PhD/Doctoral Studentship

Title: A Computational Algebra Approach to Learning with Errors

Supervisors: Dr Carlos Cid and Prof. Sean Murphy

Start Date: September 2013 **End Date**: March 2017

The Government Communications Headquarters (GCHQ) in Cheltenham has agreed in principle to sponsor a PhD/Doctoral Studentship to be held with the Information Security Group of Royal Holloway (University of London) in the area of the application of computational algebra techniques in the analysis of stochastic cryptographic equation systems.

The studentship is only open to UK nationals and the successful candidate will be required to spend in the region of 2 - 4 weeks per year at GCHQ headquarters in Cheltenham. To be considered for this studentship, candidates must therefore be prepared to undergo GCHQ's security clearance procedures.

The studentship will be funded for a period of 3.5 years. GCHQ will cover the costs of university fees and will provide an annual stipend to the student of £15,590 per annum (corresponding to the National Minimum Stipend plus London allowance), plus an additional sum of £7,000 per annum.

Stochastic cryptographic equations systems arise naturally in many areas of cryptology, including important well-established areas of cryptology, such as symmetric cryptanalysis and side-channel cryptanalysis, as well as important emerging areas, such as lightweight cryptography, post-quantum cryptography and homomorphic encryption. The research project aims to study the application of computational algebra techniques in the analysis of such stochastic cryptographic equation systems, in particular those arising from schemes based on the "Learning with Errors" problem.

Applicants should have or be expecting to obtain a first class honours degree or a masters degree in Mathematics or similar subject. In particular, applicants would be expected to have interests and strengths in one or more of the areas of algebra, statistics or cryptology, as well as having strong programming skills.

Prospective applicants should first make informal enquiries to Dr Carlos Cid (carlos.cid@rhul.ac.uk) or Prof. Sean Murphy (s.murphy@rhul.ac.uk).