

NoahVSELY

Cryptographer

Contact

 London, UK
 +44 7903 224172
 fowlslegs@riseup.net
 github.com/nvesely

Languages

Rust, Go, Python, C/C++,
SQL, Clojure, Shell, LaTeX



Technologies

Cryptography. libzexe,
bellman, libsodium
Security. Tor, IPTables,
OSSEC, tcpdump/
Wireshark
Data Science. scikit-learn,
Jupyter Notebooks, NumPy,
Clojush
Devops. Docker, KVM,
Container Linux, libvirt,
Ansible, Vagrant, systemd,
VirtualBox
Frameworks. Django,
Flask
Revision. git, Github
Development. Agile, TDD
Firmware. Coreboot





Interests

Zero-knowledge proofs
Anonymous communication
Machine learning
Functional programming
Formal verification
Guitar
Rock climbing

Experience

- Sum. '19 **Celo Research Scientist** San Francisco, USA
Research and design of an ultra-light client for a BFT-style blockchain network utilizing zk-SNARKS, proof-carrying data, and SNARK-friendly primitives.
- Sum. '18 **Glyff Research Scientist** London, UK
Designed a privacy-preserving smart contract platform based on Ethereum. Co-authored a whitepaper. Audited a prototype implementation.
- 2017–8 **Freelance Security and Cryptography Engineer** Mexico City, MX
Information security and cryptography related development, consulting, and training. Clients included Data Cívica and Human Rights Data Analysis Group.
- 2015–7 **Freedom of the Press Foundation Security Engineer** San Francisco, USA
/securedrop. Developed an open-source whistleblower submission platform. Stringent security requirements and a multi-machine, multi-OS architecture demanded wide-breadth domain knowledge including cryptographic, network, OS, and application-level security expertise.
/fingerprint-securedrop. Designed and implemented a machine learning (ML) system to evaluate website fingerprinting attacks and defenses for Tor onion services. Led Tor meeting group sessions on the topic and presented my work to KU Leuven's COSIC research group.
/wa-knn-fingerprint-securedrop. The fastest implementation of a specialized ML classifier.
- 2013– **Web Precision Security Consultant & Systems Administrator** Mission Viejo, CA, USA
Intermittent consulting. Most recently (2018): designed a sandboxing solution for a multi-tenant web server that successfully isolated website compromises to unprivileged tenant domains.
- 2012–5 **Hampshire College Quantitative Resource Center Manager** Amherst, MA, USA
Tutored primarily mathematics and computer science. Managed the hiring process, budgeting, and staff schedule. Under my oversight the center saw record attendance levels.

Projects

- 2018 **Winternitz Author** /winternitz
The first standalone implementation of the post-quantum WOTS-T one-time signature scheme.
- 2018 **Shamir's Secret Sharing Author** /RustySecrets
An implementation of Shamir's Secret Sharing Scheme that provides authentication of shares.
- 2018 **SodiumOxide Maintainer & Contributor** /sodiumoxide
Rust bindings to the C++ libsodium cryptography library.
- 2017– **Application Layer Padding Concerns Adversaries (ALPaCA) Author** /libalpaca
A library that implements ALPaCa, an application-layer defense against website fingerprinting.

Education

2018

Master of Science in Information Security

University College London

Polynomial Commitment Schemes with Applications to Zero-Knowledge Proofs

We introduce two new efficient PC schemes, one that is *succinct* and another that is *transparent* (i.e., that doesn't require a trusted setup). Our main application introduces a new, state-of-the-art [redacted]. One building block of our transparent PC scheme is a new [redacted]. In the appendices we show a few additional applications of this [redacted] including highly efficient aggregation of pairing-based zkSNARKs and signatures.

Other highlights:

- Started two research papers in zero-knowledge proofs, one of which has been submitted to OAKLAND 2020 and the other still in progress.
- Currently implementing a novel zero-knowledge proof system for R1CS introduced in one of our research papers.

2015

 **Bachelor of Science** in Mathematics, minor in Computer Science

Hampshire College

McEliece-Type Cryptosystems as Post-Quantum Standards

An analysis of McEliece-Type cryptosystems as a post-quantum replacement for RSA. Review of literature focusing on developments towards an IND-CCA2 variant with sufficiently small key size for embedded devices.

An Evolved Cryptographic Compression Function

Used the PushGP genetic programming environment to evolve a cryptographic compression function.

Other highlights:

- Worked in a genetic programming research group.
- Founded a student group to promote open-source & privacy enhancing technologies.