Wilson Nguyen

Stanford, CoDa 236
wdnguyen@cs.stanford.edu
https://c.rypto.systems

Research Focus

My research is on **applied** cryptography. I am concerned about the *concrete efficiency* and *post-quantum security* of zero-knowledge proof systems (zk-SNARKs), and explore how zero-knowledge can be used to keep corporations (banks, health insurance, social media) *accountable*.

Education

PhD, Stanford University, *Computer Science* 2020-*expected* 2025
Research: applied cryptography, zero-knowledge, SNARKs
Advisor: Dan Boneh

BS, Stanford, *Computer Science* 2020
Research: internet measurement, security, secure compilers
Advisors: Zakir Durumeric, Marco Patrignani

Employment

Microsoft Research, *research intern*, zero-knowledge & proof systems 2024
Advisor: Srinath Setty

Spearbit, *consultant*, zero-knowledge & proof systems 2022–2023

Stanford CURIS, *research intern*, internet measurement & infrastructure 2019
Advisor: Zakir Durumeric

Google, *security engineering intern*, security reviews & automated tooling 2018

Praetorian, *security intern*, security reviews & penetration testing 2017

Publications

Refereed Conference Papers

- **Accumulation without Homomorphism**
  Bünz, B., Mishra, P., Nguyen, W., Wang, W., In *Innovations in Theoretical Computer Science (ITCS)*, 2025. https://eprint.iacr.org/2024/474
- **MuxProofs: Succinct Arguments for Machine Computation from Vector Lookups**
  Di, Z., Xia, L., Nguyen, W., Tyagi, N., In *International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, 2025. https://eprint.iacr.org/2023/974

- **Mangrove: A scalable framework for folding-based SNARKs**
  Nguyen, W., Datta, T., Chen, B., Tyagi, N., Boneh, D., In *Annual International Cryptology Conference (CRYPTO)*, 2024. `https://eprint.iacr.org/2021/1342`
- **Revisiting the nova proof system on a cycle of curves**
  Nguyen, W., Boneh, D., Setty, S., In *Advances in Financial Technologies (AFT)*, 2023. `https://eprint.iacr.org/2023/969`

Manuscripts

- Nguyen, W., Setty, S., (2025). “Neo: Lattice–based folding scheme for CCS over small fields and pay–per–bit commitments”. In: *Cryptology ePrint Archive*. `https://eprint.iacr.org/2025/294`.
- Bünz, B., Mishra, P., Nguyen, W., Wang, W., (2024). “Arc: Accumulation for Reed–Solomon Codes”. In: *Cryptology ePrint Archive*. `https://eprint.iacr.org/2024/1731`.
- Boneh, D., Nguyen, W., Ozdemir, A., (2021). “Efficient functional commitments: How to commit to a private function”. In: *Cryptology ePrint Archive*. `https://eprint.iacr.org/2021/1342`.
- Simoiu, C., Nguyen, W., Durumeric, Z., (2021). “An Empirical Analysis of HTTPS Configuration Security”. In: *arXiv preprint arXiv:2111.00703*.

Teaching

Instructor

Advanced Cryptography, *Stanford CS355* 2024
symmetric foundations, zero-knowledge, multi-party computation, post-quantum
with Aditi Partap and Trisha Datta

Advanced Cryptography, *Stanford CS355* 2023
with Alex Ozdemir and Lior Rotem

Advanced Cryptography, *Stanford CS355* 2022
with Alex Ozdemir and Neil Perry

Teaching Assistant

Hacklab, *Stanford IPS/INTPOL268*, Head Teaching Assistant 2019
teach practical hacking to law and international policy students
develop labs, assigments, exams, practice environments, coordinate TA team
instructors: Alex Stamos, Riana Pfefferkorn

Hacklab, *Stanford IPS/INTPOL268*, Teaching Assistant 2018
instructors: Alex Stamos

Service

Outreach

Student Application Support Program, *Stanford CS* 2024
reviewed statements for PhD applicants from under-represented backgrounds

Master’s Research Advisor, *Stanford CS* 2021-2023
advised research project for master students, leading to conference paper & PhD program admissions

CURIS Undergraduate Research Advisor, *Stanford CS* 2022
advised research project for undergraduates, leading to PhD program admission

Event Organizer, *TreeCTF* 2018
developed & operated a computer security competition held at Stanford in partnership with TreeHacks, a hackathon with competing university students across the nation.

Event Organizer, *LASACTF* 2015-2016
developed & operated an online computer security competition for 5000+ high school and university students

Department Committees and Leadership

PhD Student Advisory Council, *Stanford CS* 2021–2023
advanced and advocated for PhD student needs and resources.

PhD Admissions Committee, *Stanford CS* 2021-2022
reviewed PhD applications and interviewed candidates

Applied Cybersecurity Organization, *Stanford* 2016-2019
co-captain, technical advisor, lab maintainer

External Conference Reviewing

CRYPTO'25, EUROCRYPT'25, SBC'24, CCS'21

Awards

Zero Knowledge Attack of the Year (Informal), *ZkSecurity* 2023

Tau Beta Pi Candidate, *Stanford* 2018-2019
Top 1/5 of engineering seniors and the top 1/8 of engineering juniors.

Collegiate Penetration Testing Competition, *National 1st place* 2017

Collegiate Penetration Testing Competition, *Western Region 1st place* 2017

Collegiate Cyber Defense Competition, *Western Region 2nd place* 2017

Invitational Cyber Defense Competition, *Western Region 1st place* 2016

Invited Talks

Mangrove

- Nexus, August 2024
- UPenn, June 2024
- Bay Area Crypto Day, April 2024
- Privacy & Scaling Explorations (Ethereum Foundation), April 2024
- UC Berkeley, March 2024

Revisiting the nova proof system over a cycle of curves

- Zero Knowledge Summit 10, September 2023
- Privacy & Scaling Explorations (Ethereum Foundation), August 2023
- Scroll, August 2023
- Spearbit, August 2023

Functional Commitments

- IEEE Foundations of Computer Science (FOCS) 2021

References

Dan Boneh, `dabo@cs.stanford.edu`, Stanford University
Applied Cryptography

Benedikt Bünz, `bb@nyu.edu`, New York University
Applied Cryptography

Nirvan Tyagi, `tyagi@cs.washington.edu`, University of Washington
Applied Cryptography