Alex Davidson

Curriculum Vitae

✍ [redacted]
☎ [redacted]
✉ **alex.davidson92@gmail.com**
★ **DBLP**, **Google Scholar**, **GitHub**
↗ **alxdavids.xyz**
❝ **English** (native), **Portuguese** (basic)
✎ References available upon request

Summary

Assistant Professor and scientific researcher with notable contributions in the design, implementation, and standardisation of globally-used privacy-preserving cryptography and Internet protocols.

Experience

February 2023 – Present

DI, FCT NOVA, Universidade Nova de Lisboa

Professor Auxiliar

May 2021 – November 2022

Brave Software (Remote, Lisboa, Portugal)

Cryptography Researcher

Performing research in areas of privacy-preserving cryptography, usable security, and private blockchain-based technologies.

November 2020 – May 2021

SPAC, LIP (Lisboa, Portugal)

Post-doctoral Researcher

Post-doctoral researcher hosted within the ERC-funded **FARE** project in the **Social Physics and Complexity Lab**, led by **Prof. Joana Gonçalves de Sá**.

October 2018 – October 2020

Cloudflare, Inc. (Lisboa, Portugal)

Cryptography Researcher & Engineer

Research lead for design, development, and **standardisation** of the **Privacy Pass protocol**. Main research focuses in the area of privacy-preserving cryptography and usable security.

February 2018 – May 2018

NTT Secure Platform Laboratories (Tokyo, Japan)

PhD Research Intern

July 2017 – October 2017
June 2016 – September 2016

Cloudflare, Inc. (London, UK)

PhD Research Intern

PhD intern within Cloudflare Research and Cryptography team.

August 2013 – August 2014

The Phoenix Partnership (Leeds, UK)

Software Developer

Education

2014 – 2018

PhD in Cyber Security

Royal Holloway, University of London, UK

Member of 2^{nd} cohort of students in the **Centre for Doctoral Training in Cyber Security**. Supervised by **Prof. Carlos Cid**.
Thesis title: **Computing Functions Securely: Theory, Implementation and Cryptanalysis**

2010-2013

BSc Hons. Mathematics

University of Warwick, UK

Selected Publications

Tara Whalen et al. "Let The Right One In: Attestation as a Usable CAPTCHA Alternative". In: *Symposium on Usable Privacy and Security (SOUPS)* (2022). **Link**.

Alex Davidson et al. "STAR: Distributed Secret Sharing for Private Threshold Aggregation Reporting". In: *Preliminary acceptance to ACM CCS* (2022). **Link**.

Martin R Albrecht et al. "Round-optimal Verifiable Oblivious Pseudorandom Functions From Ideal Lattices". In: *IACR PKC* (2021). **Link**.

Alex Davidson et al. "Adaptively Secure Constrained Pseudorandom Functions in the Standard Model". In: *IACR CRYPTO* (2020). **Link**.

Alex Davidson et al. "Privacy Pass: Bypassing Internet Challenges Anonymously". In: *PoPETS* (2018). **Link**.

Other academic contributions

Organising committees: **IMACC 2019**.
Peer reviews: **Eurocrypt** (2017-2019, 2021), **Asiacrypt** (2018, 2020), **Crypto** (2018, 2020), IMACC (2017, 2019), **PoPETS** (2019, 2021), USENIX 2017, **Design Codes and Cryptography Journal**.

Internet standards contributions

STAR: Distributed Secret Sharing for Private Threshold Aggregation Reporting (draft-dss-star)

Oblivious Pseudorandom Functions using Prime-Order Groups (draft-irtf-cfrg-voprf)

Privacy Pass Protocol (draft-ietf-privacypass-protocol)

Privacy Pass Architecture (draft-ietf-privacypass-architecture)

Open source research software

github.com/privacypass/challenge-bypass-extension
JavaScript WebExtension for anonymously bypassing Internet challenges using Privacy Pass protocol.

github.com/brave/sta-rs
Implementation of **STAR protocol** used for sending private analytics information in various products at Brave Software.

Technical expertise and skills

Programming languages	Rust, Go, Typescript/Javascript, Lua, Java, Python, Sage.
Tooling	Linux, MacOS, Windows, Docker, Kubernetes, Chromium, AWS, GCP, Prometheus, SQL, nginx.

Outreach

Official blog posts intended for wide, non-technical audience.

2019	**Supporting the latest version of the Privacy Pass Protocol**
2019	**Inside the Entropy**
2019	**Preventing Request Loops Using CDN-Loop**