**Project Description Form (PDF): MSc Information Security**

# How to complete this form

This form should be completed and submitted before the end of the second term. Students should meet their supervisor at regular intervals during the term to discuss the scope of the project and the initial literature review. Drafts of the form and the literature review may be submitted to the project supervisor for review during the term, as plans for the project evolve. Apart from completing this front page, text should be provided under each of the four headings given after the declaration section below.

An initial project literature review should also be prepared, again in consultation with your supervisor. The form will use a standard project front page. If at any stage the project deviates significantly from the description given, then the student must discuss this with their project supervisor and, if necessary, complete a revised form.

Royal Holloway encourages research of highest quality by ensuring that research ethics and good practices are followed. If the proposed work raises any ethical issues, ethical approval must be sought in advance.

**Student checklist**

* A copy of this form must be completed, and submitted (via email) to your project supervisor for their approval. They will acknowledge and confirm their approval by response to your email.
* A copy of the project literature review should also be sent, attached to this form.

# Student and project details

|  |  |
| --- | --- |
| **Name** | Joshua Limbrey |
| **Student number** | 100912024 |
| **MSc track (if applicable)** |  |
| **Email address** | [Joshua.limbrey.2018@live.rhul.ac.uk](mailto:Joshua.limbrey.2018@live.rhul.ac.uk) |
| **Supervisor name** | Dr Rachel Player |
| **Provisional project title** | Cryptanalysis of Lattice Based Post-Quantum Cryptosystems |

# Ethics (to be completed jointly by the student and the supervisor)

|  |  |  |
| --- | --- | --- |
| Question | Delete/tick as appropriate | |
| 1. Will the study be covert in any way? | Yes | No √ |
| 2. Will resulting data be used for purposes outside this study? | Yes | No √ |
| 3. Are you working with a vulnerable population? | Yes | No √ |
| 4. Is it possible that your study will cause distress or harm to participants? | Yes | No √ |
| If the answer to any of the above questions is ‘YES’, the supervisor should contact the MSc Project Director and arrange for Departmental/College ethical approval. | | |

# Declarations and signatures

**Student declaration**: I declare that I have read and understood the MSc Project Handbook, in particular the sections on referencing and plagiarism. I declare that the contents of this Project Description Form are all my own work, and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that the proposed work will not raise any ethical issues.

**Signature**: Joshua   
**Date**: 23/03/2022

**Supervisor declaration**: I approve the attached project plan and literature review. I agree that the proposed project topic meets the requirements of the MSc track (if specified). I also agree that the project does not raise any ethical issues.

**Signature**:   
**Date**:

# Statement of objectives [Guidance: This statement should include a description of what you intend to achieve in your project. It should briefly cover why it is of interest, what contributions it will make, etc.]

* Gain experience and understanding of two upcoming CPA-PKE and IND-CCA(2)-KEM cryptosystems. I hope that through this project I will be able to gain knowledge about a cutting-edge area of information security.
* Understand what it is about these cryptosystems that gives them these properties.
* How can existing ideas be used to try and poke holes into these properties.
* How can we defend against these?
* Through this, I hope to be able to contribute to the creation and selection of rigorous and secure post-quantum cryptography.

# Methodology [Guidance: Describe how do you intend to achieve the objectives listed above. This should include a review of your strategy for getting started (e.g. what literature you plan to review, how you intend to find relevant literature, what software you intend to look at and/or write, etc.).]

* I shall begin by reading and understanding the round 3 NIST submission papers for both CRYSTALS-KYBER (Avanzi, et al., 2021) and SABER (Basso, et al., 2021), using Introduction to Modern Cryptography (Katz & Lindell, 2007) and The Joy of Cryptography (Rosulek, 2021) as well as my undergraduate notes as learning material to ensure I can fully understand and grasp all concepts in both proposals.
* From this preliminary literature review, I hope to be able to understand what properties of these cryptosystems give them their desired security properties as well as existing methods to attack these properties for similar LWE/LWR lattice-based cryptosystems (can GGH be used as an example here as LWE can be dependent on solving SVP or CVP? What other examples are there?)
* From this, can I apply existing ideas in a novel way, ideally with unique idea(s) in order to demonstrate potential weakness(es) in either of the two proposed cryptosystems.
* Initially, I intend to read the already stated literature before conducting more independent research not strictly literature based. If further literature is required, I plan to use <https://dblp.org> in order to search for papers either by Author (for example my supervisor has noted that L. Ducas is widely regarded for similar research) or by relevant search terms.

# Work plan [Guidance: Provide a rough schedule for your project, showing the key milestones in the project (up to and including the submission deadline in August).]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Mar | Apr | May | June | July | Aug | Sep |
| Reading and research | √ | √ | √ |  |  |  |  |
| PDF & PLR | 25th |  |  |  |  |  |  |
| Chapter 1,2,3 |  |  | √ | √ |  |  |  |
| Chapter 4,5,6 |  |  |  | √ | √ |  |  |
| Remarks, Abstract etc. |  |  |  |  | √ |  |  |
| First full draft (self-imposed deadline) |  |  |  |  | First week |  |  |
| Final draft |  |  |  |  |  | 1st |  |
| Final deadline |  |  |  |  |  | 30th |  |

# Additional comments [Guidance: Optionally provide any extra comments on your proposal on matters not covered above. Where relevant include details of the involvement of external organisations. Some students (and supervisors) find useful to have a *draft* table of contents included in this section.]

Draft table of contents:

* Abstract
* Acknowledgements
* Contents
* Figures
* Abbreviations and acronyms

1. Introduction
   1. Motivation
   2. Preliminaries and notation
2. CRYSTALS-KYBER and SABER – how they work
3. Security properties and how they’re achieved
4. Attacks on these properties
5. How can we apply these to CRYSTALS-KYBER and SABER?
6. How can these be remedied?
7. Remarks and conclusion

* Bibliography

# Bibliography

Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., . . . Stehlé, D. (2021). CRYSTALS-Kyber. *Algorithm Specifications And Supporting Documentation*.

Basso, A., Bermudo Mera, J., D'Anvers, J.-P., Karmakar, A., Sinha Roy, S., Van Beirendonck, M., & Vercauteren, F. (2021). SABER: Mod-LWR based KEM. *Round 3 Submission*.

Katz, J., & Lindell, Y. (2007). *Introduction to Modern Cryptography.* CRC Press.

Rosulek, M. (2021). *The Joy of Cryptography*. Retrieved from https://joyofcryptography.com/