Sanketh Menda

c1own.com
[email]

tldr

- irl experience with crypto
- comfortable with async
- can read papers/specs

Languages

1. C/C++
2. Python
3. Rust
4. Go

Interests

1. Cryptography
2. Security
3. Networking
4. Browsers
5. Compilers
6. CTFs

Education

University of Waterloo
4a Computer Science
Fall 2016-2021

Selected Coursework

Applied Cryptography	98
Computer Security and Privacy	97
Computer Networking	92
Models of Computation	98

Experience

Developer, ISARA Corporation Jan-Apr 2020
Python, C
experience working with TLS and its post-quantum cousins • X.509 • more experience with post-quantum primitives

Developer, ISARA Corporation May-Aug 2019
Python, C
experience working with post-quantum cryptographic primitives • read more than one NIST PQC submission

Researcher, Institute for Quantum Computing Sep-Dec 2018
sage, theory
quantum algorithms for topology • knots • noisy quantum computation

Researcher, Institute for Quantum Computing Jan-Apr 2018
sage, theory
mathematics of quantum measurements • elliptic curves • entanglement

Researcher, Institute for Quantum Computing May-Aug 2017
theory
quantum interactive proofs • zero-knowledge

Projects

(more at sgmenda)

Firefox C++, JavaScript
Contributed to Firefox's fingerprint resistance by implementing new defences and squashing bugs. Also, contributed to the Editor by making it easier to use password managers (blog post) and squashing related bugs (vlog).

dinky-c: A Dinky C Compiler in Rust Rust, asm
Handwritten lexer, handwritten recursive descent parser. Compiles a subset of ISO-C to pseudoassembly, and then to x86_64.

cpp-scrypt: A C++ Implementation of Scrypt C++
A C++ implementation of scrypt (RFC 7914) including an implementation of the Salsa20 hash function, but the PBDKF2 is from OpenSSL.

Papers

Computations with Greater Quantum Depth Are Strictly More Powerful (Relative to an Oracle)
Matthew Coudron and Sanketh Menda
Proceedings of STOC 2020. arXiv:1909.10503 [quant-ph]

Oracle Separations for Quantum Statistical Zero-Knowledge
Sanketh Menda and John Watrous
arXiv:1801.08967 [cs.CC]