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

Probabilistic Modelling in Structured Encryption Schemes

BRIEF DESCRIPTION OF PROJECT

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.

EXPECTATION/S

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

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.

READING REFERENCE/S

https://eprint.iacr.org/2011/010.pdf
https://www.iacr.org/archive/eurocrypt2019/114760319/114760319.pdf
https://dl.acm.org/doi/pdf/10.1145/3319535.3354213
https://eprint.iacr.org/2021/765.pdf