# Advancing Fully Homomorphic Encryption for privacy-preserving applications

Start Date: October 2026

Application Deadline: 30th Jun 2026

**Royal Holloway, University of London** is inviting applications for a 4-year PhD studentship in cryptography, co-funded by KDDI Research Laboratories in Japan.

**Project Overview**

Fully homomorphic encryption (FHE) is a type of privacy-enhancing encryption that enables computation directly on encrypted data without needing access to the decryption key or the underlying data itself. This technology allows individuals to securely protect their own sensitive data on cloud servers, while outsourcing computation on this data to third parties. In an increasingly data-driven society, widespread deployment of FHE would enable individuals to retain agency over their sensitive data (e.g. financial, genomic, personal) as it is used in a variety of contexts of benefit to them. For example, encrypted health data can be made available for analysis to medical researchers without exposing the underlying sensitive records. Similarly, sensitive citizen data can be stored in protected form on databases while charitable organisations are able to run or train an AI model on the underlying records to more effectively deliver their services. More generally, any organisation can process sensitive data under its custody that remains encrypted throughout, greatly reducing the chances of inadvertent data exposure.

The proposed PhD project will develop approaches to advance FHE for deployment in a wide range of scenarios, as follows:

1. Performance of FHE: FHE computations are, unfortunately, currently four to five orders of magnitude slower than computation on unencrypted data. In practice, this computational overhead provides a significant barrier to deploying this technology in applications for the public good, since most organisations are unwilling to sacrifice the performance loss in order to achieve the privacy gain. This typically means that some services that FHE could enable are simply not provided, whilst others are conducted much less securely through decryption of the dataset and subsequent processing of unprotected data. This project will develop approaches to

make FHE more practical, which will require advancement in the underlying algorithmic theory as well as progress on faster implementations.

2. Verifiability (zero-knowledge proofs): Although FHE enables the outsourcing of computation while preserving data privacy, it does not allow the user to verify whether a potentially malicious server is executing only the intended computation, rather than some unrelated one. This verification can be achieved using cryptographic primitives such as (non-interactive) zero-knowledge proofs and combining them with FHE gives rise to verifiable FHE. Nevertheless, existing verifiable FHE techniques suffer from significant efficiency challenges. This project will also seek to improve the efficiency of the construction and/or implementation of (non-interactive) zero-knowledge proofs.

3. Further cryptographic applications (indistinguishability obfuscation): FHE is known not only for its intrinsic usefulness but also for its applicability to the construction of a wide range of advanced cryptographic systems. In particular, it is known to enable the construction of indistinguishability obfuscation (iO), which is an important cryptographic primitive that has been shown to enable applications such as software copy protection and the reduction of security risks. Existing constructions of iO remain largely theoretical and there are significant challenges in realising practical deployment. This project will seek to improve the efficiency of the construction and implementation of iO.

The technical emphasis of the project will inevitably depend on the background of the recruited candidate. Additionally, the project will include development and analysis of a range of beneficial social application contexts. These will be co-developed by colleagues across the university with expertise on societal needs and challenges with respect to large-scale data analysis.

The industrial partner is KDDI Research, a large Japanese telecoms provider which has a long-standing research relationship with RHUL. KDDI Research have expertise in the theory and implementation of cryptography, and a particular interest in FHE-related cryptosystems. KDDI Research will support the project through their cryptographic expertise, as well as their own perspectives (from a different societal culture) on how cryptographic applications can be deployed in beneficial use cases. The candidate will be expected to co-develop the precise project objectives alongside KDDI and visit KDDI Research Laboratories in Japan at least once during the duration of the project.

**Details of Award**

A fully funded PhD studentship for 4 years to start in October 2026.

Stipend: roughly £26,800.00 per annum, subject to increase

Annual travel support: approx. £5,000.00 per annum

Tuition fees: covered in full for home students

**Eligibility**

Home students only

**How to Apply**

Prospective applicants should email Dr Rachel Player (Rachel.player@rhul.ac.uk) with an expression of interest and a CV.

**Further Information**

This project is hoisted by the Information Security Group at Royal Holloway, University of London. For more information, see: https://www.royalholloway.ac.uk/research-and-education/departments-and-schools/information-security/