

# Wilson Nguyen

[wdn2016@nyu.edu](mailto:wdn2016@nyu.edu)  
[Personal Website]  
[Google Scholar]

## About

---

I am a Computer Science Assistant Professor/Faculty Fellow at the Courant Institute at New York University. My research is on cryptographic proof systems (more generally, interactive reductions). In particular, I am concerned about their practical efficiency (time, memory, communication complexity) and their post-quantum security (can we build practical systems from a variety of plausibly post-quantum assumptions?).

## Education

---

<b>PhD, Stanford University, Computer Science</b>	2025
Research: applied cryptography, zero-knowledge proof systems, SNARKs Advisor: Dan Boneh	
<b>BS, Stanford, Computer Science</b>	2020
Research: internet measurement, security, secure compilers Advisors: Zakir Durumeric, Marco Patrigiani	

## Employment

---

<b>NYU Courant Institute, Assistant Professor/Faculty Fellow</b>	2025–now
<b>Spearbit, lead security researcher, zero-knowledge &amp; proof systems</b>	2022–now
<b>Microsoft Research, research intern, zero-knowledge &amp; proof systems</b>	2024
Advisor: Srinath Setty	
<b>Stanford CURIS, research intern, internet measurement &amp; infrastructure</b>	2019
Advisor: Zakir Durumeric	
<b>Google, security engineering intern, security reviews &amp; automated tooling</b>	2018
<b>Praetorian, security intern, security reviews &amp; penetration testing</b>	2017

## Publications

---

### Selected Papers

- 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>

## 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>

### **Arc: Accumulation for Reed–Solomon Codes**

- Bünz, B., Mishra, P., Nguyen, W., Wang, W., In *Annual International Cryptology Conference (CRYPTO)*, 2025. <https://eprint.iacr.org/2024/1731>

### **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>

## 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>.
- 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*.

## 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

## Teaching

---

### Main Instructor

<b>Advanced Cryptography, Stanford CS355</b> symmetric foundations, zero-knowledge, multi-party computation, post-quantum with Aditi Partap and Trisha Datta	2024
<b>Advanced Cryptography, Stanford CS355</b> with Alex Ozdemir and Lior Rotem	2023
<b>Advanced Cryptography, Stanford CS355</b> with Alex Ozdemir and Neil Perry	2022

### Recitation Instructor

<b>Basic Algorithms, NYU CSCI-UA.0310</b> Main instructor: Oded Regev	2025
--------------------------------------------------------------------------	------

### Teaching Assistant

<b>Hacklab, Stanford IPS/INTPOL268</b> , Head Teaching Assistant taught practical hacking to law and international policy students developed labs, assignments, exams, practice environments, and coordinated TAs Main instructor: Alex Stamos, Riana Pfefferkorn	2019
<b>Hacklab, Stanford IPS/INTPOL268</b> , Teaching Assistant Main instructor: Alex Stamos	2018

## Service

---

### Conference Reviewing

<b>Program Committee, CRYPTO'26</b>
<b>External Reviewer, CRYPTO'25, EUROCRYPT'25, SBC'24, CCS'21</b>

### Department Committees and Leadership

<b>PhD Student Advisory Council, Stanford CS</b> advanced and advocated for PhD student needs and resources.	2021–2023
<b>PhD Admissions Committee, Stanford CS</b> reviewed PhD applications and interviewed candidates	2021-2022
<b>Applied Cybersecurity Organization, Stanford</b> co-captain, technical advisor, lab maintainer	2016-2019

### Outreach

<b>Student Application Support Program, Stanford CS</b> reviewed statements for PhD applicants from under-represented backgrounds	2024
<b>Master's Research Advisor, Stanford CS</b> advised research projects for master students, leading to conference paper & PhD admissions	2021-2023

---

<b>CURIS Undergraduate Research Advisor</b> , <i>Stanford CS</i>	2022
advised research projects for undergraduates, leading to PhD admissions	
<b>Event Organizer</b> , <i>TreeCTF</i>	2018
developed & operated a computer security competition held at Stanford in partnership with TreeHacks, a hackathon with competing university students across the nation.	
<b>Event Organizer</b> , <i>LASACTF</i>	2015-2016
developed & operated an online computer security competition for 5000+ high school and university students	

## Awards

---

<b>Zero Knowledge Attack of the Year</b> , <i>ZkSecurity</i>	2023
<b>Tau Beta Pi Candidate</b> , <i>Stanford</i>	2018-2019
Top 1/5 of engineering seniors and the top 1/8 of engineering juniors.	
<b>Collegiate Penetration Testing Competition</b> , <i>National 1st place</i>	2017
<b>Collegiate Penetration Testing Competition</b> , <i>Western Region 1st place</i>	2017
<b>Collegiate Cyber Defense Competition</b> , <i>Western Region 2nd place</i>	2017
<b>Invitational Cyber Defense Competition</b> , <i>Western Region 1st place</i>	2016

## References

---

**Dan Boneh**, [dabo@cs.stanford.edu](mailto:dabo@cs.stanford.edu), Stanford University  
Applied Cryptography

**Nirvan Tyagi**, [tyagi@cs.washington.edu](mailto:tyagi@cs.washington.edu), University of Washington  
Applied Cryptography

**Benedikt Büinz**, [bb@nyu.edu](mailto:bb@nyu.edu), New York University  
Applied Cryptography