

Alex Davidson

Curriculum Vitae

📍 Rua Marques da Silva 33, S/C B
Lisboa, Portugal – 1170-222

☎ +351 963452432

✉ alex.davidson92@gmail.com

★ **DBLP, Google Scholar, GitHub**

🔗 alxdavids.xyz

“ **English** (native), **Portuguese** (basic)

📄 References available upon request

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**

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 2nd 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**