AMEY SHUKLA

PERSONAL INFORMATION

email	amey.shukla@uconn.edu
website	amey.dev
phone	(M) +1 (316) 227 7002
address	371 Fairfield Way, Unit 4155, Storrs, CT 06269

GOAL

Advance practical cryptography by developing theoretical tools for authentication and privacy that address challenges in building resilient systems. Enable non-experts to implement resilient systems effectively.

EDUCATION

PhD in Computer Science

2023–2028   University of Connecticut

In the area of applied cryptography under Dr. Benjamin FULLER.

Masters in Computer Science, Thesis

2021–2023   Wichita State University

In the area of cybersecurity under Dr. Sergio Salinas MONROY.

Bachelors in Computer Science

2017–2021   Wichita State University

Dual/Accelerated program under Dr. Sergio Salinas MONROY.

WORK EXPERIENCE

University of Connecticut

2023–Present   Graduate Research Assistant

Working on exciting problems in applied cryptography, such as noisy authentication, oblivious computation, and searchable encryption.

Wichita State University

2021–2023   Graduate Teaching Assistant

TA'd: Introduction to Cybersecurity, Routing & Switching I, Applied Computing & Networks, Applied Programming & Scripting, Applied Web Apps & Database Development, as well as designed a brand new CTF prep course from scratch.

Responsibilities: Graded assignments, reached out and guided struggling students, reinforced material, answered student questions during office hours, and tracked attendance

NetApp

2019–2021   Software Engineer Intern

NetApp, formerly Network Appliances, is a storage appliance company that focuses on SAN, NAS, and other hybrid-cloud storage solutions. My work was mostly written in Java, Python, and C++.

Developed and maintained E-Series REST API, which served as an interface to low-level details of the storage appliance.

Developed a next-generation container execution framework utilizing Kubernetes, Docker, and Ansible to run storage software and functions on corresponding software with load balancing and highly available topology.

Developed a resource provisioning framework to provision storage software builds virtually on demand, saving many hours of developer downtime.

Implemented stress tests for storage appliances to test recovery in case of faults.

PUBLICATIONS

ACM CCS

Amey Shukla, Luke Demarest, Benjamin Fuller, Sohaib Ahmad, Caleb Manicke, Alexander Russell, Sixia Chen. *Fuzzy Extractors are Practical: Cryptographic Strength Key Derivation from the Iris.* ACM CCS 2025.

Pending

Maryam Rezapour, Amey Shukla, Arinjita Paul, Benjamin Fuller. *MORSE: Multi Adversarial Owner and Reader Searchable Encryption.* Submitted to IEEE S&P 2026.

OTHER INFORMATION

Awards

2025 · UConn Computer Science Predoctoral Fellowship.

2025 · UConn Fall Conference Participation Award.

2023 · UConn CSE Fellowship.

2021 · Global Select Scholarship.

Invited Talks

Fuzzy Extractors are Practical.

Google · Talk about Fuzzy Extractors at Google.

Microsoft Research · Talk about Fuzzy Extractors at Microsoft Research.

JP Morgan · Talk about Fuzzy Extractors at JP Morgan.

Boston University · Talk about Fuzzy Extractors at BU Crypto Seminar.

OTHER EXPERIENCES

2017–Present Volunteer

Volunteer

Invited to help moderate a cybersecurity summer camp for children in High School. Helped children during workshop, answered questions, debugged their code, and tasks to point out issues.

Volunteered at a program that helped university freshman make the best of their first semester.

2019–2021 Vice President

Wichita State Linux Users Group

Managed a Linux Users Group with 100+ members, and led workshops on applied cryptography, security, systems programming, ansible, computer graphics, and of course Linux.

Keywords

C · Python · Git · LaTeX · Docker · Ansible · Kubernetes · LXC · KVM · Mercurial · Cryptography.

Can write most imperative programming languages with access to documentation.

January 12, 2026