

Cryptography consultant and CryptoHack founder, interested in applying my strong skills in mathematics, programming, and analytic problem-solving to defining, implementing and researching cryptographic protocols.

EXPERIENCE

CryptoHack Co-Founder 2020-*present*

- Co-founder of [CryptoHack.org](https://crypto.hack.org), a gamified learning environment with an emphasis on breaking insecure implementations of modern cryptography
- Designed lessons and challenges exploring weaknesses in common protocols
- Currently host 150+ challenges to 33,000+ users with a total of 340,000+ solutions submitted
- Recently partnered with ETH, to collaboratively design a set of PQcrypto challenges

NCC Group Managing Security Consultant 2021-*present*

- Performed static code analysis of a wide range of cryptographic code and protocols
- Wrote detailed audit reports, paired with customer presentations communicating security findings
- Published research posts on cryptographic security topics, e.g. [Bit security of pairing-friendly curves](#)
- Regularly gave internal presentations, focused on the intersection of maths and cryptography

Northrop Grumman Software Engineer 2020-2021

- Researched and developed security tools, delivered with accompanying technical white papers
- Wrote lectures and lab environments on web exploitation designed for accelerated learning of a customer's growing workforce

University of Liverpool Ph.D. Student 2016-2020

- Communicated my research at international conferences, giving seminars and designing posters
- Published three research papers in JHEP, the top journal in my field ([2111.09017](#)) ([1905.09167](#)) ([2008.06929](#))
- Taught popular classes on Mathematics and Physics to undergraduate students
- Founded and partook in a PhD seminar series, broadening my understanding of advanced topics

EDUCATION

Ph.D. Department of Mathematics, University of Liverpool 2016-2020

M.A.St. Master's in Mathematics, University of Cambridge (First Class) 2014-2015

M.Phys. Master's in Physics, University of Exeter (First Class) 2010-2014

SKILLS

- Exposure to **cryptanalysis** and protocol implementation from self-study, currently focused on post-quantum asymmetric cryptography
- Proficient with **Python**, **SageMath**, familiar with **C**, **C++**, **Rust** and **Go**
- Particularly interested in elliptic curve cryptography and the recent developments in isogeny graphs
- Active CTF player highly competitive Organizers team (Global rank #2 2021)

PRIZES

- GTA Studentship funding Ph.D. research 2016-2020
- Gertrude Mather Jackson prize for highest maths performance in Girton College 2015
- Jubilee and Millhayes Science Scholarships for academic excellence 2010-2014