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

Yi Tang @ U-M CSE Prospective Student Visit Days 2022

Joint work with Huck Bennett and Chris Peikert, ITCS 2022

Motivation: Post-Quantum Cryptography

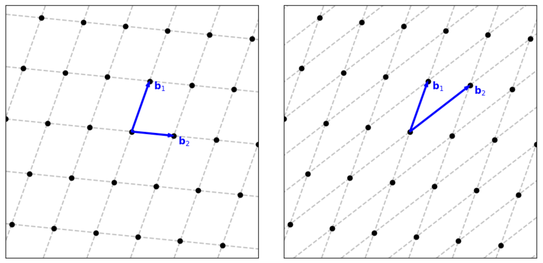
Problem: Attacker with quantum computation can break number theoretical cryptography that are widely used, such as RSA.
Solution: Use *lattice-based* cryptography!

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

Problem: Can attacker solve these problems in 2^n vs. $2^{n/10}$ vs. $2^{\sqrt{n}}$ time? It has a huge impact on security.
Our work: Address this by showing *fine-grained* hardness results for lattice problems, under variants of *ETH*.

Lattices

Lattice: regular grid of points in space.
Formally, lattice $\mathcal{L}$ of rank n: set of all *integer* linear combinations of a basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

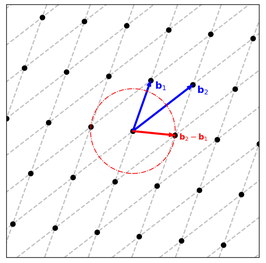


References

- 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 ℓ_p norms. In *CCC*, pages Art. 36, 21. 2020.
- Friedrich Eisenbrand and Moritz Venzin. Approximate 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.

Lattice Problems: Shortest Vector Problem (SVP)

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



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

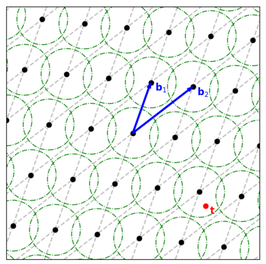
Instance: Basis $\mathbf{B}$ of lattice $\mathcal{L}$.
Goal: Decide whether $\lambda_1^{(p)}(\mathcal{L}) \le 1$ or $\lambda_1^{(p)}(\mathcal{L}) > \gamma$.

Lattice Problems: Bounded Distance Decoding (BDD)

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

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

Smaller α corresponds to stronger promise and easier problem.



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

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-$\mathrm{SAT}_{1-\delta,1}$ & Gap-k-$\mathrm{SAT}_{1-\delta(k),1}$.
- Randomized/non-uniform variants: randomized/non-uniform time.

Assumption strength:

- ETH $\le$ SETH;
- plain $\le$ gap;
- plain $\le$ randomized $\le$ non-uniform.

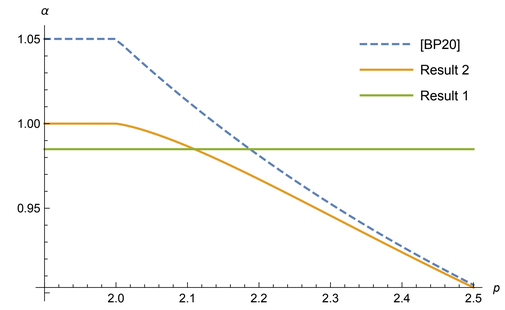
Our work exploits the power of different ETH variants, showing stronger hardness results for $\mathrm{BDD}/\mathrm{SVP}$ under stronger variants.

More specifically, 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].

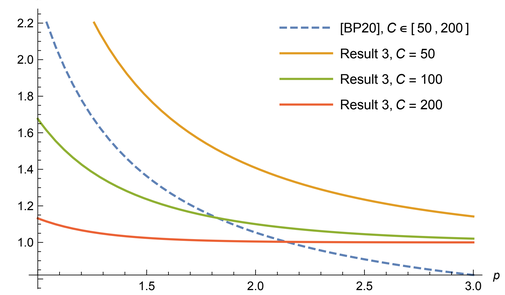
Our Results: ETH-Type Hardness of BDD

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.



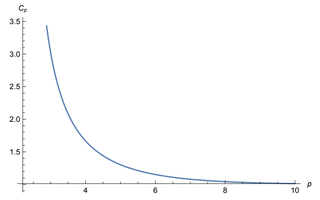
Our Results: SETH-Type Hardness of BDD

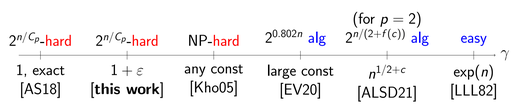
3. $\mathrm{BDD}_{p,\alpha}$ cannot be solved in $2^{n/C}$ time for any $p \in [1, \infty)$, $p \notin 2\mathbb{Z}$, $C > 1$, and $\alpha > \alpha_{p,C}^{\dagger}$, under non-uniform Gap-SETH.



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 $p \to \infty$.)

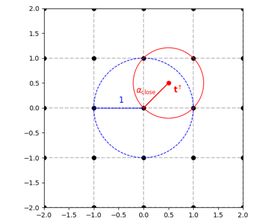




Core Proof Technique: Locally Dense Gadgets

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

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



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

Main Theorem for BDD

Main theorem for BDD, informal & simplified

If there exist locally dense gadgets with parameters α_{close} and ν, then $\mathrm{BDD}_{p,\alpha}$:

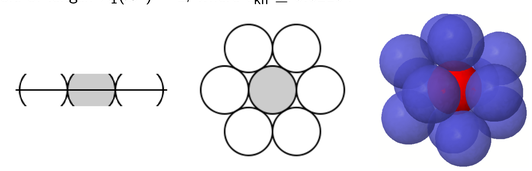
- cannot be solved in $2^{o(n)}$ time for any $\alpha > \alpha_{\mathsf{close}}$, under Gap-ETH variants;
- cannot be solved in $2^{n/C}$ time for any

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

under Gap-SETH variants.

Instantiating the Main Theorem

[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 $c_{\mathsf{kn}} \ge 0.02194$.



Result 1 and 3: Use gadgets from kissing number:

- **Gadgets**: exponential kissing number lattice $\mathcal{L}^{\dagger}$ with $\mathbf{t}^{\dagger} = \mathbf{0}$.
- **Parameters**: $\alpha_{\mathsf{close}} = 1$, $\nu = 2^{c_{\mathsf{kn}}}$.
- Result 3: Immediately get $\alpha_{p,C}^{\dagger} := 1 + \varepsilon_p(2^{c_{\mathsf{kn}}(C-1)})$ by main theorem.
- Result 1: Get $\alpha_{\mathsf{kn}} := 2^{-c_{\mathsf{kn}}}$ by perturbing $\mathbf{t}^{\dagger}$ away from $\mathbf{0}$.

Result 2 and 4: Use gadgets from integer lattices:

- **Gadgets**: $\mathcal{L}^{\dagger} = \mathbb{Z}^n$, $\mathbf{t}^{\dagger} = t \cdot \mathbf{1}_n$.
- Result 2: Minimize α_{close} subject to $\nu > 1$, and get $\alpha_p^{\ddagger}$ as the optimum.
- Result 4: Similar theorem for SVP based on gadgets, and same gadgets.

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 (α_{kn} and $\alpha_{p,C}^{\dagger}$).