PhD/Doctoral Studentship

Title: Randomness in Cryptography – Theory Meets Practice

Supervisor: Prof. Kenny Paterson

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 theoretical and practical aspects of randomness in Cryptography.

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.

Randomness is needed in almost all cryptographic systems and protocols. Indeed, the existence of suitable random sources is taken for granted in much of the research literature in cryptography, with formal security analyses of cryptographic schemes failing if perfect randomness assumptions are not met. Yet there have been several prominent recent examples of randomness failures having potentially severe security consequences. This project aims to take a fresh look at the role of randomness in cryptography, from both applied and theoretical perspectives. We will explore two main strands. In the first strand, we will focus on the analysis of existing random number generators, trying to find attacks or provide formal security analyses of generators. In the second strand, we will study what can be done to "hedge" cryptographic primitives against various forms of "bad" randomness.

Applicants should have or be expecting to obtain a first class honours degree or a masters degree in Computer Science, Mathematics, or a closely related subject. The ideal applicant would have some existing knowledge of cryptography, complexity theory and algorithms, and have strong programming skills.

Prospective applicants should first make informal enquiries to Prof. Kenny Paterson (kenny.paterson@rhul.ac.uk).