Design and Analysis of Secure Cryptographic Protocols

Start Date: 21 September 2026

Application Deadline: 17th April 2026

Royal Holloway, University of London is inviting applications for a 3.5-year PhD studentship in Cryptography.

Project Overview

The successful candidate will work on the design, development, and rigorous analysis of cryptographic protocols, with a particular focus on privacy and end-to-end verifiability.

The project emphasises formal modelling and provable security, aiming to develop precise definitions, threat models, and proofs that capture the security and privacy properties required in complex, real-world settings. A key objective is to bridge the gap between abstract cryptographic models and the concrete requirements of users, ensuring that formal guarantees meaningfully reflect how systems are expected to be used and trusted in practice.

The research will consider a range of application domains, including electronic voting, auctions, peer-review systems, anonymous credential schemes, and delay-based signatures. The candidate will investigate both foundational and applied questions, such as defining appropriate security notions, constructing protocols with rigorous proofs, and analysing their resilience under realistic adversarial models. The project is well suited to applicants with interests in modern cryptography, particularly those motivated by formal modelling, provable security, and the development of robust, trustworthy systems grounded in clear and accurate assumptions.

Eligibility and Details of the Award

We seek applicants with a strong background in mathematics and/or computer science. Familiarity with cryptography, number theory, probability theory, or computational algebra would be advantageous.

This 3.5-year studentship is open to UK Home fee-status students only. The award covers Home-rate tuition fees and provides a tax-free stipend at the UKRI rate, which increases annually in line with UKRI guidance. For the 2026/27 academic year, the stipend will be £23,805, including £2,000 London Weighting. The studentship may be undertaken full-time or part-time.

How to Apply

Interested candidates should send:

- a CV, and
- a motivation letter

to Dr Elizabeth Quaglia (Elizabeth.Quaglia@rhul.ac.uk)

Further Information

This studentship is part of Dr Elizabeth Quaglia's EPSRC-funded Open Plus Fellowship on Understandable Cryptography. The fellowship also funds postdoctoral researchers, meaning the successful candidate will join an active research team and a broader programme dedicated to advancing impactful cryptographic research.

The student will also benefit from being part of the Cryptography Group at Royal Holloway (https://cryptography.isg.rhul.ac.uk/), a world-leading centre for research and teaching in cryptography.