DEIRDRE CONNOLLY

github @dconnolly

email durumcrustulum@gmail.com

Applied cryptographer. I like memory-safe languages, quantum-resistant cryptography, fast prime-order groups, elegant protocols, privacy-respecting systems, secure primitive abstractions, formal methods / computer-aided cryptography, and tooling that enables humans to write secure software with minimal friction.

EDUCATION

2004-2008 Bachelor of Science

MIT Electrical Engineering and Computer Science

SKILLS

Languages Rust, Tokio/async, Golang, JavaScript, NodeJS, Python, Coq, SASS/CSS, Java, LaTeX

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

Computer-aided Cryptography hacspec, SSProve, Coq, Tamarin, EasyCrypt

WORK EXPERIENCE

May 2019–Present Cryptographic Engineer

Zcash Foundation

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, in Rust (modulo a few dependencies.) Zebra successfully validated the latest Zcash Network Upgrade in May 2022. Grew and mentored team from two to six contributors over two years

Implemented Zcash's Orchard, Sapling, and Sprout shielded , including key, note, commitment, and note commitment merkle tree derivation / computation in Rust, including property testing and test vector compatibility coverage. Implemented and upstreamed batch verification for Groth16 zkSNARK proofs and RedDSA Schnorr-style signatures that support re-randomization. This batch math was integrated with async futures-based verification in Zebra

Implemented the FROST threshold Schnorr signature protocol as a generic Rust library, 'frost-core', used to implement 5 spec-compatible ciphersuites of the threshold protocol in 300 lines of Rust each; co-author on the FROST IRTF specification (in last call)

Implemented and published ristretto255-dh, Diffie-Hellman key exchange over the Ristretto255 group, in Rust; created a faux version of the Zcash Protocol Specification that used the Ristretto255 group as part of an interview take home exercise

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

July 2014 - April 2019 **Senior Software Engineer**

Brightcove

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

Feb 2013 - June 2014 **Software Engineer**

Akamai

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 using Jersey/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

Feb 2012 - Dec 2012 **Product Developer**

HubSpot

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

Aug 2011 - Feb 2012 **DevOps Engineer**

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

April 2010 - Aug 2011 **Software Engineer in Test**

Automated browser and REST API testing with python and selenium, designed new testing frameworks based on nose

PUBLICATIONS

2023 Supersingular Curves You Can Trust · IACR Eurocrypt 2023

Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, Benjamin Wesolowski

Two-Round Threshold Schnorr Signatures with FROST · IRTF Crypto Forum Research Group (CFRG)

Deirdre Connolly, Ian Goldberg, Chelsea Komlo, Chris Wood

TALKS

2022 A Requiem for SIDH: Efficient algorithms for supersingular isogeny Diffie-Hellman · Papers We Love 2022

FROST Engineering Updates · Zcon3

2021 The Orchard Shielded Pool, feat. Halo2, w/ Sean Bowe & Daira Hopwood · Zcon2 Lite

2019 Making Zcash Shine with Rust, w/ Anna Kaplan · Zcon1

2017 Supersingular Isogeny Diffie-Hellman · DEF CON Crypto Privacy Village

Supersingular Isogeny Diffie-Hellman · Cloudflare Crypto Meetup

2015 Elliptic Curve Cryptography · Facebook Security @Scale

SERVICE

HACS (High-Assurance Crypto Software) Workshop 2023+ · Organizer

USENIX Enigma 2023 · Program Committee / Reviewer

Black Hat USA · Cryptography Track Reviewer, previously Lead

Indocrypt 2016 · Subreviewer

BUT WAIT, THERE'S MORE

Podcast Security Cryptography Whatever · Creator, host, producer

Sports Boston Women's Rugby Football Club · CTO · Jan 2012 - Aug 2015

Competitive Powerlifting, Strongman