# MATTHEW KLEIN

CRYPTOGRAPHY ENGINEER ⚲ LONDON, UNITED KINGDOM 📞 +447866408597

## DETAILS

London
United Kingdom
+447866408597
matthewklein345@gmail.com

## LINKS

LinkedIn

Github Portfolio

Personal Site

## SKILLS

Rust

C++

TypeScript

Cryptography

Compilers

## LANGUAGES

English

Hebrew

## PROFILE

Software engineer currently at Nethermind.

Passionate about well written, clean code and useful software.

I have experience in applied cryptography, compilers and machine learning.

Lover of all things zero-knowledge.

## EMPLOYMENT HISTORY

**Cryptography Engineer at Nethermind, Remote**
October 2024 — Present

**Cryptography Research Intern at Nethermind, Remote**
June 2024 — September 2024

Researching, implementing and optimising cryptographic primitives and zero-knowledge systems. Mostly developing in Rust programming language.

## EDUCATION

**Computer Science, King's College London, London**
September 2021 — August 2024

First class honours in Computer Science. Focusing on compilers and artificial intelligence.

**Talmudic College, Jerusalem**
August 2017 — September 2021

**Hasmonean High School, London**
September 2010 — August 2017

Graduated with A Levels in Maths (A*), Further Maths (A*), Chemistry (A), Physics (A) and Biblical Hebrew (A).

## PROJECTS

**ZK engineering**
January 2025 — Present

Spearheaded implemention of Zinc protocol, a new SNARK over the integers.

**Lattice Cryptography**
June 2024 — Present

Core contributor to the latticefold repo, which implements a lattice based folding scheme. Contributed to Nethermind's PQ signature project, focusing on Falcon signatures. Appeared on the Zero Knowledge podcast, to discuss my lattice based cryptography research.

**Compilers for small languages**
October 2023 — January 2024

Part of university coursework. Compiling an imperative language to run on the JVM and a functional language to LLVM-IR. Coursework written in Scala programming language.

In addition, for my dissertation I wrote a functional programming language that has date and time data as primitive types.