isis agora lovecruft

curriculum vitae

personal

Github	https://github.com/isislovecruft
Twitter	@isislovecruft
Email	isis@patternsinthevoid.net
Blog	https://patternsinthevoid.net
Pronouns	they/them

corporate

I'm the founder and owner of a security and cryptography contracting and consulting firm, Patterns in the Void, Ltd. Past clientele have included The Tor Project, Signal Foundation, and others.

Company	Patterns in the Void, Ltd.
Title	Owner, Founder, and Chief Executive Officer
Address	297 Kingsbury Grade #100, P.O. Box 4470 Lake Tahoe, Nevada 89449 USA

professional experience

Applied Cryptographer **2019 – present**

Private Clientele, Consultant/Contractor

Cryptographic protocol design and review, microarchitecture and context specific cryptographic optimisations, custom signature and zero-knowledge proof design and research. Extensive research into signature malleabilities and design and optimisation of threshold and aggregate signature schemes. Developed a generalisation of Pippenger's algorithm for pre-computation of basepoint tables for scalar multiplication, leading to time-memory tradeoffs with 40% speed improvements on some hardware. Consulted and worked with a client who is shipping my Dalek Cryptography libraries to billions of users. Experience included working with and optimising the outputs of several systems for formal methods, including fiat-crypto and cryptol.

Applied Cryptographer **2018 – 2019**

Private Funder, Research Grant

Custom elliptic-curve cryptographic signature research, design, development, and optimisation.

Applied Cryptographer **2018**

Signal Foundation, Contractor

Custom zero-knowledge proof design and multi-architecture cryptographic development targeting numerous mobile devices and a web assembly API for a browser extension.

Applied Cryptographer **2016 – present**

Dalek Cryptography, Contractor

Research on elliptic curve cryptography, zero-knowledge protocol design, and anonymous credentials. Co-authored what is now the world's fastest cryptographic library, curve25519-dalek, including designing and prototyping the Ristretto prime-order group for use in practical, real-world sigma protocols. See the Dalek Cryptography Github organisation and our documentation on the Ristretto design. Significant effort was also put into writing two sets of extensive documentation for curve25519-dalek, one aimed at security engineers with light to moderate experience in cryptographic engineering, and the other aimed at fellow mathematicians and cryptographers.

Core Tor Software Developer **2010 – 2018**

The Tor Project, Contractor

Lead developer and maintainer of systems and components for Tor bridge distribution, which includes managing access to a database of all secret entrance relays in the Tor network, compartmentalising this data via hashring structures in order to restrict access by which distribution method is used, and securing the interfaces by which which Tor users may retrieve this data from adversaries hostile to Tor usage. Past work on identifying and patching user fingerprinting and security issues for Tor Browser. Ongoing efforts include improving Tor's circuit-level protocols and cryptography, designing and implementing an anonymous-credentials based system for censorship-resilient secret sharing, and reviewing RFC-like proposals for changes to the Tor protocol.

Software Developer and Security Consultant **2011 – 2012**

LEAP Encryption Access Project, Part-time

Development of several asynchronous servers, including a distributed and scalable transparently-encrypting remailer, which, at the time of design and implementation, handled seventeen million email users per day. The system, without modification, now handles over a hundred million daily users. Conducted security audits for systems components and dependencies, and filed several CVEs in widely used software, from Python's package manager to a GnuPG library in use by over thirty Bitcoin exchanges. Provided extensive consulting with respect to systems architecture and cryptographic engineering, including the design of an alternative OpenPGP keyserver.

Software Design Consultant **2011 – 2012**

Electronic Frontier Foundation

Worked with developers from the Electronic Frontier Foundation's (EFF) technical team to design a system for heuristic classification of benign network anomalies (e.g. due to NAT routers mangling packets) and malicious behaviours in TCP/UDP packet routing. The system, called Switzerland, can be used between two parties to determine if a malicious adversary is altering their digital communications, as well as to inform users of the types of malicious behaviours present in packet flows.

Software Developer and Distributed Systems Architect **2010 – 2012**

The Tor Project/Open Observatory of Network Interference

Reverse engineered the software and network testing methodologies of dozens of proprietary network testing and anomaly detection software tools. Designed the Open Observatory of Network Inference (OONI): a global, distributed platform for detection and measurement of network anomalies, including online censorship and both passive and active malicious behaviours. Designed and developed distributed backend systems for collection of measurement data which are now deployed on over 300,000 MLab and PlanetLab servers worldwide. Researched, designed, and published open specifications for effective methodologies for detection of anomalous behaviour. Designed and developed numerous tests which run on the OONI platform, including tests for misbehaving and poisoned DNS servers, captive portal detection and misbehaviour, and anomalous behaviours within Transport Layer Protocol (TLS) handshake and session resumption negotiation.

Cryptographic Protocol Researcher **2009 – 2012**
Open Whispersystems

Designed a modified Fully-Hashed Menezes-Qu-Vanstone protocol in an attempt to design a multi-party, forward-secret, end-to-end-encrypted, synchronous communications protocol with low overhead, such that it could feasibly be deployed over an SMS-based transport within Open Whispersystems flagship open source product TextSecure (now called Signal). Later, researched the feasibility and efficiency of applying the Multi-Party Off-The-Record (MPOTR) protocol. During this time, I also mentored several students in various secure mobile applications development projects, including aspects of protocol design, cryptography, and backend systems design, for Open Whispersystems.

Machine Learning Researcher **2008 – 2010**
Private Grant

Ported a fully back-propagational linguistic neural network from SPARC to x86 and made several optimisations allowing for parallelisation, developed an extensive interface for researchers to obtain data regarding neural states during execution, and constructed an OpenMPI-based cluster on which several research experiments on the neural network were conducted over the following two years.

Security and Cryptographic Design Consultant **2007 – present**
Private Clientele, Contractor

Security auditing and cryptographic design consulting to numerous clients, including several startups within the Bitcoin community. Conducted security audits for several S&P 500 companies to find exploitable vulnerabilities in networked applications, including banking and financial software, hypervisor and virtual machine management software, and a major browser.

Software Developer **2006 – 2009**
March Hare Communications Collective

Designed and developed open source mobile applications for grass-roots activists to conduct better crisis management and have capabilities for secure communication in political protest situations. The development was centered around the Android platform, but work was conducted alongside an iOS developer in order to produce a cross-platform solution. The applications included solutions for secure crisis mapping in hostile situations, secure location and event reporting, secure and metadata-free synchronous messaging, and a tool to remotely trigger the deletion of personal information on a device.

Various Contributions **2006 – present**
Volunteer

Volunteer contributions to numerous Open Source Software (OSS) projects, including Open Whispersystems, March-Hare Communications Collective, LEAP Encryption Access Project, Briar Project, Tahoe-LAFS, The Tor Project, the Electronic Frontier Foundation, and others.

mentorships & leadership roles

Dalek Cryptography **2018 – present**
Mentor

Assisted several high school through university students in writing their first patches to various Dalek Cryptography libraries.

Tor Internship **2017**

Mentor

Conducted a hiring and interviewing process, and then lead an intern in the development of several Rust libraries and tools for measuring the available bandwidth of Tor bridge relays.

Tor Summer of Privacy **2015**

Assistant Mentor

Assisted in the mentorship of a volunteer student project, called GetTor, which provides alternate mechanisms for securely downloading and installing Tor and/or Tor Browser in places where access to The Tor Project servers is censored.

Google Summer of Code **2014**

Mentor

Mentored a student in designing a new distribution system for Tor bridge relays to Tor users in censored regains via Twitter's HTTP API.

Google Summer of Code **2013**

Assistant Mentor

Mentored a student project to design and implement a censorship analysis system (https://explorer.ooni.torproject.org/world/) using data from the Open Observatory of Network Interference.

Open Whispersystems Spring Break of Code **2012**

Mentor

Mentored several students in asynchronous programming and scalable redesign of several backend servers for an encrypted voice call system, secure location sharing, and server-private contact list storage.

invited talks

Slides from my talks — including their LaTeX sources — are generally made available in a public Github repo, and video–when available–is provided on my YouTube channel.

!!Con West **2020**

University of California, Santa Cruz

Keynote presentation on implementing supersingular isogeny key encapsulation over a 434-bit finite field in handwritten 6510 assembly, including "illegal" opcodes, for a commodore 64.

Rustconf **2018**

Portland, Oregon

Co-presented a talk on incrementally rewriting the Tor network daemon in Rust and the security vulnerabilities and challenges we found and faced along the way.

Noisebridge **2017**

San Francisco, California

Presented a history of security vulnerabilities and side-channel attacks on real-world cryptographic libraries, along with the countermeasures we took to avoid these problems in the design of the Dalek Cryptography libraries.

Rustconf **2017**

Portland, Oregon

Co-presented a talk on creating curve25519-dalek, which is currently the world's fastest cryptographic library and is in use by billions of people.

University of Waterloo **2016**

Waterloo, Ontario, Canada

Invited talk presenting Hyphae, , a censorship-resistant system for using zero-knowledge proof-of-social-graphs and private behaviour tracking via anonymous credentials based on algebraic MACs, to the Cryptography, Security, and Privacy (CrySP) department.

Radboud Universiteit **2016**

Nijmegen, Netherlands

Guest lecture for the Advanced Network Security course on the history and current status of mixnets, anonymity networks, and anonymous communcations systems, given at Raboud Unversiteit in Nijmegen to students following the TRU/e Computer Security Master's Programme. Afterwards, I freely posted the video recording on YouTube, where it received 4,000 views within the first week.

Radboud Universiteit **2016**

Nijmegen, Netherlands

Talk given to graduate students, researchers, and faculty of the Digital Security group at the Institute for Computing and Information Sciences at Raboud Unversiteit in Nijmegen, the Netherlands, concerning my work with The Tor Project on protecting Tor bridges from discovery by nation-state adversaries.

EI/ψ **2015**

Utrecht, Netherlands

I spoke to the Cryptography Working Group at the Eindhoven Institute for the Protection of Systems and Information (part of Wiskunden en Informatica at Technisches Universiteit Eindhoven) in Utrecht, the Netherlands, about the cryptography for my current work on using pairing-based anonymous credential schemes for social distribution of Tor bridge relays.

ThoughtWorks **2015**

Berlin, Germany

I spoke about Tor's circuits, path selection, and hidden services, (and the basics of the cryptography for those things) at a women's-only event held at ThoughtWorks' Werkstatt Berlin space.

FOSDEM: FOSS Developers' European Meeting **2013**

Brussels, Belgium

I spoke on mine and my team's work to create a peer-reviewed taxonomy for discussion of surveillance and censorship, as well as a free and open source software toolset, called the Open Observatory of Network Interference (OONI), for producing open data. This talk covered the vision of OONI as well as technical details of our tools. (See https://archive.fosdem.org/2013/schedule/event/ooni/ for recordings.)

DebConf'13: Debian Developers Conference **2013**

Vaumarcus, Switzerland

Workshop with Debian Developers on tactics for higher-security package management, including an introduction to software reproducible builds for Debian package maintainers.

Google **2012**

Brussels, Belgium

Talk to Google's Internal Security Team and the Measurement Lab (MLAB) team regarding secure

distributed systems design and measurement data protection and integrity, with respect to the deployment of a global distributed network anomaly detection system on 300,000 machines.

University of Washington, Olympia **2009**
Olympia, Washington

Lecture and workshop for journalism students in the Department of Communication at the University of Washington, on the topic of secure communications for journalists and their sources.

skills

Languages	Rust, C/C++, Python, Swift, Julia, Go, x86/ARM/MIPS/6510 ASMs, Common Lisp, Bash, Lua, Javascript, HTML5, CSS3, and Java
Software	Low- to High-Level Cryptographic Design, Cryptographic Engineering, Network Programming, Asynchronous Programming, Distributed Systems Design, Misuse-Resistant API Design, Security Best Practices, Reverse Engineering

references

Available upon request