Faculty of Science
Department of Mathematics

MA4198 PROJECT PROPOSAL (PROJECT CUM SEMINAR GROUP)

SUPERVISOR'S INFO

Name:	Ruth Ng Ii-Yung
Email:	niiyung@dso.org.sg
Tel number:	67968103
Office location:	DSO

TITLE

Introduction to Provable Security and Structured Encryption

BRIEF DESCRIPTION OF PROJECT

Modern cryptography has moved away from heuristic methods for demonstrating security and towards a more mathematical approach to formalizing security. In this project, students will learn the basics of writing a security proof in the code-based game-playing model of Bellare and Rogaway, and gain exposure to simple proofs in this area. [Stretched goal: From here, the students will be guided to write a novel proof of their own for a simple cryptographic scheme of their choosing.

EXPECTATION/S

PREREQUISITE/S (at level 3000 or below, with at most one course at level 3000)

Singaporean only.
Students must be able to write up proofs in TeX, and be willing to come to DSO regularly for meetings/lectures. Students doing this project will be asked to work through the many nitty-gritty details of long proofs, so it is best suited to students who enjoy details and iterating over a proof to achieve elegance. For this reason, it is preferred that students have background in scientific, technical, or proof writing.

READING REFERENCE/S

https://cseweb.ucsd.edu/~mihir/cse207/index.html
https://www.youtube.com/playlist?list=PL-SStBoAJuw0vj8MgTFhY5y9wSFnjGbOB
https://eprint.iacr.org/2006/210.pdf
https://eprint.iacr.org/2011/010.pdf