# Implementing Approximate Voronoi Cells for Solving CVP in Lattices with Low Dimensions

CS564 - Computational Geometry

Barış Gülek - 22504017

March 4, 2026

Lattice-based cryptography has its security based on a computationally hard problem called "closest vector problem". The closest vector problem is, given a lattice $\mathcal{L}$ and a target point $t$, find a point $v \in \mathcal{L}$, that is the closest point to $t$. This project focuses on implementing *approximate Voronoi cells* [1] [2] to solve the CVP within lower dimensions.

The implementation will be based on papers on lattice cryptanalysis and they will be cited in the final report. By comparing exact and approximate Voronoi cells, it can be seen that even though both are hard to compute, the latter one is much easier in both time and space. The exact variant takes $\mathcal{O}(2^{2d})$ time and $\mathcal{O}(2^d)$ space [3] whereas the approximate variant takes about $\mathcal{O}(2^{td})$ time and $\mathcal{O}(2^{sd})$ space where $t, s < 1$ [1]. While both approaches become impractical to compute in higher dimensions, the approximate variants provide a wider range for the computable dimensions.

## References

[1] E. Doulgerakis, T. Laarhoven, and B. de Weger. "Finding Closest Lattice Vectors Using Approximate Voronoi Cells". In: *Post-Quantum Cryptography (PQCrypto 2019)*. Ed. by J. Ding and R. Steinwandt. Vol. 11505. Lecture Notes in Computer Science. Cham: Springer, 2019. DOI: 10.1007/978-3-030-25510-7_1. URL: https://doi.org/10.1007/978-3-030-25510-7_1.

[2] Thijs Laarhoven. "Approximate Voronoi cells for lattices, revisited". In: *Journal of Mathematical Cryptology* 15.1 (2021), pp. 60–71. DOI: 10.1515/jmc-2020-0074. URL: https://doi.org/10.1515/jmc-2020-0074.

[3] Daniele Micciancio and Panagiotis Voulgaris. "A Deterministic Single Exponential Time Algorithm for Most Lattice Problems Based on Voronoi Cell Computations". In: *SIAM Journal on Computing* 42.3 (2013), pp. 1364–1391. DOI: 10.1137/100811970. eprint: https://doi.org/10.1137/100811970. URL: https://doi.org/10.1137/100811970.