



Quantum cryptanalysis of post-quantum cryptographic schemes

Start Date: January 2027

Application Deadline: 30 November 2026

Interview Date: TBC

Royal Holloway, University of London and The National Physical Laboratory (NPL) are inviting applications for a joint PhD position in post-quantum cryptography.

Project Overview

Traditional public-key cryptography (PKC) relies on the difficulty of solving certain (presumed) hard problems. These problems are hard to solve with existing classical computers, but if a large-scale quantum computer is built, existing deployments of traditional PKC would become insecure. In contrast, post-quantum cryptography (PQC) concerns cryptosystems that are based on different problems, that are believed to be hard to solve using both classical and quantum computers; while Quantum Key Distribution (QKD) directly uses quantum physics to securely establish a shared symmetric key. PQC and QKD could be used, separately or in combination, to provide security even against an adversary with a large-scale quantum computer.

In 2024, the US National Institute of Standards and Technology (NIST) announced a suite of post-quantum cryptographic standards, and since then organisations globally have begun to migrate their systems to PQC. One important question in standardising and deploying a PQC primitive is to set parameters that balance security and efficiency requirements. In addressing this task, it is important to understand the available algorithms, classical or quantum, that could be used by an adversary to solve the underlying hard problem. Moreover, cryptographic primitives are rarely deployed in isolation: rather, they are integrated as part of wider protocols or (possibly distributed) systems. Another important question is therefore to understand how PQC and QKD could be used in combination to assure security in different application contexts.

Quantum computation using qubits is fundamentally different to classical computation using bits, and at present, the quantum computers that have been built are at a very small scale. Qubits are fragile, and there are challenges associated with error correction. It is not clear if there would be a quantum analogue of Random Access Memory, as commonly used in classical computation; nor how large-scale (networks of) quantum computers would be architected.

Without a clear understanding of how to model quantum computation, it can be difficult to assess the explicit costs (running time, memory usage) of quantum algorithms at a scale relevant to cryptography. This is the case when considering an adversary with a single quantum computer or a distributed network of quantum processors. As a result, we may be configuring our quantum security solutions inefficiently. The goals of this PhD position are to develop more realistic models of quantum computation, supported by benchmarking; to understand how quantum technologies can strengthen the network layer; and to apply this understanding to provide tailored and efficient security solutions to the quantum threat. This research is supported by RHUL's expertise on PQC and cryptanalysis and NPL's expertise on quantum networking and benchmarking of quantum computation.

Details of Award

- A full-time, fully funded PhD studentship for 3 years to start in January 2027.
- The studentship is joint between Royal Holloway, University of London (RHUL) and The National Physical Laboratory (NPL).
- The student would be based at NPL 2-3 days per week, and at Royal Holloway the remainder of the time.
- Stipend: roughly £23,800.00 per annum, subject to increase
- Annual travel support: up to £5,000.00 per annum
- Tuition fees: covered in full for home students

Eligibility

Home students only. Please note that this position is subject to security checks, and the successful candidate might be asked to obtain security clearance.

How to Apply

Prospective applicants should email Dr Rachel Player (Rachel.player@rhul.ac.uk) and Professor Alexander Tzalenchuk (NPL/RHUL) alexander.tzalenchuk@npl.co.uk with an expression of interest and a CV.

Further Information

The project is hosted by NPL (<https://www.npl.co.uk>) and the Information Security Group in the Department of Computing, Security and Mathematics at Royal Holloway, University of London (<https://www.royalholloway.ac.uk/research-and-education/subjects/information-security/>)