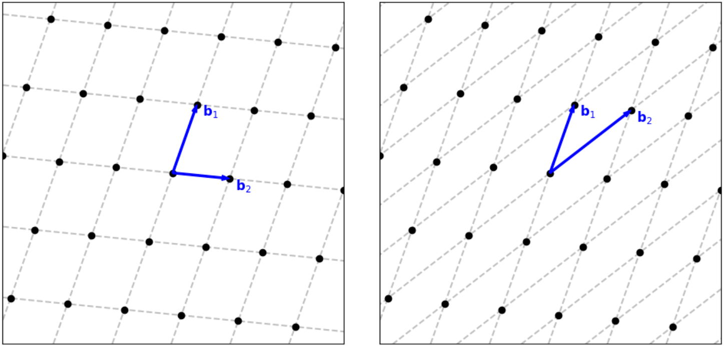
# Improved Hardness of BDD and SVP under Gap-(S)ETH

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 $\boldsymbol{B} = (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$.



# 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

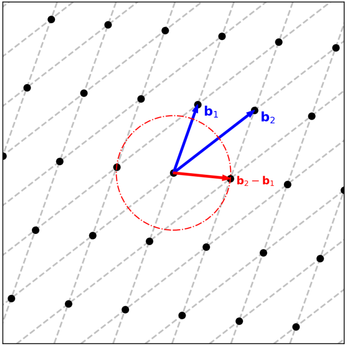
**Problem**: Attacker with quantum computation can break number theoretical cryptography.
**Solution**: Use lattice-based cryptography!

**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 $\mathcal{L}$: $\lambda_1^{(p)}(\mathcal{L})$.

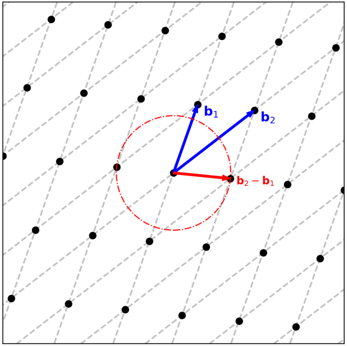



$\gamma$-approximate SVP in $\ell_p$ ($\mathrm{SVP}_{p,\gamma}$)

**Instance**: Basis $\boldsymbol{B}$ 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 $\ell_p$ ($\mathrm{SVP}_{p,\gamma}$)

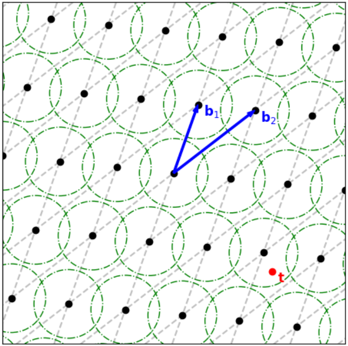
**Instance**: Basis $\boldsymbol{B}$ of lattice $\mathcal{L}$.
**Goal**: Decide whether $\lambda_1^{(p)}(\mathcal{L}) \leq 1$ or $\lambda_1^{(p)}(\mathcal{L}) > \gamma$.

# Preliminaries: Bounded Distance Decoding (BDD)

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

**Instance**: Lattice $\mathcal{L}$ and target $\boldsymbol{t}$ with $\mathrm{dist}_p(\boldsymbol{t}, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$.
**Goal**: Find closest lattice vector to $\boldsymbol{t}$ in $\mathcal{L}$.

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



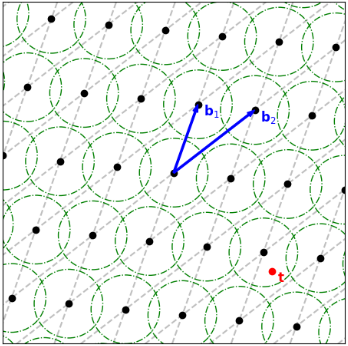

$(p = 2, \alpha = 0.6)$

# Preliminaries: Bounded Distance Decoding (BDD)

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

**Instance**: Lattice $\mathcal{L}$ and target $\boldsymbol{t}$ with $\mathrm{dist}_p(\boldsymbol{t}, \mathcal{L}) \leq \alpha \cdot \lambda_1^{(p)}(\mathcal{L})$.
**Goal**: Find closest lattice vector to $\boldsymbol{t}$ 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-$\mathrm{SAT}$ cannot be solved in $2^{o(n)}$ time.
- Strong ETH (SETH): $k$-$\mathrm{SAT}$ cannot be solved in $2^{(1-\varepsilon)n}$ time.
- Gap-(S)ETH: $\mathrm{Gap\text{-}3\text{-}SAT}_{1-\delta,1}$ & $\mathrm{Gap}\text{-}k\text{-}\mathrm{SAT}_{1-\delta(k),1}$.
- Randomized/non-uniform variants.

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

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

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

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

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

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

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

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

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

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

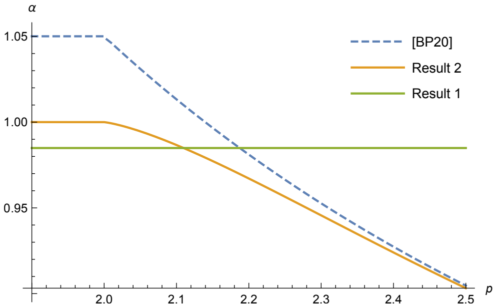
Our work exploits the power of different ETH variants, showing stronger hardness results for $\mathrm{BDD}/\mathrm{SVP}$ under stronger variants.

We reduce $\mathrm{SAT}$ 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].

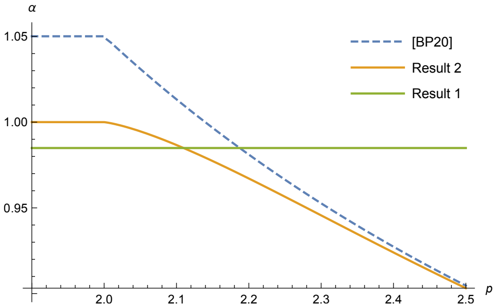
# Our Results: ETH-Type Hardness of BDD

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



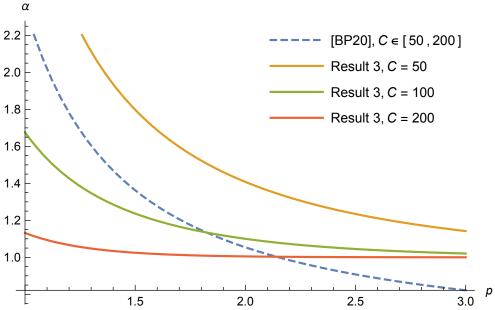
# Our Results: ETH-Type Hardness of $\mathrm{BDD}$

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



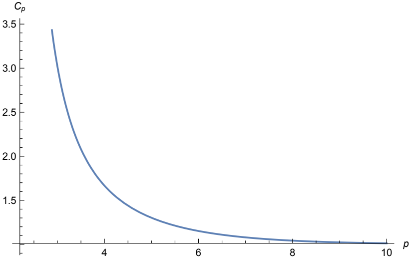
# Our Results: SETH-Type Hardness of $\mathrm{BDD}$

3. $\mathrm{BDD}_{p,\alpha}$ 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.



# Our Results: SETH-Type Hardness of $\mathrm{SVP}$

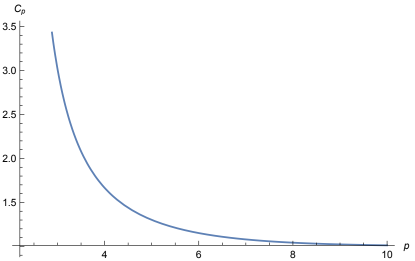
4. For any $p > p_0 \approx 2.1397$, $p \notin 2\mathbb{Z}$ and $C > C_p$, $\mathrm{SVP}_{p,\gamma}$ cannot be solved in $2^{n/C}$ time for some constant $\gamma > 1$, under randomized Gap-SETH. ($C_p \to 1$ for $p \to \infty$.)




| $2^{n/C_p}$-hard | $2^{n/C_p}$-hard | NP-hard | $2^{0.802n}$ alg | (for $p = 2$) $2^{n/(2+f(c))}$ alg | easy | |
|---|---|---|---|---|---|---|
| 1, exact | $1+\varepsilon$ | any const | large const | $n^{1/2+c}$ | $\exp(n)$ | $\gamma$ |
| [AS18] | **[this work]** | [Kho05] | [EV20] | [ALSD21] | [LLL82] | |

# Our Results: SETH-Type Hardness of SVP

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

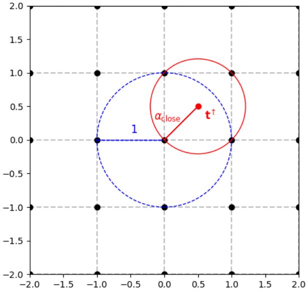



| | | | | (for $p = 2$) | | |
|---|---|---|---|---|---|---|
| | $2^{n/C_p}$-hard | $2^{n/C_p}$-hard | NP-hard | $2^{0.802n}$ alg | $2^{n/(2+f(c))}$ alg | easy |
| $\gamma$ | 1, exact | $1+\varepsilon$ | any const | large const | $n^{1/2+c}$ | $\exp(n)$ |
| | [AS18] | **[this work]** | [Kho05] | [EV20] | [ALSD21] | [LLL82] |

# Core Proof Technique: Locally Dense Gadgets

Locally dense gadget $(\mathcal{L}^\dagger, \boldsymbol{t}^\dagger)$ 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 $\boldsymbol{t}^\dagger$.
- $\mathcal{L}^\dagger$ is *locally dense* at $\boldsymbol{t}^\dagger$ 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 $\nu$.

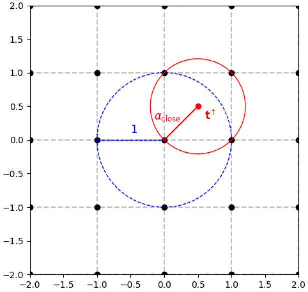



$(n = 2,\ \mathcal{L}^\dagger = \mathbb{Z}^2,\ \boldsymbol{t}^\dagger = (\frac{1}{2}, \frac{1}{2}),\ \alpha_{\text{close}} = \frac{\sqrt{2}}{2},\ \nu^n = 4)$

# Core Proof Technique: Locally Dense Gadgets

Locally dense gadget $(\mathcal{L}^\dagger, \boldsymbol{t}^\dagger)$ 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 $\boldsymbol{t}^\dagger$.
- $\mathcal{L}^\dagger$ is *locally dense* at $\boldsymbol{t}^\dagger$ 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 $\nu$.

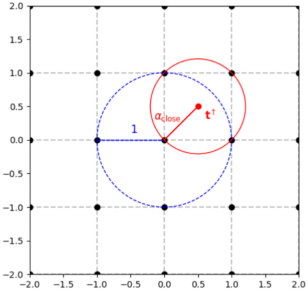



$(n = 2,\ \mathcal{L}^\dagger = \mathbb{Z}^2,\ \boldsymbol{t}^\dagger = (\frac{1}{2}, \frac{1}{2}),\ \alpha_{\text{close}} = \frac{\sqrt{2}}{2},\ \nu^n = 4)$

# Core Proof Technique: Locally Dense Gadgets

Locally dense gadget $(\mathcal{L}^\dagger, \boldsymbol{t}^\dagger)$ 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 $\boldsymbol{t}^\dagger$.
- $\mathcal{L}^\dagger$ is *locally dense* at $\boldsymbol{t}^\dagger$ 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 $\nu$.




$(n = 2,\ \mathcal{L}^\dagger = \mathbb{Z}^2,\ \boldsymbol{t}^\dagger = (\frac{1}{2}, \frac{1}{2}),\ \alpha_{\text{close}} = \frac{\sqrt{2}}{2},\ \nu^n = 4)$

# Main Theorem for $\mathrm{BDD}$

## Main theorem for $\mathrm{BDD}$, informal & simplified

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

- 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 $\mathrm{BDD}$

## Main theorem for $\mathrm{BDD}$, informal & simplified

If there exist locally dense gadgets $(\mathcal{L}^\dagger, \boldsymbol{t}^\dagger)$ with parameters $\alpha_{\mathsf{close}}$ and $\nu$, then for $\mathrm{BDD}_{p,\alpha}$:

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

$$\alpha > \alpha_{\mathsf{close}} + \varepsilon_p(\nu^{C-1}) \ ,$$

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 $\mathrm{BDD}$

## Main theorem for $\mathrm{BDD}$, informal & simplified

If there exist locally dense gadgets $(\mathcal{L}^\dagger, \boldsymbol{t}^\dagger)$ with parameters $\alpha_{\mathsf{close}}$ and $\nu$, then for $\mathrm{BDD}_{p,\alpha}$:

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

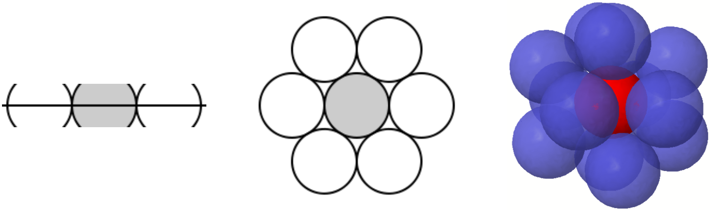
$$\alpha > \alpha_{\mathsf{close}} + \varepsilon_p(\nu^{C-1}) \; ,$$

under Gap-SETH variants.[1]

[1] The function $\varepsilon_p(\cdot)$ is strictly decreasing, and $\varepsilon_p(x) \to 0$ as $x \to \infty$.

# Gadgets We Use

[Vlă19]: There exist lattices $\mathcal{L}^\dagger$ with *exponential kissing number*: $2^{c_{\mathsf{kn}} n - o(n)}$ vectors of length $\lambda_1(\mathcal{L}^\dagger) = 1$, where $c_{\mathsf{kn}} \geq 0.02194$.



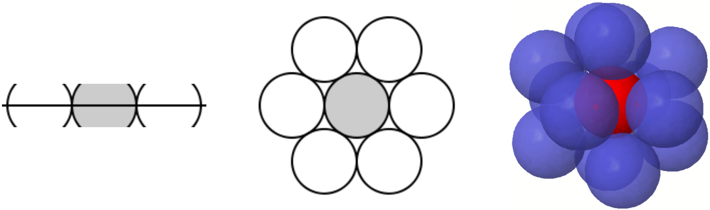
Gadgets from kissing number:

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

Gadgets from integer lattices: $\mathcal{L}^\dagger = \mathbb{Z}^n$, $\boldsymbol{t}^\dagger = t \cdot \mathbf{1}_n$.

# Gadgets We Use

[Vlă19]: There exist lattices $\mathcal{L}^\dagger$ with *exponential kissing number*: $2^{c_{\mathsf{kn}} n - o(n)}$ vectors of length $\lambda_1(\mathcal{L}^\dagger) = 1$, where $c_{\mathsf{kn}} \geq 0.02194$.



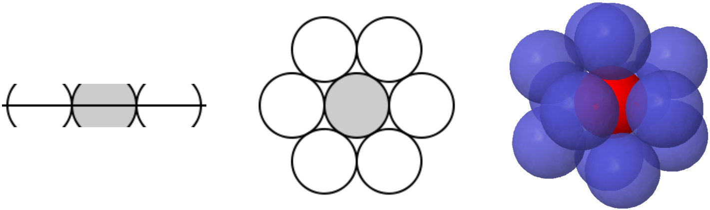
Gadgets from kissing number:

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

Gadgets from integer lattices: $\mathcal{L}^\dagger = \mathbb{Z}^n$, $\boldsymbol{t}^\dagger = t \cdot \mathbf{1}_n$.

# Gadgets We Use

[Vlă19]: There exist lattices $\mathcal{L}^\dagger$ with *exponential kissing number*: $2^{c_{\mathrm{kn}} n - o(n)}$ vectors of length $\lambda_1(\mathcal{L}^\dagger) = 1$, where $c_{\mathrm{kn}} \geq 0.02194$.



Gadgets from kissing number:

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

Gadgets from integer lattices: $\mathcal{L}^\dagger = \mathbb{Z}^n$, $\boldsymbol{t}^\dagger = t \cdot \mathbf{1}_n$.

# Instantiating the Main Theorem

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

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

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

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

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

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

Result 4: $\mathrm{SVP}_{p,\gamma}$ 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: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{\mathsf{kn}}$

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

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

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

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

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

Result 4: $\mathrm{SVP}_{p,\gamma}$ 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: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{\mathsf{kn}}$

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

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

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

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

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

Result 4: $\mathrm{SVP}_{p,\gamma}$ 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: $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{o(n)}$ time for all $\alpha > \alpha_{\mathsf{kn}}$

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

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

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

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

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

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

- Similar theorem for $\mathrm{SVP}$ 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 ($\alpha_{\mathsf{kn}}$ and $\alpha^{\dagger}_{p,C}$).

# References


Divesh Aggarwal, Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz.
Fine-grained hardness of CVP(P)—everything that we can prove (and nothing else).
In *SODA*, pages 1816–1835, 2021.

Divesh Aggarwal and Eldon Chung.
A note on the concrete hardness of the shortest independent vectors problem in lattices, 2020.

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.
In *EUROCRYPT*, pages 467–497. 2021.

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.
In *FOCS*, pages 13–24. 2017.

Huck Bennett and Chris Peikert.
Hardness of bounded distance decoding on lattices in $\ell_p$ norms.
In *CCC*, pages Art. 36, 21. 2020.

Friedrich Eisenbrand and Moritz Venzin.
Approximate $\mathrm{CVP}_p$ in time $2^{0.802n}$.
In *ESA*, pages Art. No. 43, 15. 2020.

Subhash Khot.
Hardness of approximating the shortest vector problem in lattices.
*J. ACM*, 52(5):789–808, 2005.

A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász.
Factoring polynomials with rational coefficients.
*Math. Ann.*, 261(4):515–534, 1982.

Serge Vlăduț.
Lattices with exponentially large kissing numbers.
*Mosc. J. Comb. Number Theory*, 8(2):163–177, 2019.