DSO projects for MA4198

What is it?

- Offered by Defence Science Organization (DSO)
- 1-semester project supervised by DSO staff
- Can be used to satisfy MA4198
- Only for Singaporeans
- DSO will conduct interview to select students

S/N	Project Title	Description	Requirements
1	Introduction to Provable Security and Structured Encryption	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.]	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.
2	Probabilistic Modelling in Structured Encryption Schemes	Structured Encryption (StE) is a generic framework for describing cryptographic schemes which outsource data to the cloud. Through this, they will aim to use probability and statistics to provide recommendations for schemes and parameters to be used in real world use-cases. As a stretch goal, the students can corroborate their results via simulations on synthetic and/or real-world data.	Singaporean only. Students should have exposure to algorithms, or be able to interpret code, so that they can interpret pseudocode. Programming background (any language) is preferred to complete the simulations. Students doing this project will be asked to independently come up with mathematical models and/ or simulation experiments with minimal guidance, so it best suits students who are pro-active and self-directed.

S/N	Project Title	Description	Requirements
3	Theta functions in genus two isogeny cryptography	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 look at theta functions which is a way to perform arithmetic and isogenies of abelian varieties.	Singaporean only. Students should be pro-active and self-directed to read up papers on isogeny-based cryptography as part of the project work. Student should be comfortable looking at implementations.
4	Endomorphisms of abelian varieties in genus two isogeny cryptography	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.	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.

To indicate your interest in these projects, please fill in this survey form by 23 June, 2024: https://forms.office.com/r/1MU6VZGiKk

To find out more about the DSO projects, you may contact DSO staff below:

- Dr Ruth Ng Ii-Yung at niiyung@dso.org.sg (for projects 1 and 2)
- Dr Ti Yan Bo at tyanbo@dso.org.sg (for projects 3 and 4)