Thomas Kerber

✉ thomas@kerber.uk • 🌐 drwx.org

Education

The University of Edinburgh **Edinburgh**
PhD in Cryptography *2017–2021*
Thesis: **Foundations of Decentralised Privacy** 🔗
Supervised by Prof. Aggelos Kiayias & Dr. Markulf Kohlweiss.

The University of Edinburgh **Edinburgh**
BSc Computer Science *2013–2017*
With first-class honours, and a course average of 85%.

Experience

Input Output Global **Remote**
Technical Architect *From Mar. 2021*
Responsible for technical and cryptographic decisions on an unannounced project.

Input Output Global **Remote**
Researcher *Sep. 2017–Feb. 2021*
PhD affiliation and related consulting.

The University of Edinburgh **Edinburgh**
Teaching Support *2015–2020*
Teaching assistant in for the *Computer Security* 3rd year course, as well as tutoring for the *Processing Formal and Natural Languages* 2nd year course, and the *Introduction to Computation* 1st year course.

The University of Edinburgh **Edinburgh**
Research Intern *Jun.–Jul. 2016*
Analysing low-level security of SIM cards and smartcards.

Research

Peer-Reviewed

Composition with Knowledge Assumptions 🔗
Thomas Kerber, Aggelos Kiayias, Markulf Kohlweiss
2021 CRYPTO Conference

Mining for Privacy: How to Bootstrap a Snarky Blockchain 🔗
Thomas Kerber, Aggelos Kiayias, Markulf Kohlweiss
2021 Conference on Financial Cryptography and Data Security

Kachina – Foundations of Private Smart Contracts 🔗
Thomas Kerber, Aggelos Kiayias, Markulf Kohlweiss
2021 IEEE Computer Security Foundations Symposium

Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake
Thomas Kerber, Aggelos Kiayias, Markulf Kohlweiss, Vassilis Zikas
2019 IEEE Symposium on Security and Privacy

Technical Knowledge

Expert: Distributed consensus, Blockchain, {Composable, Simulation-based} security, Git, Rust, Linux

Experienced: Zero-knowledge, Adaptive security, C, Python, Ethereum, NixOS

Some experience: Java, Ruby, Go, Haskell, Agda, Scala, PHP, Javascript, Idris, Racket

Languages

English: Native

German: Native

Awards

The University of Edinburgh *2017*
Jointly received the class prize for best overall performance in the degree of BSc. Computer Science.

The University of Edinburgh *2017*
Jointly received the JP Morgan prize for best final year performance in the School of Informatics.

Build-it, Break-it, Fix-it *2016*
Second place builder in the world-wide competition.

Deloitte CTF *2016*
On the runner up team of the UK-wide CTF competition.

Scottish Universities Cyber Challenge (Cyber Challenge UK) *2016*
On the runner up team.

The University of Edinburgh *2016*
Received the Morgan Stanley award for the top performing student in the penultimate year in Computer Science.

The University of Edinburgh *2016*
Received the Google award for the best computer science large practical.