ROYAL
HOLLOWAY
UNIVERSITY
OF LONDON

JOB DESCRIPTION

Job Title:	Postdoctoral Research Assistant in Cryptography
Department / Unit:	Faculty of Science
Grade:	7
Accountable to:	Principle Investigator

Purpose of the Post

Background

As a result of a collaboration between L3 TRL Technology and Royal Holloway, University of London, applications are invited for a research assistant position in the Information Security Group (ISG) at Royal Holloway to work in the area of post-quantum cryptography.

Post-Quantum (PQ) cryptography refers to cryptographic algorithms and schemes that are expected to be resistant to cryptanalytic attacks based on quantum computers. Examples include lattice-based encryption and signature schemes, code-based public-key cryptosystems, Multivariate Quadratic (MQ) cryptosystems, and hash-based digital signature schemes. The goal of this industry-funded two-year project is to investigate and propose novel methods and techniques for hardware implementation of popular and promising post-quantum cryptographic schemes.

The successful applicant will be based in the ISG at Royal Holloway, and will work with Prof Carlos Cid, Dr Martin Albrecht and other members of the ISG, in the research of efficient and secure hardware implementation of post-quantum cryptographic schemes. An initial focus will be on the FPGA implementation aspects of lattice-based key exchange schemes (e.g. RLWE schemes and variants) and code-based key exchange schemes (e.g. McEliese cryptosystem and variants). They will consider the specific mathematical structure and features of these schemes, and will investigate the most suitable algorithmic and parameter choices for FPGA implementations. Moreover, potential trade-offs involving implementation costs, speed and scalability, will be evaluated, considering for example the deployment in particular environments (e.g. high-performance).

We are looking for a candidate with a PhD degree and strong background and experience in FPGA implementation, ideally of cryptographic algorithms. The post will last for two years and the ideal candidate should be able to start on or near the 1st of October 2017.

Established in 1990, the Information Security Group at Royal Holloway was one of the first dedicated academic groups in the world to conduct research and teaching in information security. The ISG is today a world-leading interdisciplinary research group with 20 full-time members of staff, 10 post-doctoral research assistants and over 50 PhD students working on a range of subjects in cyber security, in particular cryptography.

Key Tasks

Main Responsibilities

The main responsibility of the post is to conduct original research in cryptography (as directed by Prof Carlos Cid and Dr Martin Albrecht). The project will include a range of activities, including:

- Carry out independent research on the implementation of post-quantum cryptographic algorithms and schemes.
- Disseminate novel research results through written papers, reports and presentations.
- Any other duties as required by the line manager or Head of Department that are commensurate with the grade.

Other Duties

The duties listed are not exhaustive and may be varied from time to time as dictated by the changing needs of the College. The post holder will be expected to undertake other duties as appropriate and as requested by his/her manager.

The post holder may be required to work at any of the locations at which the business of Royal Holloway is conducted.