MA4198 PROJECT PROPOSAL (PROJECT CUM SEMINAR GROUP)

SUPERVISOR'S INFO

Name:	Ti Yan Bo
Email:	yanbo.ti@gmail.com
Tel number:	91734133
Office location:	DSO

TITLE

Endomorphisms of abelian varieties in genus two isogeny cryptography

BRIEF DESCRIPTION OF PROJECT

Isogeny-based cryptography is a potential post-quantum cryptosystem. This is based upon maps between abelian varieties (which elliptic curves are a part of). This project will aim to generalise isogeny-based cryptography to genus two. This can bring about reductions in key sizes or increases in efficiency. This project will introduce students to endomorphism rings which holds a lot of information about the abelian varieties. Furthermore, there are algorithms that can solve the isogeny problem given the endomorphism rings of the two abelian varieties in question.

EXPECTATION/S

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

Singaporean only.
Students should be pro-active and self-directed to read up papers on isogeny-based cryptography as part of the project work.
This is a very mathematical project and requires learning about abelian varieties.

READING REFERENCE/S

1. Joseph Silverman: The Arithmetic of Elliptic Curves
2. Hindry and Silverman: Diophantine Geometry: An Introduction (Part A only)
3. Steven Galbraith: Mathematics of Public Key Cryptography
4. eprint.iacr.org/2024/146