Deirdre Connolly

Email: durumcrustulum at gmail dot com

Cryptographic engineer / applied cryptographer. I like memory-safe languages, quantum-resistant cryptography, elegant protocols, privacy-respecting systems, secure primitive abstractions, and making sure the development cycle enables humans to write secure software with minimal friction.

Education

Massachusetts Institute of Technology

2004 - 2008

SB - Electrical Engineering and Computer Science

Skills

Languages + Frameworks

Rust, Golang, JavaScript/ECMAScript, NodeJS, Python, React, SASS/CSS, Java

Tools

Cargo, GitHub Actions, Google Cloud, AWS, OpenTelemetry, macOS, Linux/Unix, git, property-based testing, fuzzing, svn, perforce, RocksDB, MySQL

Experience

Cryptographic Engineer

Zcash Foundation | May 2019 - Present

- Lead engineer on Zebra, a Rust implementation of Zcash, a privacy-preserving cryptocurrency. Drove from a proof-of-concept async, modular, network protocol implementation based on the Tokio runtime and Tower service abstractions to a full validation node that syncs and validates multiple kinds of zkSNARKs, elliptic curve signatures, blinded commitment merkle trees, and more in half the time of the standard reference implementation of Zcash, all in Rust modulo a few dependencies. Grew and mentored team from two to six contributors over two years.
- Implemented Zcash's Orchard, Sapling, and Sprout key, note, commitment, and note commitment tree derivation / computation in Rust, including property testing and test vector compatibility coverage.
- Implemented and upstreamed batch verification for Groth16 zkSNARK proofs and RedJubjub Schnorr-style signatures that support re-randomization. This batch math was integrated with async futures-based verification in Zebra.
- Implemented the FROST threshold signature protocol for RedJubjub with Chelsea Komlo, which was audited in March 2021. This has been integrated into at least one Zcash wallet so far.
- Set up and maintained Zebra CI/CD testing, review, build, and deployment pipeline, leveraging GitHub Actions, dependency locking & updating with Dependabot, code coverage collection and tracking, restricting merging to #main only from U2F/WebAuthn'd team members on green CI, automatic deployment of multiple zebrad nodes on green #main CI, monitored and kept up by automated deployment systems, with panics logged & correlated with change version, reported to the dev team.
- ZIP Editor on behalf of the Zcash Foundation; reviewed Zcash Improvement Proposals and updates to the Zcash Specification for soundness, completeness, accuracy, compatibility, security, maintainability, complexity, privacy leaks, in collaboration with ZIP Editors from the Electric Coin Company.

Senior Software Engineer

Brightcove | July 2014 - April 2019

- Developed and released new VideoCloud Studio, specifically Upload module with fast multipart video uploading and ingestion as a client side experience, and shipped fully HTML5 in-browser image capture from video and ingestion in Media module.

- Managed Node.js backing server for new Studio platform, including service proxies and AWS temporary authentication logic for clients. Migrated from dedicated hardware to scalable AWS-based architecture including continuous integration and deployment.
- Ported module builds to new shared, versioned and extensible Grunt-based build configuration that allowed fast migration from Coffescript to ES6 with minimal changes. Migrated all modules from Require.js to CommonJS module syntax built with Browserify.

Software Engineer

Akamai Technologies | Feb 2013 - June 2014

- Worked on Property Manager, a web application enabling customers to configure complex Akamai Edge Network products without support. Front end engineering work with JSMVC/CanJS, Sass, and backend work usingJersey/JAX-RS/JAX-B and Spring
- Contributed to continuous integration and deployment infrastructure, moving the team codebase from Perforce to git hosted by Atlassian Stash and builds/deploys with Jenkins, now being rolled out across the organization
- Drove improvements in dev tooling and automation, including new static dev environment with Grunt and NodeJS w/ Express with automated i18n generation, unit tests, style and script compilation on the fly

Product Developer

HubSpot | Feb 2012 - Dec 2012

- Django+Javascript front ends such as the platform dashboard, in-app alerts, customer on-boarding experiences, product settings, and data migration workflows
- Wrote multiple python REST clients for internal user, account, and product gating services

DevOps Engineer

HubSpot | Aug 2011 - Feb 2012

- Internal deploy tooling and infrastructure, weaving together custom Django interfaces, python scripts, AWS automation, and Jenkins continuous integration
- Replaced local deploy script with Django webapp to enable no-setup, one-click build deploys, using Celery jobs and later Jenkins tasks

Software Engineer in Test

HubSpot | April 2010 - Aug 2011

- Automated browser and REST API testing with python and selenium
- Team designed new testing frameworks based on nose.

Talks

Making Zcash Shine with Rust — *Zcon1 | June 2019*

Supersingular Isogeny Diffie-Hellman — *DEF CON Crypto|Privacy Village | Aug 2017*

Supersingular Isogeny Diffie-Hellman — *Cloudflare Crypto Meetup | Feb 2017*

Elliptic Curve Cryptography — *Facebook Security @Scale | Nov 2015*

Contributions

ristretto255-dh — *Diffie-Hellman key exchange over the Ristretto255 group in Rust*

Black Hat USA Review Board — *Cryptography Track*

RFC 7748: Elliptic Curves for Security — *Acknowledged Contributor*

Indocrypt 2016 — *Subreviewer*

Contributor to various open source projects.

Extracurriculars

Security, Cryptography, Whatever — *Podcast creator, host, producer*

Boston Women's Rugby Football Club — *CTO | Jan 2012 - August 2015*

Competitive Powerlifting, Strongman