

# NoahVESELY

Cryptographer

## Contact

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

## Languages

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

## Technologies

**Security.** libsodium, 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

Anonymous communication  
Zero-knowledge proofs  
Privacy technologies (PETs)  
Cryptography  
Machine learning  
Functional programming  
Formal verification  
Guitar  
Rock climbing

## Experience

- 2018– **Glyff Cryptographer** London, UK  
Designed a privacy-preserving smart contract platform based on Ethereum. Co-authored a whitepaper. Audited a prototype implementation.
- 2017–8 **Freelance Security Engineer** Mexico City, MX  
Information security 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  
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

*McEliece-Type Cryptosystems as Post-Quantum Standards*

 /McEliece

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*

 /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.