

Engineering and Physical Sciences Research Council Doctoral Landscape Award

PROJECT TITLE: End-to-End Verification of Security Protocols in Isabelle

Lead Supervisor Details:

Diego Marmsoler

Webpage: <https://marmsoler.com/>

Email address: d.marmsoler@exeter.ac.uk

Additional Supervisor(s): Achim Brucker <A.Brucker@exeter.ac.uk>

Project details: Modern security systems often rely on complex software that translates programs into forms that can be checked automatically. To trust such systems, it is not enough to verify the underlying security protocol: we must also know that the checked representation faithfully captures the intended program.

This PhD project will investigate how theorem proving can be used to establish such end-to-end guarantees. The work will focus on verified translations between programs and the representations used by security protocols, using Isabelle/HOL as the main formalisation environment. Zero-knowledge proof systems, including STARK-style protocols, will provide one important application area.

The central research question is how to connect programs, compilation and cryptographic protocols so that correctness and security guarantees can be composed and reused. The project spans formal methods, programming languages, cybersecurity and cryptography, with scope to shape its direction according to the student's interests.

The student will develop and verify semantic models and compilation techniques in Isabelle/HOL, showing that generated representations faithfully capture source-program behaviour. The longer-term goal is to connect these results with mechanised security arguments for the underlying verification protocol.

The supervisory team brings expertise in Isabelle, formal methods, smart-contract verification and security-protocol verification.

The project is suitable for candidates interested in formal verification, programming languages, cybersecurity, cryptography, compilers or theorem proving. Prior experience with Isabelle or zero-knowledge proofs is useful but not essential.

Project specific entry requirements: N/A

Potential PhD programme of study: PhD in Computer Science

Department: Computer Science

Location: Streatham (Kathleen Booth Building)

Please direct project specific enquiries to: Please contact lead supervisor:
d.marmsoler@exeter.ac.uk



Engineering and Physical Sciences Research Council Doctoral Landscape Award

Please ensure you read the entry requirements for the potential programme you are applying for.

To Apply for this project please click on the following link - [**APPLY HERE**](#)



University
of Exeter

Engineering and Physical Sciences Research Council Doctoral Landscape Award