

# Huck Bennett

---

School of Electrical Engineering and Computer Science  
Oregon State University

Email: [huck.bennett@oregonstate.edu](mailto:huck.bennett@oregonstate.edu)

Website: <https://web.engr.oregonstate.edu/~bennethu/>

## RESEARCH INTERESTS

Theoretical computer science, with an emphasis on lattices and geometric algorithms.

## ACADEMIC POSITIONS

**University of Colorado** – Boulder, CO Spring 2024 – Present  
**Assistant Professor of Computer Science**

**Oregon State University** – Corvallis, OR Fall 2021 – Fall 2023  
**Assistant Professor of Electrical Engineering and Computer Science**

**University of Michigan** – Ann Arbor, MI Fall 2019 – Summer 2021  
**Adjunct/Visiting Assistant Research Scientist (Postdoc)**  
Mentor: Chris Peikert.

**Northwestern University** – Evanston, IL Fall 2017 – Summer 2019  
**Postdoctoral Fellow**  
Research mentors: Anindya De and Aravindan Vijayaraghavan.

## EDUCATION

**Courant Institute of Mathematical Sciences,  
New York University** Fall 2012 – Summer 2017

- Ph.D. in Computer Science.
- Advisors: Daniel Dadush (CWI, Amsterdam) and Chee Yap (NYU).

**University of Colorado – Boulder** Fall 2010 – Spring 2012

- M.S. in Computer Science.
- Advisor: Sriram Sankaranarayanan.

**University of Wisconsin – Madison** Fall 2006 – Spring 2010

- B.S. in Mathematics, certificate (minor) in Computer Science.

## PUBLICATIONS Peer-Reviewed Conference Papers:

- [C1] Willow Barkan-Vered, Huck Bennett, and Amir Nayyeri. *Topological  $k$ -metrics*. International Symposium on Computational Geometry (SOCG) 2024.
- [C2] Huck Bennett and Chris Peikert. *Hardness of the (Approximate) Shortest Vector Problem: A Simple Proof via Reed-Solomon Codes*. International Conference on Randomization and Computation (RANDOM) 2023.
- [C3] Huck Bennett, Mahdi Cheraghchi, Venkat Guruswami, and João Ribeiro. *Parameterized Inapproximability of the Minimum Distance Problem over all Fields and the Shortest Vector Problem in all  $\ell_p$  Norms*. Symposium on Theory of Computing (STOC) 2023.
- [C4] Divesh Aggarwal, Huck Bennett, Zvika Brakerski, Alexander Golovnev, Rajendra Kumar, Zeyong Li, Spencer Peters, Noah Stephens-Davidowitz, and Vinod Vaikuntanathan. *Lattice Problems Beyond Polynomial Time*. Symposium on Theory of Computing (STOC) 2023.

- [C5] Huck Bennett, Atul Ganju, Pura Peetathawatchai, and Noah Stephens-Davidowitz. *Just how hard are rotations of  $\mathbb{Z}^n$ ? Algorithms and cryptography with the simplest lattice*. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2023.
- [C6] Huck Bennett, Chris Peikert, and Yi Tang. *Improved Hardness of BDD and SVP Under Gap-(S)ETH*. Innovations in Theoretical Computer Science (ITCS) 2022.
- [C7] Huck Bennett, Anindya De, Rocco Servedio, and Emmanouil V. Vlatakis-Gkaragkounis. *Reconstructing Weighted Voting Schemes from Partial Information about their Power Indices*. Conference on Learning Theory (COLT) 2021.
- [C8] Divesh Aggarwal, Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. *Fine-grained hardness of CVP(P)— Everything that we can prove (and nothing else)*. Symposium on Discrete Algorithms (SODA) 2021.
- [C9] Huck Bennett and Chris Peikert. *Hardness of Bounded Distance Decoding on Lattices in  $\ell_p$  Norms*. Computational Complexity Conference (CCC) 2020.
- [C10] Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. *On the Quantitative Hardness of CVP*. Foundations of Computer Science (FOCS) 2017.
- [C11] Huck Bennett, Daniel Dadush, and Noah Stephens-Davidowitz. *On the Lattice Distortion Problem*. European Symposium on Algorithms (ESA) 2016, Track A.
- [C12] Huck Bennett, Evanthia Papadopoulou, and Chee Yap. *Planar Minimization Diagrams via Subdivision with Applications to Anisotropic Voronoi Diagrams*. Eurographics Symposium on Geometry Processing (SGP) 2016.
- [C13] Huck Bennett, Daniel Reichman, and Igor Shinkar. *On Percolation and NP-hardness*. International Colloquium on Automata, Languages, and Programming (ICALP) 2016, Track A. Preliminary version of [J2].
- [C14] Huck Bennett and Chee Yap. *Amortized Analysis of Smooth Quadrees in All Dimensions*. Scandinavian Symposium and Workshops on Algorithm Theory (SWAT) 2014. Preliminary version of [J3].

**Peer-Reviewed Journal Papers and Surveys:**

- [J1] Huck Bennett. *The Complexity of the Shortest Vector Problem*. ACM SIGACT News 54 (1), pp. 37-61, 2023.
- [J2] Huck Bennett, Daniel Reichman, and Igor Shinkar. *On Percolation and NP-hardness*. Random Structures & Algorithms 54 (2), pp. 228-257, 2019.
- [J3] Huck Bennett and Chee Yap. *Amortized Analysis of Smooth Quadrees in All Dimensions*. Computational Geometry: Theory and Applications 63, pp. 20-39, 2017.

**Preprints:**

- [P1] Huck Bennett, Surendra Ghentiyala, and Noah Stephens-Davidowitz. *The more the merrier! On the complexity of finding multicollisions, with connections to codes and lattices*. Preprint, 2024.
- [P2] Huck Bennett, Karthik Gajulapalli, Alexander Golovnev, and Philip G. Warton. *Matrix Multiplication Verification Using Coding Theory*. Preprint, 2023.
- [P3] Huck Bennett. *An Enumeration Technique for Lattice Basis Reduction*. Preprint, 2019.

**Other:**

- [O1] Huck Bennett. *AlphaGo and Artificial Intelligence*. Blog post, March 2016. <https://hdbennett.wordpress.com/2016/03/18/alphago-and-artificial-intelligence/>.
- [O2] Huck Bennett, Evanthia Papadopoulou, and Chee Yap. *A Subdivision Approach to Weighted Voronoi Diagrams*. Fall Workshop on Computational Geometry (FWCG) 2014. Preliminary version of [C12].
- [O3] Huck Bennett and Chee Yap. *Amortized Analysis of Balanced Quadrees*. Fall Workshop on Computational Geometry (FWCG) 2013. Preliminary version of [C14].
- [O4] Huxley Bennett and Sriram Sankaranarayanan. *Model Counting Using the Inclusion-Exclusion Principle*. Short paper and poster. Theory and Applications of Satisfiability Testing (SAT) 2011.

**TEACHING****As Lead Instructor:**

- Honors Analysis of Algorithms. Oregon State University, Winter 2023.
- Analysis of Algorithms. Oregon State University, Fall 2021, Winter 2023, Fall 2023.
- Foundations of Computer Science. University of Michigan, Fall 2019 (joint with Chris Peikert and Ilya Volkovich).
- Lattices in Computer Science. Northwestern University, Spring 2019; Oregon State University, Spring 2022; University of Colorado, Spring 2024.
- Mathematical Foundations of Computer Science. Northwestern University, Winter 2018, Spring 2018, Fall 2018.
- Computational Geometry. Northwestern University, Fall 2017, Winter 2019.

**As Teaching Assistant:**

- Programming Languages (master's level), New York University, Summer 2015.
- Programming Languages (junior level), University of Colorado, Spring 2012.

**MENTORSHIP****Ph.D. Students:**

Philip Warton (co-advised with Amir Nayyeri) 2022 – Present

**M.S. Students:**

Kaung (John) Myat Htay Win 2023 – Present  
Willow Barkan (co-advised with Amir Nayyeri) 2022 – 2023

**Undergraduate Students:**

Ian Tassin (senior honors thesis) 2021 – 2023  
Ryan Little 2021 – 2022  
Andrew Hwi Gue Cho 2018

**FUNDING**

NSF Award No. 2312297. Collaborative Research: AF: SaTC: Medium: Theoretical Foundations of Lattice-Based Cryptography. Joint PI with Noah Stephens-Davidowitz. Total: \$1.2 million, my share: \$600,000.

**SERVICE**

**Reviewing:** APPROX, CRYPTO, FOCS, ICALP, IMACC, ITCS, MFCS, SOCG, SODA, STACS, STOC, WADS, Algorithmica, Information and Computation, Journal of Combinatorial Optimization, SIDMA.

**Organization:** Workshop on Fine-Grained Cryptography at FSTTCS 2022 (jointly

organized with Divesh Aggarwal, Alexander Golovnev, Rajendra Kumar, and Noah Stephens-Davidowitz).

<b>WORK EXPERIENCE</b>	<b>Centrum Wiskunde &amp; Informatica</b> – Amsterdam, Netherlands	Fall 2016
	<b>Google</b> – Mountain View, CA; Kirkland, WA	Summer 2013, Summer 2014
	<b>Private Tutoring</b> – New York, NY	Various
	<b>Fusion-io</b> – Superior, CO	Summer 2012
	<b>Epic Systems</b> – Verona, WI	Summer 2010, Summer 2011

## SKILLS

### Programming Languages/Software:

Mostly imperative: C, C++, Java, Python, Visual Basic  
Mostly functional: OCaml, Scala, Scheme, Standard ML  
Mathematical: Lua, Mathematica, NumPy, R, Sage  
Constraint solving: MiniSat, Prolog, Z3  
Assembly: MIPS, x86  
Web: CSS, HTML, JavaScript  
Other: L<sup>A</sup>T<sub>E</sub>X, Lex/Yacc variants, Linux, OpenGL

**Languages:** English (native), Spanish (basic)

<b>AWARDS</b>	<b>Warren Postdoctoral Fellowship</b>	2018 – 2019
	<b>MacCracken Fellowship</b>	2012 – 2017
	<b>University Fellowship</b>	2010 – 2011
	<b>William F. Vilas Scholarship</b>	2006 – 2010
	<b>National Merit Finalist</b>	2006

<b>OTHER</b>	<b>1st Place, U.S. Open (Go) 3-dan division</b>	2009
	<b>1st Place, U.S. Open (Go) 1-dan division</b>	2008
	<b>Mountain Climbing</b> – Including 31 of 54 of Colorado's 14,000+ foot peaks.	

<b>PERSONAL INFORMATION</b>	<b>Legal Name:</b> Huxley David Bennett
	<b>Citizenship:</b> United States of America