Title: Localised Cryptography

Type of award	PhD Research Studentship
Department	Computer Science
Scholarship Details	Provided by HM Government , the scholarship covers full UK PhD tuition fees and a tax-free stipend of approximately £22,000 p.a. (subject to confirmation)
Duration	3.5 years
Eligibility	Home UK Nationals only
Start Date	October 2017

PhD Topic Background/Description

Context: Cryptography underpins much of the security of computing and communication infrastructures on which modern society increasingly relies. Yet, ensuring that systems that rely on cryptography meet their desired goals is notoriously difficult. There is ample space for errors, ranging from the overall design of the system down to the concrete implementation and the underlying computational platforms on which it is deployed. To reduce the risk of designing and subsequently deploying insecure applications, modern security research advocates the use of mathematical models. The idea is to provide mathematical formalizations for what is a system, what constitutes a successful breach against it, and then prove that such breaches are not possible.

Project: The project aims to develop a framework that consists of a tool that will provide support for cryptographers both in designing and verifying cryptographic proofs. The key features that will distinguish our approach from other existing ones is that we aim to keep the language for specifying and reasoning about systems as close as possible to the typical language that cryptographers use in their proofs nowadays, will develop a simplified methods for reasoning about systems at more abstract levels than usual.

The successful applicant will be based in a vibrant research group, with more than 17 PhD students and 6 postdoctoral researchers working in a variety of topics related to cryptography.

Further Particulars

Candidate Requirements

A minimum 2.1 honours degree or equivalent in Computer Science or Mathematics.

Basic skills and knowledge required:
The ideal candidate will have a background in programming language semantics, complexity theory, or cryptography.

Informal enquiries

For informal enquiries, contact Dr. Bogdan Warinschi, csxbw@bristol.ac.uk

For general enquiries, please email gsen-pgrs@bristol.ac.uk

Application Details

To apply for this studentship submit a PhD application using our online application system [www.bristol.ac.uk/pg-howtoapply]

Please ensure that in the Funding section you tick "I would like to be considered for a funding award from the Computer Science Department" and specify the title of the scholarship in the "other" box below with the name of the supervisor, Dr Warinschi.

Closing date for completed applications 31 March 2017.