

Enrique Larraia, PhD.



elarraia@gmail.com

Phone: +34 747 853 987

DBLP: Enrique Larraia. **ORCID:** 0009-0004-6801-0667

GitHub: github.com/larraia

LinkedIn: linkedin.com/in/elarraia

EXPERIENCE

Senior Cryptography Engineer

Openchip (Barcelona, Spain)

2025 – present

Senior Cryptography Researcher

Heliax (Switzerland – remote position)

2024 – 2025

Design and development of the Anoma protocol. Including private message retrieval with **Fuzzy Message Detection**, fast on-chain verification via **proof aggregation**, and design of **light arithmetic circuits** for efficient SNARK provers.

Cryptography Researcher

nChain (London, UK – remote position)

2021 – 2024

Filed patents and **published academic articles** on NFTs, auction schemes, Bitcoin redaction, and more topics. Code optimizations in Script language for **ZKP on-chain applications**. Lead of the internal Cryptography Working Group.

Product Owner & Researcher

Scyt Electronic Voting (Barcelona, Spain)

2018 – 2021

Design and analysis of e-voting protocols deployed in national elections in several countries. **Team lead** of the Cryptography library. **Writing up specifications**.

Technical Consultant

Sistemas Informaticos Abiertos (Barcelona, Spain)

2017 – 2018

Consultancy on identity management for major Spanish Companies.

Post Doctoral Researcher

Royal Holloway University. (London, UK)

2015 – 2016

Conducting research on Cryptography. Focusing on Multilinear Maps and Indistinguishability Obfuscation.

EDUCATION

PhD in Cryptography

University of Bristol, UK.

Research on **Multi Party Computation**. Also, FHE, Secret Sharing and Oblivious Transfer. Participated in the design of the **SPDZ family**.

Thesis supervised by **Prof. Nigel P. Smart**.

Msc with Honors

Royal Holloway University, UK.

Mathematics of Cryptography and Communications.

Licentiate in Mathematics

Universidad Complutense de Madrid

SKILLS

Software development Production-ready code in **Rust**. Code reviews in **Java, C++**.

Frameworks and Tooling **ZKP:** RISCO, Arkworks, Cairo, and more. Familiarity with **NIST standards**, LaTeX, **Rust**, Git. Familiarity with Python.

Learning and knowledge sharing

- Delivering complex content to both technical and non-technical audiences.
- Ability to parse and digest complex academic articles.
- **Continuously updated with state of the art on cryptography.**

Experience leading teams and advising end clients.

CRYPTOGRAPHY EXPERTISE

Public-key and symmetric cryptography. ECC.

Advanced cryptography. Zero-knowledge proofs (**STARKs, SNARKs**), Multi Party Computation (**MPC**), and others like Secret Sharing. Oblivious Transfer. Also familiarity with Fully Homomorphic Encryption (**FHE**), Post Quantum and Lattice-based constructions.

Provable security. Strong expertise on security analysis of cryptographic primitives.

SELECTED PUBLICATIONS

2024 (ICBC). “How to Redact the Bitcoin Backbone Protocol”. Mehmet Sabir Kiraz, et al In: *IEEE International Conference on Blockchain and Cryptocurrency*.

2023 (ACNS Workshops) “NFT Trades in Bitcoin with Off-Chain Receipts”.) Mehmet Sabir Kiraz, et al.

2023 (Financial Cryptography Workshops). “Publicly Verifiable Auctions with Privacy”. Paul Germouty et al.

2021 (Remote eVoting. CANS). “How (not) to Achieve both Coercion Resistance and Cast as Intended Verifiability” Tamara Finogina,et al.

2021 (In J. Cryptol. 34(3): 34). “High-Performance Multi-party Computation for Binary Circuits Based on Oblivious Transfer”. Sai Sheshank Burra et al.

2018 (Public Key Cryptography). “Graded Encoding Schemes from Obfuscation”. Pooya Farshim et al.