Christopher Patton

Senior Research Engineer

chrispatton+cv@gmail.com
cjpatton.net
github.com/cjpatton



Experience

2020—∞ **Cloudflare Research**, *Cloudflare–SF*
I'm a senior research engineer at Cloudflare focused on cryptography. I've worked on various privacy enhancing technologies (Privacy Preserving Measurement, Encrypted Client Hello), but these days I focus primarily on the post-quantum transition. I'm involved in bringing Merkle Tree Certificates to the web, developing post-quantum alternatives for "fancy" primitives, such as anonymous credentials, and various internal initiatives that interact with virtually all deployed cryptography at Cloudflare.

Summer 2018 **Delegated credentials for TLS**, *Internship at Cloudflare–SF*
Delegated credentials for TLS is an extension that allows an operator to delegate short-lived credentials for terminating connections on its behalf. I implemented the extension for boringSSL, added support to Cloudflare's edge servers, and helped develop the standard. Once browsers adopt it, this extension will make TLS more secure in practice. One problem with short-lived credentials is that client-clock skew limits their effective lifetime. To help address this, I also deployed the Roughtime protocol, which is now live.

Summer 2016 **Malware detection**, *Internship at Google–Montréal*
I worked on the Chrome Protector team, which is tasked with defending users from malware and other unwanted software. My project took a data-driven approach to detecting malware campaigns in the wild, and involved studying how malicious code gets injected into the browser. I also explored using Riposte for anonymous reporting in Chrome.

Summer 2015 **Trustworthy computing**, *Internship at Google–Kirkland*
CloudProxy is an open source project that binds the identity of a service (that is, its public key) to the code that executes it, as well as the environment in which it executes. My project for the Cloud Security team involved bringing this platform to bear on production servers at Google. I also worked on the open source codebase and implemented a mixnet for the platform.

2013–15 **QRAAT**, *John Muir Institute of the Environment (JMIE)*
The Quail Ridge Automated Animal Tracking (QRAAT) system is designed to provide ecologists with high resolution, real-time animal tracking data. It is comprised of a network of radio receivers deployed across the Quail Ridge Nature Reserve in Napa Valley, California, and uses radio telemetry to track species ranging in size from field mice to foxes. My master's project involved developing statistical methods for improving the system's performance.

2012–13 **Qurinet**, *JMIE*
Qurinet is an experimental, wireless, solar-powered mesh network that provides the network infrastructure for the QRAAT project and other monitoring equipment. I was responsible for network administration and site reliability, and I assisted in experiments for the networking lab at UC Davis.

Education

2016–20 **PhD**, *University of Florida*, Cryptography, advised by Tom Shrimpton

2013–15 **MS**, *University of California (Davis)*, CS, advised by Nina Amenta

2008–13 **BAS**, *University of California (Davis)*, CS and German

2010–11 *Freie Universität (Berlin)*, study abroad.

Papers

WPES 2026 **Private SCT Auditing, Revisited**, L. Heimberger, C. Patton, and B. Westerbaan, ia.cr/2025/556

PETS 2025 **Mastic: Private Weighted Heavy-Hitters and Attribute-Based Metrics**, D. Mouris, C. Patton, H. Davis, P. Sarkar, and N. Tsoutsos, ia.cr/2024/221

PETS 2023 **Verifiable Distributed Aggregation Functions**, H. Davis, C. Patton, M. Rosulek, and P. Schoppmann, ia.cr/2023/130

AsiaCCS 2022 **SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication**, C. Peeters, C. Patton, I. Munyaka, D. Olszewski, T. Shrimpton, and P. Traynor, 10.1145/3488932

Crypto 2020 **Quantifying the security cost of migrating protocols to practice**, C. Patton and T. Shrimpton, ia.cr/2020/573

CCS 2019 **Probabilistic data structures in adversarial environments**, D. Clayton, C. Patton, and T. Shrimpton

Crypto 2019 **Security in the presence of key reuse: Context-separable interfaces and their applications**, C. Patton and T. Shrimpton, ia.cr/2019/519

AsiaCCS 2019 **A hybrid approach to secure function evaluation using SGX**, J. Choi, D. Tian, G. Hernandez, C. Patton, B. Mood, T. Shrimpton, K. Butler, and P. Traynor

NDSS 2019 **Digital healthcare-associated infection: A case study on the security of a major multi-campus hospital system**, L. Vargas, L. Blue, V. Frost, C. Patton, N. Scaife, K. Butler, and P. Traynor

CCS 2018 **Partially specified channels: The TLS 1.3 record layer without elision**, C. Patton and T. Shrimpton, ia.cr/2018/634

Crypto 2017 **Hedging public-key encryption in the real world**, A. Boldyreva, C. Patton, and T. Shrimpton, ia.cr/2017/510

Internet-Drafts

Downgrade Prevention for the Internet Key Exchange Protocol Version 2 (IKEv2), V. Smyslov and C. Patton, draft-ietf-ipsecme-ikev2-downgrade-prevention

Verifiable Distributed Aggregation Functions, R. Barnes, D. Cook, C. Patton, and P. Schoppmann, draft-irtf-cfrg-vdaf

Distributed Aggregation Protocol for Privacy Preserving Measurement, T. Geoghegan, C. Patton, E. Rescorla, and C. Wood, draft-ietf-ppm-dap

Code

PQ anonymous credentials, vole-mole, C++ implementations of various post-quantum anonymous credentials in the VOLE-in-the-Head framework.

VDAF, prio, Rust implementations of the Verifiable Distributed Aggregation Functions specification. While I am not the maintainer of this crate, I have contributed a ton of code, including the FLP implementation.

DAP, daphne, Rust implementation of the Distributed Aggregation Protocol specification, targeting the Cloudflare Workers platform. Currently unmaintained.

TLS Encrypted Client Hello, cloudflare/go, Cloudflare Research maintains a fork of the Go standard library in order to facilitate experiments. I contributed a significant amount of code to this library, including its implementation of the Encrypted Client Hello extension for TLS (draft-ietf-tls-esni).

Delegated credentials for TLS, boringSSL server / NSS client, A protocol extension (RFC9345) that allows a TLS operator to delegate credentials for terminating connections on its behalf.

Roughtime, roughtime, A simple protocol for synchronizing clocks with enough accuracy for common cryptographic applications. I deployed the server on Cloudflare's infrastructure during my internship.

Talks

Merkle Tree Certificates and the next phase of the WebPKI, *Cloudflare Connect 2026*, Recording

Mastic: Private Weighted Heavy-Hitters and Attribute-Based Metrics, *PETS 2025*, No recording available

Secure aggregation at IETF, *Google Research Conference on Ads Privacy 2025*, No publc recording available

How to write proofs for cryptographic protocols at IETF, *Usable Formal Methods Research Group, IETF 120*, YouTube recording and corresponding writeup

Computing on your data with MPC, *Cryptographic Applications Workshop, co-located with Eurocrypt 2024*, Slides

MPC for Privacy Preserving Measurement, *ASCrypto 2023, co-located with Latincrypt 2023*, Slides

Standardizing MPC for Privacy-preserving Measurement, *RWC 2022*, YouTube recording. Please forgive the terrible recording. There was an AV issue during our session, the result of which is that only the Zoom recording survived

Quantifying the Security Cost of Migrating Protocols to Practice, *Crypto 2020*, YouTube recording

Interpretation of Provable Security for Cryptographic Practice, *PhD defense, delivered via Zoom*, YouTube recording

Partially specified channels, *CCS 2018*, YouTube recording

Hedging public-key encryption in the real world, *Crypto 2017*, YouTube recording

Service

PC RWC (Real World Crypto) 2027, PETS (Privacy Enhancing Technologies Symposium) 2027, PETS 2026, PETS 2025, SSR (Secure Standardisation Research) 2024, SSR 2023, and SSR 2022.

Paper review *Conference:* Asiacrypt 2016, Usenix 2017, Crypto 2019, Crypto 2020, CCS 2020, Eurocrypt 2025, and Eurocrypt 2027.

Journal: TDSC Vol. 15, No. 5.

Awards

Grants NSF: SaTC: CORE: Small: API-centric Cryptography (CNS-1816375).

Scholarships Benjamin A. Gilman International Scholarship Program, 2010.