

David J. Wu

Department of Computer Science
University of Texas at Austin

Email: dwu4@cs.utexas.edu
Website: <https://www.cs.utexas.edu/~dwu4/>

Employment

University of Texas at Austin, Austin, TX
Assistant Professor in Computer Science *Aug 2021–present*

University of Virginia, Charlottesville, VA
Visiting Assistant Professor in Computer Science *Aug 2021–Jul 2023*
Anita Jones Career Enhancement Assistant Professor in Computer Science *Jan 2019–Aug 2021*

Education

Stanford University, Stanford, CA *Sep 2013–Aug 2018*
Ph.D. in Computer Science
Thesis: *Lattice-Based Non-Interactive Argument Systems*
Thesis Advisor: Dan Boneh

Stanford University, Stanford, CA *Sep 2011–Jun 2013*
M.S. in Computer Science

Stanford University, Stanford, CA *Sep 2009–Jun 2013*
B.S. in Computer Science with Honors and Distinction, Minor in Physics
Thesis: *End-to-End Text Recognition with Convolutional Neural Networks*
Thesis Advisor: Andrew Y. Ng

Awards and Distinctions

- **Sloan Research Fellow**, 2025
- **Amazon Research Award**, 2025
- **1st Place (Phase 1), 2nd Place (Phase 2)**, U.S./U.K. Privacy-Enhancing Technologies Prize Challenge, 2023
- **Google Research Scholar**, 2022
- **Microsoft Research Faculty Fellow**, 2021
- **NSF CAREER Award**, 2021

Paper Awards and Recognition

- **Best Paper Award**, CRYPTO, 2022 [\[40\]](#)
- **Best Young-Researcher Paper Award**, CRYPTO, 2018 [\[55\]](#)
- **Best Young-Researcher Paper Award**, CRYPTO, 2017 [\[59\]](#)
- **Outstanding Paper Award**, ESORICS, 2016 [\[64\]](#)
- **Best Student Paper Award**, ICDAR, 2011 [\[70\]](#)

Publications

The convention for publications in cryptography and theoretical computer science is to list authors alphabetically. Most publications below follow this convention. Publications in other areas list students first and in order of contribution. For these works, a star (*) is used to denote authors with equal contribution.

Total citations: 7570; **h-index:** 38 (as of April 2026 according to [Google Scholar](#))

Refereed Conference Proceedings

- [1] **Heli: Heavy-Light Private Aggregation**
Ryan Lehmkuhl, Henry Corrigan-Gibbs, Emma Dauterman, and [David J. Wu](#)
USENIX Security Symposium (USENIX Security), 2026
- [2] **Silent Threshold Cryptography from Pairings: Expressive Policies in the Plain Model**
Brent Waters and [David J. Wu](#)
EUROCRYPT, 2026
- [3] **Threshold Batched Identity-Based Encryption from Pairings in the Plain Model**
Junqing Gong, Brent Waters, Hoeteck Wee, and [David J. Wu](#)
EUROCRYPT, 2026
- [4] **Distributed Monotone-Policy Encryption for DNFs from Lattices**
Jeffrey Champion and [David J. Wu](#)
EUROCRYPT, 2026
- [5] **Simultaneous-Message and Succinct Secure Computation: Reusable and Multiparty Protocols**
Siddharth Agarwal, Abhishek Jain, Akshayaram Srinivasan, and [David J. Wu](#)
EUROCRYPT, 2026
- [6] **The Structured Generic-Group Model**
Henry Corrigan-Gibbs, Alexandra Henzinger, and [David J. Wu](#)
EUROCRYPT, 2026
- [7] **Succinct Witness Encryption for Batch Languages and Applications**
Lalita Devadas, Abhishek Jain, Brent Waters, and [David J. Wu](#)
ASIACRYPT, 2025
- [8] **Pairing-Based Batch Arguments for NP with a Linear-Size CRS**
Binyi Chen, Noel Elias, and [David J. Wu](#)
ASIACRYPT, 2025
- [9] **Pairing-Based Aggregate Signatures without Random Oracles**
Susan Hohenberger, Brent Waters, and [David J. Wu](#)
ASIACRYPT, 2025
- [10] **A Hidden-Bits Approach to Statistical ZAPs from LWE**
Eli Bradley, George Lu, Shafik Nassar, Brent Waters, and [David J. Wu](#)
Theory of Cryptography Conference (TCC), 2025
- [11] **The Pseudorandomness of Legendre Symbols under the Quadratic-Residuosity Assumption**
Henry Corrigan-Gibbs and [David J. Wu](#)
Theory of Cryptography Conference (TCC), 2025
- [12] **Unbounded Distributed Broadcast Encryption and Registered ABE from Succinct LWE**
Hoeteck Wee and [David J. Wu](#)
CRYPTO, 2025

- [13] **Registered ABE and Adaptively-Secure Broadcast Encryption from Succinct LWE**
Jeffrey Champion, Yao-Ching Hsieh, and [David J. Wu](#)
CRYPTO, 2025
- [14] **A Pure Indistinguishability Obfuscation Approach to Adaptively-Sound SNARGs for NP**
Brent Waters and [David J. Wu](#)
CRYPTO, 2025
- [15] **Monotone-Policy BARGs and More from BARGs and Quadratic Residuosity**
Shafik Nassar, Brent Waters, and [David J. Wu](#)
International Conference on Practice and Theory of Public-Key Cryptography (PKC), 2025
[Invited to the *Journal of Cryptology*](#)
- [16] **Adaptively-Secure Big-Key Identity-Based Encryption**
Jeffrey Champion, Brent Waters, and [David J. Wu](#)
International Conference on Practice and Theory of Public-Key Cryptography (PKC), 2025
- [17] **New Techniques for Preimage Sampling: Improved NIZKs and More from LWE**
Brent Waters, Hoeteck Wee, and [David J. Wu](#)
EUROCRYPT, 2025
- [18] **A Generic Approach to Adaptively-Secure Broadcast Encryption in the Plain Model**
Yao-Ching Hsieh, Brent Waters, and [David J. Wu](#)
EUROCRYPT, 2025
- [19] **Multi-Authority Registered Attribute-Based Encryption**
George Lu, Brent Waters, and [David J. Wu](#)
EUROCRYPT, 2025
- [20] **Distributed Broadcast Encryption from Lattices**
Jeffrey Champion and [David J. Wu](#)
Theory of Cryptography Conference (TCC), 2024
- [21] **Monotone Policy BARGs from BARGs and Additively Homomorphic Encryption**
Shafik Nassar, Brent Waters, and [David J. Wu](#)
Theory of Cryptography Conference (TCC), 2024
- [22] **Batching Adaptively-Sound SNARGs for NP**
Lalita Devadas, Brent Waters, and [David J. Wu](#)
Theory of Cryptography Conference (TCC), 2024
- [23] **Batch Arguments to NIZKs from One-Way Functions**
Eli Bradley, Brent Waters, and [David J. Wu](#)
Theory of Cryptography Conference (TCC), 2024
- [24] **Dot-Product Proofs and Their Applications**
Nir Bitansky, Prahladh Harsha, Yuval Ishai, Ron D. Rothblum, and [David J. Wu](#)
IEEE Symposium on Foundations of Computer Science (FOCS), 2024
[Invited to the *SIAM Journal on Computing \(SICOMP\)*](#)
- [25] **RESPIRE: High-Rate PIR for Databases with Small Records**
Alexander Burton, Samir Jordan Menon, and [David J. Wu](#)
ACM Conference on Computer and Communications Security (CCS), 2024
- [26] **Reducing the CRS Size in Registered ABE Systems**
Rachit Garg, George Lu, Brent Waters, and [David J. Wu](#)
CRYPTO, 2024

- [27] **The One-Wayness of Jacobi Signatures**
Henry Corrigan-Gibbs and [David J. Wu](#)
CRYPTO, 2024
- [28] **YPIR: High-Throughput Single-Server PIR with Silent Preprocessing**
Samir Jordan Menon and [David J. Wu](#)
USENIX Security Symposium (USENIX Security), 2024
- [29] **Adaptively-Sound Succinct Arguments for NP from Indistinguishability Obfuscation**
Brent Waters and [David J. Wu](#)
ACM Symposium on Theory of Computing (STOC), 2024
- [30] **Succinct Functional Commitments for Circuits from k -Lin**
Hoeteck Wee and [David J. Wu](#)
EUROCRYPT, 2024
- [31] **Lattice-Based Functional Commitments: Fast Verification and Cryptanalysis**
Hoeteck Wee and [David J. Wu](#)
ASIACRYPT, 2023
- [32] **Realizing Flexible Broadcast Encryption: How to Broadcast to a Public-Key Directory**
Rachit Garg, George Lu, Brent Waters, and [David J. Wu](#)
ACM Conference on Computer and Communications Security (CCS), 2023
- [33] **How to Use (Plain) Witness Encryption: Registered ABE, Flexible Broadcast, and More**
Cody Freitag, Brent Waters, and [David J. Wu](#)
CRYPTO, 2023
- [34] **Non-Interactive Zero-Knowledge from Non-Interactive Batch Arguments**
Jeffrey Champion and [David J. Wu](#)
CRYPTO, 2023
- [35] **Authenticated Private Information Retrieval**
Simone Colombo, Kirill Nikitin, Henry Corrigan-Gibbs, [David J. Wu](#), and Bryan Ford
USENIX Security Symposium (USENIX Security), 2023
- [36] **Succinct Vector, Polynomial, and Functional Commitments from Lattices**
Hoeteck Wee and [David J. Wu](#)
EUROCRYPT, 2023
- [37] **Registered Attribute-Based Encryption**
Susan Hohenberger, George Lu, Brent Waters, and [David J. Wu](#)
EUROCRYPT, 2023
- [38] **Multi-Authority ABE from Lattices without Random Oracles**
Brent Waters, Hoeteck Wee, and [David J. Wu](#)
Theory of Cryptography Conference (TCC), 2022
- [39] **Fully Succinct Batch Arguments for NP from Indistinguishability Obfuscation**
Rachit Garg, Kristin Sheridan, Brent Waters, and [David J. Wu](#)
Theory of Cryptography Conference (TCC), 2022
- [40] **Batch Arguments for NP and More from Standard Bilinear Group Assumptions**
Brent Waters and [David J. Wu](#)
CRYPTO, 2022
[Best Paper Award; Invited to the *Journal of Cryptology*](#)

- [41] **SPIRAL: Fast, High-Rate Single-Server PIR via FHE Composition**
Samir Jordan Menon and [David J. Wu](#)
IEEE Symposium on Security and Privacy (Oakland), 2022
- [42] **Traceable PRFs: Full Collusion Resistance and Active Security**
Sarasij Maitra and [David J. Wu](#)
International Conference on Practice and Theory of Public-Key Cryptography (PKC), 2022
[Invited to the *Journal of Cryptology*](#)
- [43] **Beyond Software Watermarking: Traitor-Tracing for Pseudorandom Functions**
Rishab Goyal, Sam Kim, Brent Waters, and [David J. Wu](#)
ASIACRYPT, 2021
- [44] **Shorter and Faster Post-Quantum Designated-Verifier zkSNARKs from Lattices**
Yuval Ishai, Hang Su, and [David J. Wu](#)
ACM Conference on Computer and Communications Security (CCS), 2021
- [45] **CRYPTGPU: Fast Privacy-Preserving Machine Learning on the GPU**
Sijun Tan, Brian Knott, Yuan Tian, and [David J. Wu](#)
IEEE Symposium on Security and Privacy (Oakland), 2021
- [46] **Collusion Resistant Trace-and-Revoke for Arbitrary Identities from Standard Assumptions**
Sam Kim and [David J. Wu](#)
ASIACRYPT, 2020
- [47] **On Succinct Arguments and Witness Encryption from Groups**
Ohad Barta, Yuval Ishai, Rafail Ostrovsky, and [David J. Wu](#)
CRYPTO, 2020
- [48] **Can Verifiable Delay Functions be Based on Random Oracles?**
Mohammad Mahmoody, Caleb Smith, and [David J. Wu](#)
International Colloquium on Automata, Languages and Programming (ICALP), 2020
- [49] **New Constructions of Statistical NIZKs: Dual-Mode DV-NIZKs and More**
Benoît Libert, Alain Passelègue, Hoeteck Wee, and [David J. Wu](#)
EUROCRYPT, 2020
- [50] **New Constructions of Reusable Designated-Verifier NIZKs**
Alex Lombardi, Willy Quach, Ron D. Rothblum, Daniel Wichs, and [David J. Wu](#)
CRYPTO, 2019
- [51] **Watermarking PRFs from Lattices: Stronger Security via Extractable PRFs**
Sam Kim and [David J. Wu](#)
CRYPTO, 2019
- [52] **Watermarking Public-Key Cryptographic Primitives**
Rishab Goyal, Sam Kim, Nathan Manohar, Brent Waters, and [David J. Wu](#)
CRYPTO, 2019
- [53] **Exploring Crypto Dark Matter: New Simple PRF Candidates and Their Applications**
Dan Boneh, Yuval Ishai, Alain Passelègue, Amit Sahai, and [David J. Wu](#)
Theory of Cryptography Conference (TCC), 2018
- [54] **Function-Hiding Inner Product Encryption is Practical**
Sam Kim, Kevin Lewi, Avradip Mandal, Hart Montgomery, Arnab Roy, and [David J. Wu](#)
International Conference on Security and Cryptography for Networks (SCN), 2018

- [55] **Multi-Theorem Preprocessing NIZKs from Lattices**
Sam Kim and David J. Wu
CRYPTO, 2018
[Best Young-Researcher Paper Award; Invited to the *Journal of Cryptology*](#)
- [56] **Quasi-Optimal SNARGs via Linear Multi-Prover Interactive Proofs**
Dan Boneh, Yuval Ishai, Amit Sahai, and David J. Wu
EUROCRYPT, 2018
- [57] **Access Control Encryption for General Policies from Standard Assumptions**
Sam Kim and David J. Wu
ASIACRYPT, 2017
- [58] **Constrained Keys for Invertible Pseudorandom Functions**
Dan Boneh, Sam Kim, and David J. Wu
Theory of Cryptography Conference (TCC), 2017
- [59] **Watermarking Cryptographic Functionalities from Standard Lattice Assumptions**
Sam Kim and David J. Wu
CRYPTO, 2017
[Best Young-Researcher Paper Award; Invited to the *Journal of Cryptology*](#)
- [60] **Lattice-Based SNARGs and Their Application to More Efficient Obfuscation**
Dan Boneh, Yuval Ishai, Amit Sahai, and David J. Wu
EUROCRYPT, 2017
- [61] **Functional Encryption: Deterministic to Randomized Functions from Simple Assumptions**
Shashank Agrawal and David J. Wu
EUROCRYPT, 2017
- [62] **Constraining Pseudorandom Functions Privately**
Dan Boneh, Kevin Lewi, and David J. Wu
International Conference on Practice and Theory of Public-Key Cryptography (PKC), 2017
- [63] **Order-Revealing Encryption: New Constructions, Applications, and Lower Bounds**
Kevin Lewi and David J. Wu
ACM Conference on Computer and Communications Security (CCS), 2016
- [64] **Privacy, Discovery, and Authentication for the Internet of Things**
David J. Wu, Ankur Taly, Asim Shankar, and Dan Boneh
European Symposium on Research in Computer Security (ESORICS), 2016
[Outstanding Paper Award](#)
- [65] **Practical Order-Revealing Encryption with Limited Leakage**
Nathan Chenette, Kevin Lewi, Stephen A. Weis, and David J. Wu
Fast Software Encryption (FSE), 2016
- [66] **Privacy-Preserving Shortest Path Computation**
David J. Wu, Joe Zimmerman, J  r  my Planul, and John C. Mitchell
Network and Distributed System Security Symposium (NDSS), 2016
- [67] **Private Database Queries using Somewhat Homomorphic Encryption**
Dan Boneh, Craig Gentry, Shai Halevi, Frank Wang, and David J. Wu
International Conference on Applied Cryptography and Network Security (ACNS), 2013

- [68] **Deep Learning with COTS HPC Systems**
Adam Coates, Brody Huval, Tao Wang, [David J. Wu](#), Andrew Y. Ng, and Bryan Catanzaro
International Conference on Machine Learning (ICML), 2013
- [69] **End-to-End Text Recognition with Convolutional Neural Networks**
Tao Wang*, [David J. Wu*](#), Adam Coates, and Andrew Y. Ng
International Conference on Pattern Recognition (ICPR), 2012
- [70] **Text Detection and Character Recognition in Scene Images with Unsupervised Feature Learning**
Adam Coates, Blake Carpenter, Carl Case, Sanjeev Satheesh, Bipin Suresh, Tao Wang, [David J. Wu](#), and Andrew Y. Ng
International Conference on Document Analysis and Recognition (ICDAR), 2011
[Best Student Paper Award](#)

Journal Articles

- [71] **Watermarking Cryptographic Functionalities from Standard Lattice Assumptions**
Sam Kim and [David J. Wu](#)
Journal of Cryptology, 34 (28), 2021
Full version of a paper that originally appeared in CRYPTO 2017 [\[59\]](#)
- [72] **Avoiding Genetic Racial Profiling in Criminal DNA Profile Databases**
Jacob A. Blindenbach*, Karthik A. Jagadeesh*, Gill Bejerano, and [David J. Wu](#)
Nature Computational Science, 1 (4), 2021
- [73] **Multi-Theorem Preprocessing NIZKs from Lattices**
Sam Kim and [David J. Wu](#)
Journal of Cryptology, 33 (3), 2020
Full version of a paper that originally appeared in CRYPTO 2018 [\[55\]](#)
- [74] **Secure Genome-Wide Association Analysis using Multiparty Computation**
Hyunghoon Cho, [David J. Wu](#), and Bonnie Berger
Nature Biotechnology, 36 (6), 2018
- [75] **Deriving Genomic Diagnoses Without Revealing Patient Genomes**
Karthik A. Jagadeesh*, [David J. Wu*](#), Johannes A. Birgmeier, Dan Boneh, and Gill Bejerano
Science, 357 (6352), 2017
- [76] **Privately Evaluating Decision Trees and Random Forests**
[David J. Wu](#), Tony Feng, Michael Naehrig, and Kristin Lauter
Proceedings on Privacy Enhancing Technologies (PETS), 2016 (4), 2016

Refereed Workshop Proceedings

- [77] **Quantum Operating Systems**
Henry Corrigan-Gibbs, [David J. Wu](#), and Dan Boneh
Workshop on Hot Topics in Operating Systems (HotOS), 2017

Manuscripts and Technical Reports

- [78] **Keeping Patient Phenotypes and Genotypes Private while Seeking Disease Diagnoses**
Karthik A. Jagadeesh*, [David J. Wu*](#), Johannes A. Birgmeier, Dan Boneh, and Gill Bejerano
Available on bioRxiv as Report 10.1101/746230
- [79] **Immunizing Multilinear Maps Against Zeroizing Attacks**
Dan Boneh, [David J. Wu](#), and Joe Zimmerman
Available on the Cryptology ePrint Archive as Report 2014/930

Other Articles

- [80] **Fully Homomorphic Encryption: Cryptography's Holy Grail**
David J. Wu
XRDS: Crossroads, The ACM Magazine for Students (XRDS), 21 (3), 2015

Advising

Ph.D. Students

- Anish Banerjee (UT Austin) 2025–present
Co-advised with Brent Waters
- Shafik Nassar (UT Austin) [10] [15] [21] 2023–present
Co-advised with Brent Waters
- Jeffrey Champion (UT Austin) [4] [13] [16] [20] [34] 2022–present

Visiting Ph.D. Students

- Yao-Ching Hsieh (University of Washington) [13] [18] Jul 2024–Aug 2024

M.S. Students

- Hang Su (University of Virginia) [44] 2020–2021
Thesis: *Shorter and Faster Post-Quantum Designated-Verifier zkSNARKs from Lattices*

Undergraduate Students

- Noel Elias (UT Austin) [8] 2023–2025
Thesis: *Pairing-Based Batch Arguments with a Linear-Size CRS*
- Zeki Gurbuz (UT Austin) 2023–2024
Thesis: *Registered Functional Signatures*
- Alexander Burton (UT Austin) [25] 2022–2024
Thesis: *RESPIRE: Modifying SPIRAL Towards High-Rate PIR on Small-Record Databases*
- Jeriah Yu (UT Austin) 2023–2024
Thesis: *Policy-Based Oblivious Message Retrieval*
- Stephanie Cheng (UT Austin) 2022–2023
Thesis: *Retrieval by Keywords, Set Membership, and More from PIR*
- Jacob Blindenbach (University of Virginia) [72] 2019–2022
- Sijun Tan (University of Virginia) [45] 2019–2021
Thesis: *Fast Privacy-Preserving Machine Learning on the GPU*

Ph.D. Thesis Committees

- George Lu (UT Austin; advisor: Brent Waters) 2026
- Mingxun Zhou (Carnegie Mellon University; advisor: Giulia Fanti and Elaine Shi) 2025
- Rachit Garg (UT Austin; advisor: Brent Waters) 2024
- Valerio Cini (TU Wien; advisor: Daniel Slamanig and Matteo Maffei) 2024
- Muhammad Haris Mughees (UIUC; advisor: Ling Ren) 2023
- Jiahui Liu (UT Austin; advisor: Scott Aaronson) 2023
- Xiao Zhang (University of Virginia; advisor: David Evans) 2022
- Satya Vusirikala (UT Austin; advisor: Brent Waters) 2021
- Saeed Mahloujifar (University of Virginia; advisor: Mohammad Mahmoody) 2020

Funding and Grants

- **Stellar Development Foundation** Jan 2026
Silent Threshold Cryptography
- **Sloan Research Fellowship** Sep 2025
- **Amazon Research Award** Jun 2025
Fast Private Information Retrieval and More using Homomorphic Encryption
- **NSF Grant CNS-2318701 (SaTC Medium)** Oct 2023
Removing Trust Assumptions from Encryption Systems
Co-PIs: Susan Hohenberger and Brent Waters
- **Ethereum Foundation** Jul 2023
Functional Commitments and SNARKs from Lattices: Constructions and Cryptanalysis
- **Protocol Labs** Jul 2023
Scalable Private Information Retrieval Protocols using Lattices
- **Google Research Scholar** Apr 2022
High-Rate, High-Throughput Private Information Retrieval via FHE Composition
- **Microsoft Research Faculty Fellow** Sep 2021
Cryptographic Protocols for Securing and Verifying Computations
- **NSF Grant CNS-2140975 / CNS-2045180 (CAREER)** Aug 2021
Foundations of Cryptographic Proof Systems
- **NSF Grant CNS-2151131 / CNS-1917414 (SaTC Small)** Jan 2020
Expanding the Frontiers of Lattice-Based Cryptography
- **UVA SEAS Research Innovation Award** Jul 2019
Privacy-Preserving Machine Learning via Robust Learning and Noisy Computation
Co-PIs: David Evans, Mohammad Mahmoody, and Yuan Tian

Teaching

University of Texas at Austin

- **CS 388H:** Cryptography (Graduate)
Spring 2025, Fall 2022, Fall 2021
- **CS 346:** Cryptography (Undergraduate)
Fall 2025, Fall 2024, Fall 2023, Spring 2023
- **CS 395T:** Topics in Cryptography
Spring 2024, Spring 2022

University of Virginia

- **CS 6222:** Introduction to Cryptography
Spring 2021, Spring 2020
- **CS 4102:** Algorithms
Fall 2020, Fall 2019
- **CS 6501:** Advanced Topics in Cryptography
Spring 2019

Stanford University

- **CS 355: Topics in Cryptography**
Spring 2018
- **CS 359C: Classics of Cryptography**
Spring 2017

Selected Invited Talks

For a full listing, see <https://www.cs.utexas.edu/~dwu4/talks.html>.

- **Silent Threshold Cryptography from Pairings**
NIST Workshop on Multi-Party Threshold Schemes Jan 2026
- **Lattice Assumptions with Hints: Succinct LWE and its Applications**
Simons Institute Workshop on Obfuscation Jun 2025
- **Private Information Retrieval: Opportunities and Challenges**
AWS Security Jun 2025
- **Exotic Lattice Assumptions and How to Tame Them**
Oberwolfach Workshop on Cryptography (Plenary Talk) Jan 2025
- **New Techniques for Preimage Sampling: NIZKs and More from LWE**
Shonan Workshop on Encrypted Computation Oct 2024
- **Adaptively-Sound SNARGs for NP from Indistinguishability Obfuscation**
Charles River Crypto Day Sep 2024
- **Distributed Broadcast Encryption from Lattices**
CMU Workshop on Cryptography Sep 2024
- **Removing Trust Assumptions from Advanced Encryption Schemes**
TPLC: Theory and Practice of Laconic Cryptography (Invited Keynote) May 2024
Chinacrypt (Invited Keynote) Dec 2023
- **Lattice-Based Functional Commitments: Constructions and Cryptanalysis**
ENSL/CWI/KCL/IRISA Joint Cryptography Seminar Jun 2024
CHARM Seminar May 2024
- **Succinct Vector, Polynomial, and Functional Commitments from Lattices**
Lattice Meets Hashes Workshop May 2023
Bay Area Crypto Day Apr 2023
- **SPiRAL: Fast High-Rate Single-Server Private Information Retrieval**
EPFL Summer Research Institute Jul 2023
Google Research (New York) Oct 2022
- **Computing on Private Data: Private Genomics and More**
CATT Global Analytics Conference Nov 2022
- **Batch Arguments for NP and More from Standard Bilinear Group Assumptions**
Charles River Crypto Day Apr 2022
- **Watermarking and Traitor Tracing for PRFs**
Simons Institute Lattices Seminar Apr 2020

- **Computing with Lattices: Commitments, Signatures, and Zero-Knowledge**
Simons Institute Workshop on Lattices Mar 2020
- **Order-Revealing Encryption: Definitions, Constructions, and Challenges**
ICERM Workshop on Encrypted Search Jun 2019

Research Visits

Simons Institute , Berkeley, CA, Visiting Scientist	<i>Jun 2025–Aug 2025</i>
NTT Research , Sunnyvale, CA, Visiting Scientist	<i>Jul 2023–Aug 2023</i>
NTT Research , Sunnyvale, CA, Visiting Scientist	<i>Jul 2022–Aug 2022</i>

Patents and Patent Applications

- [1] **Secure Secret-Sharing-Based Crowdsourcing for Large-Scale Association Studies of Genomic and Phenotypic Data** (US 10910087)
Hyunghoon Cho, Bonnie Berger Leighton, [David J. Wu](#)
- [2] **Secure Computer Evaluation of k-Nearest Neighbor Models** (US 9825758)
Tony Feng, [David J. Wu](#), Michael Naehrig, and Kristin Lauter
- [3] **Secure Computer Evaluation of Decision Trees** (US 9787647)
[David J. Wu](#), Tony Feng, Michael Naehrig, and Kristin Lauter
- [4] **Optimizing Recategorization of Financial Transactions using Collaborative Filtering** (US 8538967)
[David J. Wu](#), Levon Budagyan, and Marko Rukonic

Professional Activities and Service

Organized Activities

- **Texas Crypto Day**, Co-Organizer *2022–present*
- **Workshop in PIR**, Co-Organizer *2024*

Conference Program Committees

- **CRYPTO** 2026, 2022, 2021, 2020
Annual International Cryptology Conference
- **EUROCRYPT** 2024, 2023, 2019
International Conference on the Theory and Applications of Cryptographic Techniques
- **IEEE S&P** 2023
IEEE Symposium on Security and Privacy
- **ACM CCS** 2026, 2023
ACM Conference on Computer and Communications Security
- **ASIACRYPT** 2024, 2022
Annual International Conference on the Theory and Application of Cryptology and Information Security
- **TCC** 2026, 2022
Theory of Cryptography Conference
- **PKC** 2026, 2025, 2023, 2022
International Conference on Practice and Theory of Public-Key Cryptography
- **CFAIL** 2022
The Conference for Failed Approaches and Insightful Losses in Cryptology

- **ISMB/ECCB 2019**
Intelligent Systems for Molecular Biology / European Conference on Computational Biology
- **CANS 2017**
International Conference on Cryptology and Network Security

Journal Editorial Board

- Theoretical Computer Science *2026–present*

External Reviewing

Conference Reviewing: CRYPTO, EUROCRYPT, ASIACRYPT, TCC, PKC, Financial Cryptography, SAC, STOC, SODA, ICALP, USENIX Security, ACM CCS, ISMB, ISIT

Journal Reviewing: SIAM Journal on Computing (SICOMP); Journal of Cryptology (JoC); ACM Transactions on Privacy and Security (TOPS); Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT); Communications of the ACM (CACM); IEEE Transactions on Knowledge and Data Engineering (TKDE); IEEE Transactions on Information Forensics and Security (TIFS); Design, Codes, and Cryptography; Journal of Computer Science and Technology; Proceedings of the National Academy of Sciences (PNAS); Nature Communications; Bioinformatics; Cell Systems

Grant Reviewing: National Science Foundation (NSF), Israel Science Foundation (ISF), Austrian Science Fund (FWF), Swiss National Science Foundation (SNSF)

University Service

University of Texas at Austin

- **Co-Organizer**, Cryptography and Security Seminar *2023–present*
- **Co-Organizer**, Theory Seminar *2022–present*
- **Member**, Google PhD Fellowship Internal Selection Committee *2026*
- **Member**, Turing Scholars Admissions Committee *2025–2026*
- **Member**, PhD Admissions Committee *2024–2025*
- **Member**, PhD Admissions Committee *2023–2024*
- **Chair**, MS/PhD Admissions Committee *2022–2023*
- **Member**, PhD Admissions Committee *2021–2022*

University of Virginia

- **Member**, Cybersecurity Faculty Search Subcommittee *2020–2021*
- **Member**, CS Department Graduate Program Committee *2019–2021*
- **Organizer**, CS Department Research Symposium *2019*