David J. Wu

Department of Computer Science
University of Texas at Austin

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

Positions

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

University of Virginia, Charlottesville, VA *Aug 2021–present*
Visiting Professor in Computer Science

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

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

- **Microsoft Research Faculty Fellow**, 2021
- **NSF CAREER Award**, 2021
- **Best Young-Researcher Paper Award**, CRYPTO, 2018
- **Best Young-Researcher Paper Award**, CRYPTO, 2017
- **Qualcomm Innovation Fellowship Finalist**, 2017
- **Outstanding Paper Award**, ESORICS, 2016
- **HLI Award for Secure Outsourcing**, UCSD iDASH Secure Genome Analysis Competition, 2015
- **National Science Foundation Graduate Research Fellowship**, 2013
- **Frederick Emmons Terman Engineering Scholastic Award**, 2013
- **Best Student Paper Award**, ICDAR, 2011

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.

Refereed Conference Proceedings

[1] **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

[2] **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

[3] **Collusion Resistant Trace-and-Revoke for Arbitrary Identities from Standard Assumptions**
Sam Kim and David J. Wu
ASIACRYPT, 2020

[4] **On Succinct Arguments and Witness Encryption from Groups**
Ohad Barta, Yuval Ishai, Rafail Ostrovsky, and David J. Wu
CRYPTO, 2020

[5] **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

[6] **New Constructions of Statistical NIZKs: Dual-Mode DV-NIZKs and More**
Benoît Libert, Alain Passelègue, Hoeteck Wee, and David J. Wu
EUROCRYPT, 2020

[7] **New Constructions of Reusable Designated-Verifier NIZKs**
Alex Lombardi, Willy Quach, Ron D. Rothblum, Daniel Wichs, and David J. Wu
CRYPTO, 2019

[8] **Watermarking PRFs from Lattices: Stronger Security via Extractable PRFs**
Sam Kim and David J. Wu
CRYPTO, 2019

[9] **Watermarking Public-Key Cryptographic Primitives**
Rishab Goyal, Sam Kim, Nathan Manohar, Brent Waters, and David J. Wu
CRYPTO, 2019

[10] **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

[11] **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

[12] **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*

[13] **Quasi-Optimal SNARGs via Linear Multi-Prover Interactive Proofs**
Dan Boneh, Yuval Ishai, Amit Sahai, and David J. Wu
EUROCRYPT, 2018

[14] **Access Control Encryption for General Policies from Standard Assumptions**
Sam Kim and David J. Wu
ASIACRYPT, 2017

[15] **Constrained Keys for Invertible Pseudorandom Functions**
Dan Boneh, Sam Kim, and David J. Wu
Theory of Cryptography Conference (**TCC**), 2017

[16] **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*

[17] **Lattice-Based SNARGs and Their Application to More Efficient Obfuscation**
Dan Boneh, Yuval Ishai, Amit Sahai, and David J. Wu
EUROCRYPT, 2017

[18] **Functional Encryption: Deterministic to Randomized Functions from Simple Assumptions**
Shashank Agrawal and David J. Wu
EUROCRYPT, 2017

[19] **Constraining Pseudorandom Functions Privately**
Dan Boneh, Kevin Lewi, and David J. Wu
International Conference on Practice and Theory of Public-Key Cryptography (**PKC**), 2017

[20] **Order-Revealing Encryption: New Constructions, Applications, and Lower Bounds**
Kevin Lewi and David J. Wu
ACM Conference on Computer and Communications Security (**CCS**), 2016

[21] **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

[22] **Practical Order-Revealing Encryption with Limited Leakage**
Nathan Chenette, Kevin Lewi, Stephen A. Weis, and David J. Wu
Fast Software Encryption (**FSE**), 2016

[23] **Privacy-Preserving Shortest Path Computation**
David J. Wu, Joe Zimmerman, Jérémy Planul, and John C. Mitchell
Network and Distributed System Security Symposium (**NDSS**), 2016

[24] **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

[25] **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

[26] **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

[27] **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

[28] **Watermarking Cryptographic Functionalities from Standard Lattice Assumptions**
Sam Kim and David J. Wu
Journal of Cryptology, *34 (28)*, 2021

[29] **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

[30] **Multi-Theorem Preprocessing NIZKs from Lattices**
Sam Kim and David J. Wu
Journal of Cryptology, *33 (3)*, 2020

[31] **Secure Genome-Wide Association Analysis using Multiparty Computation**
Hyunghoon Cho, David J. Wu, and Bonnie Berger
Nature Biotechnology, *36 (6)*, 2018

[32] **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

[33] **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

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

Manuscripts

[35] **Beyond Software Watermarking: Traitor-Tracing for Pseudorandom Functions**
Rishab Goyal, Sam Kim, Brent Waters, and David J. Wu
Available on the Cryptology ePrint Archive as Report 2020/316

[36] **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

[37] **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

[38] **Protecting Patient Privacy in Genomic Analysis**
David J. Wu
International Journal of Population Data Science (**IJPDS**), *3 (5)*, 2018

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

Funding and Grants

- **Microsoft Research Faculty Fellow** *Sep 2021–Sep 2023*
  Cryptographic Protocols for Securing and Verifying Computations
- **NSF Grant CNS-2045180 (CAREER)** *Aug 2021–July 2026*
  Foundations of Cryptographic Proof Systems
- **NSF Grant CNS-1917414 (SaTC)** *Jan 2020–Dec 2022*
  Expanding the Frontiers of Lattice-Based Cryptography
- **UVA SEAS Research Innovation Award** *Jul 2019–Jun 2020*
  Privacy-Preserving Machine Learning via Robust Learning and Noisy Computation
  Co-PIs: David Evans, Mohammad Mahmoody, and Yuan Tian

Advising

Ph.D. Students:

- Abtin Afshar *(University of Virginia)* *2020–present*

M.S. Students:

- Hang Su *(University of Virginia)* **[1]** *2020–2021*
  Thesis: Shorter and Faster Post-Quantum Designated-Verifier zkSNARKs from Lattices

Undergraduate Students:

- Zichao Hu *(University of Virginia)* *2020–present*
- Sijun Tan *(University of Virginia)* **[2]** *2019–present*
  Thesis: Fast Privacy-Preserving Machine Learning on the GPU
- Jacob Blindenbach *(University of Virginia)* **[29]** *2019–present*

Teaching

University of Texas at Austin

- CS 388H: Cryptography (Graduate)
  Fall 2021

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

Patents and Patent Applications

[1] **Secure Genome Crowdsourcing for Large-Scale Association Studies** (US 10910087B2)
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

Conference Program Committees

- **CRYPTO** 2021, 2020
  Annual International Cryptology Conference
- **EUROCRYPT** 2019
  International Conference on the Theory and Applications of Cryptographic Techniques
- **PKC** 2022
  International Conference on Practice and Theory of Public-Key Cryptography
- **ISMB/ECCB** 2019
  Intelligent Systems for Molecular Biology / European Conference on Computational Biology
- **CANS** 2017
  International Conference on Cryptology and Network Security

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); 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)

University Service

University of Virginia:

- Cybersecurity Faculty Search Subcommittee, 2021

- CS Department Graduate Program Committee, 2019–2021
- CS Department Research Symposium, Organizer, 2019