Basic details

Type of Opportunity	PhD Project
Number of studentships	1

Application deadline date	TBA

Institution(s)	University of Birmingham
School(s)	School of Computer Science

Listing details

Supervisor(s)	Dr Sujoy Sinha Roy, Dr Christophe Petit and Dr. Flavio Garcia.
Project title	Hardware Implementations of Isogeny-based Protocols
Funding availability	PhD funding for UK students only
Name of funding awarded	The position is funded by the UK Government. Begins October 2019.

Project description

Post-quantum cryptography aims at developing new security protocols that will remain secure even after powerful quantum computers are built. Isogeny problems are among the few "hard problem" candidates that are currently considered for post-quantum cryptography. Isogeny-based protocols now include key exchange, public key encryption and signatures, so essentially all basic cryptographic primitives necessary for most common applications such as TLS communications. Isogeny-based key agreement protocol SIKE is a candidate submission in the ongoing post-quantum cryptography standardization event from the American National Institute for Standards and Technologies (NIST).

Isogeny-based cryptography offers one of the most promising approach for post-quantum cryptography and achieves forward secrecy in communications, a highly desirable feature currently available in TLS protocol suite. Protocols based on isogeny problems enjoy very small public keys compared to all other post-quantum candidates, a very useful feature since those keys are routinely transmitted as part of public key certificates. While all these properties make isogeny-based cryptography very appealing, it is also a relatively new field. As a result, it is less mature than other post-quantum candidates, and arguably not ready yet to meet the requirements of real-life security applications. In particular, there is very little work on hardware implementations of isogeny-based protocols.

The main goal of this studentship is to develop optimized, side-channel protected hardware implementations of isogeny-based protocols.

The student will be integrated within the University of Birmingham's Centre for Cyber Security and Privacy and they will collaborate with more experienced researchers on this research program. They will be supervised by Dr. Sujoy Sinha Roy, Dr. Christophe Petit and Dr. Flavio Garcia. All three are members of Birmingham's Academic Center of Excellence in Cyber security.

More information: https://www.cs.bham.ac.uk/~sinharos/

Funding notes

The candidate must be a UK national as required by the funding agency.

2:1 Honours undergraduate degree and/or postgraduate degree with Distinction (or an international equivalent) in Electrical and Electronics Engineering, Computer Science, Mathematical Engineering or closely related discipline. The ideal candidate for this position will be familiar with low-level programming, hardware architecture design and cryptography, but other candidates with a strong academic record will also be considered.

Total stipend to student: £22,000 (year1), £22,500 (year2), £23,000 (year3), £11,750 (6 months of year4). The stipend is tax free. This is a research position with limited or no teaching requirements.

Contact for enquiries

Name of supervisor	Sujoy Sinha Roy, Christophe Petit and Flavio Garcia
Web page	https://www.cs.bham.ac.uk/~sinharos/ https://www.cs.bham.ac.uk/~petitcz/ http://www.cs.bham.ac.uk/~garciaf/
Email address	s.sinharoy@cs.bham.ac.uk, C.Petit.1@cs.bham.ac.uk, f.garcia@cs.bham.ac.uk
Phone number	