

JOB DESCRIPTION

Job Title:	PDRA in Cryptography
Department / Unit:	Information Security Group (ISG)
Grade:	RHUL 7, Spine Point 35
Accountable to:	Dr. Martin Albrecht
Purpose of the Post	
<p>Together a European consortium of academics and industry, Dr. Martin Albrecht has been awarded an EC-funded grant to work on the topic of privacy preserving post-quantum systems from advanced cryptographic mechanisms using lattices (H2020 PROMETHEUS). At Royal Holloway, the focus within this project is on cryptanalysis of lattice schemes as well as prototype implementations of building blocks and protocols for privacy preserving systems.</p> <p>The PDRA will work with Dr. Albrecht, Dr. Player and researchers from the PROMETHEUS project (ENS Lyon; Orange SA; CWI Amsterdam; Ruhr-Universität Bochum; ScytI Secure Electronic Voting, S.A.; Thales Communications & Security S.A.S.; TNO; Universitat Politècnica de Catalunya · BarcelonaTech; Université de Rennes 1; Weizmann Institute of Science).</p>	
Key Tasks	
<p>The project will involve a range of activities, including the following:</p> <ul style="list-style-type: none"> • Conducting research in lattice-based cryptography in collaboration with Dr. Albrecht, Dr. Player and the other team members; • Writing papers, reports and presentations; • Attending conferences, workshops, and summer schools to disseminate the research; • Assisting in arranging project meetings and workshops; • Any other duties as required by the line manager or Head of Department that is commensurate with the grade. <p>As the needs of the College change so the above job profile, duties and location of the role within the College will be adjusted accordingly.</p>	
Other Duties	
<p>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.</p> <p>The post holder may be required to work at any of the locations at which the business of Royal Holloway is conducted.</p>	