniform variants.

Our work exploits the power of different ETH variants, showing stronger hardness results for BDD/SVP under stronger variants.

We reduce SAT on $n$ variables to lattice problems in rank $C \cdot n$ for constant $C > 0$ to show fine-grained hardness results.

Line of research in fine-grained hardness of lattice problems: CVP [BGS17, ABGS21], SVP [AS18], BDD [BP20], SIVP [AC20].
Preliminaries: Exponential Time Hypothesis (ETH)

ETH variants:

- ETH: 3-SAT cannot be solved in $2^{o(n)}$ time.
- Strong ETH (SETH): $k$-SAT cannot be solved in $2^{(1-\varepsilon)n}$ time.
- Gap-(S)ETH: Gap-3-SAT$_{1-\delta,1}$ & Gap-$k$-SAT$_{1-\delta(k),1}$.
- Randomized/non-uniform variants.

Our work exploits the power of different ETH variants, showing stronger hardness results for BDD/SVP under stronger variants.

We reduce SAT on $n$ variables to lattice problems in rank $C \cdot n$ for constant $C > 0$ to show fine-grained hardness results.

Line of research in fine-grained hardness of lattice problems: CVP [BGS17, ABGS21], SVP [AS18], BDD [BP20], SIVP [AC20].
Preliminaries: Exponential Time Hypothesis (ETH)

ETH variants:
- ETH: 3-SAT cannot be solved in \(2^{o(n)}\) time.
- Strong ETH (SETH): \(k\)-SAT cannot be solved in \(2^{(1-\varepsilon)n}\) time.
- Gap-(S)ETH: \(\text{Gap-}3\text{-SAT}_{1-\delta,1} \& \text{Gap-}k\text{-SAT}_{1-\delta(k),1}\).
- Randomized/non-uniform variants.

Our work exploits the power of different ETH variants, showing stronger hardness results for BDD/SVP under stronger variants.

We reduce SAT on \(n\) variables to lattice problems in rank \(C \cdot n\) for constant \(C > 0\) to show fine-grained hardness results.

Line of research in fine-grained hardness of lattice problems: CVP [BGS17, ABGS21], SVP [AS18], BDD [BP20], SIVP [AC20].
Preliminaries: Exponential Time Hypothesis (ETH)

ETH variants:
- ETH: 3-SAT cannot be solved in $2^{o(n)}$ time.
- Strong ETH (SETH): $k$-SAT cannot be solved in $2^{(1-\epsilon)n}$ time.
- Gap-(S)ETH: Gap-$3$-$\text{SAT}_{1-\delta,1}$ & Gap-$k$-$\text{SAT}_{1-\delta(k),1}$.
- Randomized/non-uniform variants.

Our work exploits the power of different ETH variants, showing stronger hardness results for BDD/SVP under stronger variants.

We reduce SAT on $n$ variables to lattice problems in rank $C \cdot n$ for constant $C > 0$ to show fine-grained hardness results.

Line of research in fine-grained hardness of lattice problems: $CVP$ [BGS17, ABGS21], $SVP$ [AS18], $BDD$ [BP20], $SIVP$ [AC20].
Preliminaries: Exponential Time Hypothesis (ETH)

ETH variants:

- ETH: 3-SAT cannot be solved in $2^{o(n)}$ time.
- Strong ETH (SETH): $k$-SAT cannot be solved in $2^{(1-\varepsilon)n}$ time.
- Gap-(S)ETH: Gap-3-SAT$_{1-\delta,1}$ & Gap-$k$-SAT$_{1-\delta(k),1}$.
- Randomized/non-uniform variants.

Our work exploits the power of different ETH variants, showing stronger hardness results for BDD/SVP under stronger variants.

We reduce SAT on $n$ variables to lattice problems in rank $C \cdot n$ for constant $C > 0$ to show fine-grained hardness results.

Line of research in fine-grained hardness of lattice problems: CVP [BGS17, ABGS21], SVP [AS18], BDD [BP20], SIVP [AC20].
Preliminaries: Exponential Time Hypothesis (ETH)

ETH variants:
- ETH: 3-SAT cannot be solved in $2^{o(n)}$ time.
- Strong ETH (SETH): $k$-SAT cannot be solved in $2^{(1-\varepsilon)n}$ time.
- Gap-(S)ETH: $\text{Gap-3-SAT}_{1-\delta,1}$ & $\text{Gap-k-SAT}_{1-\delta(k),1}$.
- Randomized/non-uniform variants.

Our work exploits the power of different ETH variants, showing stronger hardness results for BDD/SVP under stronger variants.

We reduce SAT on $n$ variables to lattice problems in rank $C \cdot n$ for constant $C > 0$ to show fine-grained hardness results.

Line of research in fine-grained hardness of lattice problems: $\text{CVP}$ [BGS17, ABGS21], $\text{SVP}$ [AS18], $\text{BDD}$ [BP20], $\text{SIVP}$ [AC20].
Our Results: ETH-Type Hardness of BDD

1. \( \text{BDD}_{p,\alpha} \) cannot be solved in \( 2^{o(n)} \) time for any \( p \in [1, \infty) \) and \( \alpha > \alpha_{kn} \approx 0.98491 \), under non-uniform Gap-ETH.

2. \( \text{BDD}_{p,\alpha} \) cannot be solved in \( 2^{o(n)} \) time for any \( p \in [1, \infty) \) and \( \alpha > \alpha^{\dagger}_{p} \), under randomized Gap-ETH.

<table>
<thead>
<tr>
<th>( p )</th>
<th>( \alpha )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.95</td>
<td>Result 1</td>
</tr>
<tr>
<td>1.00</td>
<td>Result 2</td>
</tr>
<tr>
<td>1.05</td>
<td>[BP20]</td>
</tr>
</tbody>
</table>

\[ \begin{aligned} \alpha &> \alpha_{kn} \\ \alpha &> \alpha^{\dagger}_{p} \end{aligned} \]
Our Results: ETH-Type Hardness of BDD

1. $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_{kn} \approx 0.98491$, under non-uniform Gap-ETH.

2. $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for any $p \in [1, \infty)$ and $\alpha > \alpha_{p}^{\dagger}$, under randomized Gap-ETH.
Our Results: SETH-Type Hardness of BDD

3. \( \text{BDD}_{p,\alpha} \) cannot be solved in \( 2^{n/C} \) time for any \( p \in [1, \infty) \), \( p \notin 2\mathbb{Z} \), \( C > 1 \), and \( \alpha > \alpha^\dagger_{p,C} \), under non-uniform Gap-SETH.

\[
egin{array}{c|c|c|c}
\alpha & 1.5 & 2.0 & 2.5 & 3.0 \\
\hline
p & 1.0 & 1.2 & 1.4 & 1.6 & 1.8 & 2.0 & 2.2
\end{array}
\]

Graph showing the relationship between \( \alpha \) and \( p \) for different values of \( C \) and the relation between [BP20] and Result 3.
Our Results: SETH-Type Hardness of SVP

4. For any $p > p_0 \approx 2.1397$, $p \not\in 2\mathbb{Z}$ and $C > C_p$, $\text{SVP}_{p,\gamma}$ cannot be solved in $2^{n/C}$ time for some constant $\gamma > 1$, under randomized Gap-SETH. ($C_p \to 1$ for $p \to \infty$.)
Our Results: SETH-Type Hardness of SVP

4. For any $p > p_0 \approx 2.1397$, $p \notin 2\mathbb{Z}$ and $C > C_p$, SVP$_{p,\gamma}$ cannot be solved in $2^{n/C}$ time for some constant $\gamma > 1$, under randomized Gap-SETH. ($C_p \to 1$ for $p \to \infty$.)
Core Proof Technique: Locally Dense Gadgets

Locally dense gadget \((\mathcal{L}^\dagger, t^\dagger)\) in rank \(n\):

- "Short" count: \(N_{\text{short}}\) lattice vectors of length less than 1.
- "Close" count: \(N_{\text{close}}\) lattice vectors of distance \(\alpha_{\text{close}}\) to \(t^\dagger\).
- \(\mathcal{L}^\dagger\) is locally dense at \(t^\dagger\) if \(N_{\text{close}} \geq \nu^n \cdot N_{\text{short}}\), i.e., exponentially more "close" than "short" lattice vectors.
- Quality parameters: \(\alpha_{\text{close}}\) and \(\nu\).

\[(n = 2, \mathcal{L}^\dagger = \mathbb{Z}^2, t^\dagger = (\frac{1}{2}, \frac{1}{2}), \alpha_{\text{close}} = \frac{\sqrt{2}}{2}, \nu^n = 4)\]
Core Proof Technique: Locally Dense Gadgets

Locally dense gadget \((\mathcal{L}^\dagger, t^\dagger)\) in rank \(n\):

- “Short” count: \(N_{\text{short}}\) lattice vectors of length less than 1.
- “Close” count: \(N_{\text{close}}\) lattice vectors of distance \(\alpha_{\text{close}}\) to \(t^\dagger\).
- \(\mathcal{L}^\dagger\) is locally dense at \(t^\dagger\) if \(N_{\text{close}} \geq \nu^n \cdot N_{\text{short}}\), i.e., exponentially more “close” than “short” lattice vectors.

- Quality parameters: \(\alpha_{\text{close}}\) and \(\nu\).

\[ (n = 2, \mathcal{L}^\dagger = \mathbb{Z}^2, t^\dagger = (\frac{1}{2}, \frac{1}{2}), \alpha_{\text{close}} = \frac{\sqrt{2}}{2}, \nu^n = 4) \]
Core Proof Technique: Locally Dense Gadgets

Locally dense gadget \((\mathcal{L}^\dagger, \mathbf{t}^\dagger)\) in rank \(n\):

- "Short" count: \(N_{\text{short}}\) lattice vectors of length less than 1.
- "Close" count: \(N_{\text{close}}\) lattice vectors of distance \(\alpha_{\text{close}}\) to \(\mathbf{t}^\dagger\).
- \(\mathcal{L}^\dagger\) is locally dense at \(\mathbf{t}^\dagger\) if \(N_{\text{close}} \geq \nu^n \cdot N_{\text{short}}\), i.e., exponentially more "close" than "short" lattice vectors.
- Quality parameters: \(\alpha_{\text{close}}\) and \(\nu\).

\((n = 2, \mathcal{L}^\dagger = \mathbb{Z}^2, \mathbf{t}^\dagger = (\frac{1}{2}, \frac{1}{2}), \alpha_{\text{close}} = \frac{\sqrt{2}}{2}, \nu^n = 4)\)
Main Theorem for BDD

Main theorem for BDD, informal & simplified

If there exist locally dense gadgets \((L^\dagger, t^\dagger)\) with parameters \(\alpha_{\text{close}}\) and \(\nu\), then for BDD_{p,\alpha}:

- it cannot be solved in \(2^{o(n)}\) time for any \(\alpha > \alpha_{\text{close}}\), under Gap-ETH variants;
- it cannot be solved in \(2^{n/C}\) time for any

\[
\alpha > \alpha_{\text{close}} + \varepsilon_p(\nu^{C-1})
\]

under Gap-SETH variants.\(^1\)

---

\(^1\)The function \(\varepsilon_p(\cdot)\) is strictly decreasing, and \(\varepsilon_p(x) \to 0\) as \(x \to \infty\).
Main Theorem for BDD

Main theorem for BDD, informal & simplified

If there exist locally dense gadgets \((L^\dagger, t^\dagger)\) with parameters \(\alpha_{\text{close}}\) and \(\nu\), then for \(BDD_{p,\alpha}\):

- it cannot be solved in \(2^{o(n)}\) time for any \(\alpha > \alpha_{\text{close}}\), under Gap-ETH variants;
- it cannot be solved in \(2^{n/C}\) time for any

\[
\alpha > \alpha_{\text{close}} + \varepsilon_p(\nu^{C-1})
\]

under Gap-SETH variants.\(^1\)

\(^1\)The function \(\varepsilon_p(\cdot)\) is strictly decreasing, and \(\varepsilon_p(x) \to 0\) as \(x \to \infty\).
Main theorem for BDD, informal & simplified

If there exist locally dense gadgets \((\mathcal{L}^\dagger, t^\dagger)\) with parameters \(\alpha_{\text{close}}\) and \(\nu\), then for BDD\(_p,\alpha\):

- it cannot be solved in \(2^{o(n)}\) time for any \(\alpha > \alpha_{\text{close}}\), under Gap-ETH variants;
- it cannot be solved in \(2^{n/C}\) time for any
  \[
  \alpha > \alpha_{\text{close}} + \varepsilon_p(\nu^{C-1}) ,
  \]
  under Gap-SETH variants.\(^1\)

\(^1\)The function \(\varepsilon_p(\cdot)\) is strictly decreasing, and \(\varepsilon_p(x) \to 0\) as \(x \to \infty\).
[Vlă19]: There exist lattices $\mathcal{L}^\dagger$ with exponential kissing number: $2^{c_{kn}n-o(n)}$ vectors of length $\lambda_1(\mathcal{L}^\dagger) = 1$, where $c_{kn} \geq 0.02194$.

Gadgets from kissing number:

- **Gadgets**: exponential kissing number lattice $\mathcal{L}^\dagger$ with $t^\dagger = 0$.
- **Parameters**: $\alpha_{\text{close}} = 1$, $\nu = 2^{c_{kn}}$.

Gadgets from integer lattices: $\mathcal{L}^\dagger = \mathbb{Z}^n$, $t^\dagger = t \cdot 1_n$. 
[Vlă19]: There exist lattices $\mathcal{L}^\dagger$ with exponential kissing number: $2^{c_{kn}n-o(n)}$ vectors of length $\lambda_1(\mathcal{L}^\dagger) = 1$, where $c_{kn} \geq 0.02194$.

Gadgets from kissing number:

- **Gadgets**: exponential kissing number lattice $\mathcal{L}^\dagger$ with $t^\dagger = 0$.
- **Parameters**: $\alpha_{\text{close}} = 1$, $\nu = 2^{c_{kn}}$.

Gadgets from integer lattices: $\mathcal{L}^\dagger = \mathbb{Z}^n$, $t^\dagger = t \cdot 1_n$. 
[Vlă19]: There exist lattices \( \mathcal{L}^\dagger \) with exponential kissing number: 
\( 2^{c_{kn}n-o(n)} \) vectors of length \( \lambda_1(\mathcal{L}^\dagger) = 1 \), where \( c_{kn} \geq 0.02194. \)

Gadgets from kissing number:

- **Gadgets**: exponential kissing number lattice \( \mathcal{L}^\dagger \) with \( t^\dagger = 0 \).
- **Parameters**: \( \alpha_{\text{close}} = 1, \nu = 2^{c_{kn}} \).

Gadgets from integer lattices: \( \mathcal{L}^\dagger = \mathbb{Z}^n, t^\dagger = t \cdot 1_n. \)
Instantiating the Main Theorem

Result 1: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{kn}$
  - Try to decrease $\alpha_{\text{close}}$ for kissing number gadgets, by perturbing $t^\dagger$ away from 0 while keeping $\nu > 1$.
  - Get $\alpha_{\text{close}}$ approaching $\alpha_{kn} := 2^{-c_{kn}}$.

Result 2: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_p^\dagger$
  - Use gadgets from integer lattices.
  - Minimize $\alpha_{\text{close}}$ subject to $\nu > 1$, where $\alpha_p^\dagger$ is the optimum.

Result 3: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for all $\alpha > \alpha_{p,C}^\dagger$
  - Use kissing number gadgets: $\alpha_{\text{close}} = 1$, $\nu = 2^{c_{kn}}$.
  - Get $\alpha_{p,C}^\dagger := 1 + \epsilon_p(2^{c_{kn}(C-1)})$ by main theorem.

Result 4: $\text{SVP}_{p,\gamma}$ cannot be solved in $2^{n/C}$ time for all $C > C_p$
  - Similar theorem for SVP based on locally dense gadgets.
  - Use the same gadgets from integer lattices as Result 2.
Instantiating the Main Theorem

Result 1: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{kn}$

- Try to decrease $\alpha_{\text{close}}$ for kissing number gadgets, by perturbing $t^\dagger$ away from $0$ while keeping $\nu > 1$.
- Get $\alpha_{\text{close}}$ approaching $\alpha_{kn} := 2^{-c_{kn}}$.

Result 2: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{p}^\dagger$

- Use gadgets from integer lattices.
- Minimize $\alpha_{\text{close}}$ subject to $\nu > 1$, where $\alpha_{p}^\dagger$ is the optimum.

Result 3: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for all $\alpha > \alpha_{p,C}^\dagger$

- Use kissing number gadgets: $\alpha_{\text{close}} = 1$, $\nu = 2^{c_{kn}}$.
- Get $\alpha_{p,C}^\dagger := 1 + \varepsilon_p(2^{c_{kn}(C-1)})$ by main theorem.

Result 4: $\text{SVP}_{p,\gamma}$ cannot be solved in $2^{n/C}$ time for all $C > C_p$

- Similar theorem for SVP based on locally dense gadgets.
- Use the same gadgets from integer lattices as Result 2.
Instantiating the Main Theorem

Result 1: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{kn}$

- Try to decrease $\alpha_{\text{close}}$ for kissing number gadgets, by perturbing $t^\dagger$ away from 0 while keeping $\nu > 1$.
- Get $\alpha_{\text{close}}$ approaching $\alpha_{kn} := 2^{-c_{kn}}$.

Result 2: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_p^{\dagger}$

- Use gadgets from integer lattices.
- Minimize $\alpha_{\text{close}}$ subject to $\nu > 1$, where $\alpha_p^{\dagger}$ is the optimum.

Result 3: $\text{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for all $\alpha > \alpha_{p, C}^{\dagger}$

- Use kissing number gadgets: $\alpha_{\text{close}} = 1$, $\nu = 2^{c_{kn}}$.
- Get $\alpha_{p, C}^{\dagger} := 1 + \varepsilon_p(2^{c_{kn}(C-1)})$ by main theorem.

Result 4: $\text{SVP}_{p,\gamma}$ cannot be solved in $2^{n/C}$ time for all $C > C_p$

- Similar theorem for SVP based on locally dense gadgets.
- Use the same gadgets from integer lattices as Result 2.
Instantiating the Main Theorem

Result 1: \(\text{BDD}_{p,\alpha}\) cannot be solved in \(2^{o(n)}\) time for all \(\alpha > \alpha_{kn}\)

- Try to decrease \(\alpha_{close}\) for kissing number gadgets, by perturbing \(t^\dagger\) away from \(\mathbf{0}\) while keeping \(\nu > 1\).
- Get \(\alpha_{close}\) approaching \(\alpha_{kn} := 2^{-c_{kn}}\).

Result 2: \(\text{BDD}_{p,\alpha}\) cannot be solved in \(2^{o(n)}\) time for all \(\alpha > \alpha_{p}^\dagger\)

- Use gadgets from integer lattices.
- Minimize \(\alpha_{close}\) subject to \(\nu > 1\), where \(\alpha_{p}^\dagger\) is the optimum.

Result 3: \(\text{BDD}_{p,\alpha}\) cannot be solved in \(2^{n/C}\) time for all \(\alpha > \alpha_{p,C}^\dagger\)

- Use kissing number gadgets: \(\alpha_{close} = 1, \nu = 2^{c_{kn}}\).
- Get \(\alpha_{p,C}^\dagger := 1 + \varepsilon_p(2^{c_{kn}(C-1)})\) by main theorem.

Result 4: \(\text{SVP}_{p,\gamma}\) cannot be solved in \(2^{n/C}\) time for all \(C > C_p\)

- Similar theorem for \(\text{SVP}\) based on locally dense gadgets.
- Use the same gadgets from integer lattices as Result 2.
Open Questions

- Derandomize the reductions?
  - Randomness is used in gadgets and in main theorem.

- Construct locally “denser” gadgets?
  - E.g. better bound on kissing number immediately leads to better quantities in Result 1 and 3 ($\alpha_{kn}$ and $\alpha_{p,C}^\dagger$).
Divesh Aggarwal, Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz.
Fine-grained hardness of CVP(P)—everything that we can prove (and nothing else).

Divesh Aggarwal and Eldon Chung.

Divesh Aggarwal, Zeyong Li, and Noah Stephens-Davidowitz.
A $2^{n/2}$-time algorithm for $\sqrt{n}$-SVP and $\sqrt{n}$-Hermite SVP, and an improved time-approximation tradeoff for (H)SVP.

Divesh Aggarwal and Noah Stephens-Davidowitz.
(Gap/S)ETH hardness of SVP.
In STOC, pages 228–238, 2018.

Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz.
On the quantitative hardness of CVP.

Huck Bennett and Chris Peikert.
Hardness of bounded distance decoding on lattices in $\ell_p$ norms.

Friedrich Eisenbrand and Moritz Venzin.
Approximate $\text{CVP}_p$ in time $2^{0.802n}$.

Subhash Khot.
Hardness of approximating the shortest vector problem in lattices.

Factoring polynomials with rational coefficients.

Serge Vlăduț.
Lattices with exponentially large kissing numbers.