Sanketh Menda

snkth.com me@snkth.com

EDUCATION

PhD in Computer Science, Cornell Tech 2021-Present

Research in applied cryptography; advised by Thomas Ristenpart.

Thesis (working title): Building the Next Generation of Authenticated Encryption

BCS in Computer Science, University of Waterloo 2016-2021

TALKS

Building the Next Generation of AEAD

*Mihir Bellare, Shay Gueron, Viet Tung Hoang, **Sanketh Menda**, Julia Len, and Thomas Ristenpart*

Real World Crypto 2024 — snkth.com/talks/rwc2024

Flexible Authenticated Encryption

***Sanketh Menda**, Julia Len, Viet Tung Hoang, Mihir Bellare, and Thomas Ristenpart*

NIST Workshop on Block Cipher Modes of Operation 2023 — snkth.com/talks/nist2023

Ask Your Cryptographer if Context-Committing AEAD Is Right for You

*Mihir Bellare, John Chan, Paul Grubbs, Viet Tung Hoang, **Sanketh Menda**, Julia Len, Thomas Ristenpart, and Phillip Rogaway*

Real World Crypto 2023 — snkth.com/talks/rwc2023

PAPERS

Robust AE With Committing Security

*Viet Tung Hoang and **Sanketh Menda***

Asiacrypt 2024 — snkth.com/papers/asiacrypt2024

"Is Reporting Worth the Sacrifice of Revealing What I Have Sent?":
Privacy Considerations When Reporting on End-to-End Encrypted Platforms

*Leijie Wang, Ruotong Wang, Sterling Williams-Ceci, **Sanketh Menda**, and Amy X. Zhang*

SOUPS 2023 — snkth.com/papers/soups2023

Context Discovery and Commitment Attacks: How to Break CCM, EAX, SIV, and More

***Sanketh Menda**, Julia Len, Paul Grubbs, and Thomas Ristenpart*

Eurocrypt 2023 — snkth.com/papers/eurocrypt2023

Computations with Greater Quantum Depth Are Strictly More Powerful (Relative to an Oracle)

*Matthew Coudron and **Sanketh Menda***

STOC 2020 — snkth.com/papers/stoc2020

Oracle Separations for Quantum Statistical Zero-Knowledge

***Sanketh Menda** and John Watrous*

arXiv preprint 2018 — snkth.com/papers/arxiv2018

EXPERIENCE

Graduate Research, Cornell Tech 2021-Present

Leading a project on designing safer cryptographic libraries for encrypting data.
Contributing to projects on designing more practical authenticated encryption schemes.
Led a project on analyzing commitment security of AEAD, resulting in Eurocrypt and RWC talks.

Applied Scientist Intern, Amazon Web Services May-Aug 2024

Designed and prototyped a hybrid post-quantum blob encryption system for use in AWS services.
Collaborated with product teams and other scientists to understand requirements and build a tailored solution.

Github PRs: aws/aws-lc/pull/1741, aws/aws-lc/pull/1777, corretto/[accp]/pull/398

Summer Associate, Trail of Bits May 2023-Aug 2023

Developed practice-focused documentation on the Inner Product Argument (which underlies Bulletproofs).
Update announcement: blog.trailofbits.com/2023/12/26/weve-added-more-content-to-zkdocs/
Participated in cryptography audits, from code review through final readout.

Security Developer Co-op, ISARA Corporation (multiple)

Improved in-repo tooling to assure correctness of post-quantum TLS implementation. Sep 2020-Dec 2020
Improved external tooling to test correctness of post-quantum TLS implementation. Jan 2020-Apr 2020
Improved external tooling to test correctness of post-quantum crypto implementations. May 2019-Aug 2019

Undergraduate Researcher, Institute for Quantum Computing (multiple)

Building quantum algorithms to solve problems in topology. Sep 2018-Dec 2018
Exploring the mathematics of quantum measurements. Jan 2018-Apr 2018
Studying the limits of restricted classes of quantum interactive proofs. May 2017-Aug 2017

PROGRAMMING

I am comfortable programming in C, Rust, Go, C++, Python, and x86 assembly.
I showed that pure Rust OCB3 can outperform Ring's GCM (now upstreamed to RustCrypto).
I showed that AMFs are practical, even on phones.
I contributed privacy features to Firefox.

AWARDS

Cornell Tech Outstanding TA Award 2022
Cornell University Fellowship 2021-2022
Waterloo Faculty of Mathematics Scholarship 2017-2021
Waterloo President's Research Award 2018
Waterloo President's Scholarship of Distinction 2017

TEACHING

Teaching Assistant for Cornell CS 5830 Cryptography Spring 2023
Teaching Assistant for Cornell CS 5830 Cryptography Spring 2022

SERVICE

Program Committee for Information Security Conference 2024 2024
External Reviewer for Crypto 2024 2024