School of Computing, Engineering, and the Built Environment
Edinburgh Napier University

PHD STUDENT PROJECT

Funding and application details

Funding status: Self funded students only

Application instructions:
Detailed instructions are available at https://blogs.napier.ac.uk/scebe-research/available-phd-student-projects/

Prospective candidates are encouraged to contact the Director of Studies (see details below) to discuss the project and their suitability for it.

Project details

Supervisory Team:

- DIRECTOR OF STUDY: Baraq Ghaleb (Email: B.Ghaleb@napier.ac.uk)
- 2ND SUPERVISOR: Bill Buchanan

Subject Group: Cyber-security and system engineering

Research Areas: Computer Science

Project Title: Fast and Secure Multi-party Computation Techniques

Project description:

Multi-party computation (MPC) protocols enable multiple parties — each holding their own private data — to evaluate a computation without ever revealing any of the secret data held by each party. This has proven useful in multiple use cases. For instance and in the context of cryptocurrencies, the private key, a secret used to sign transactions, can be divided into shares that are independently computed by each participating party. The parties then communicate through a couple of rounds to create a signature without revealing their shares to each other. This ensures that the private key is never materialized in a single place. Another use case of MPC is the possibility of utilizing it for privacy-preserving in a variety of applications, for example, to enable privacy-preserving machine learning in the cloud. Unfortunately, the state-of-the-art MPC protocols suffer from high computational and communication overhead as they rely on complex mathematical operations to achieve a high degree of security including homomorphic encryption and zero-knowledge proofs, a fact that would evidently decrease the performance of MPC protocols and render them impractical under many use cases.

The aim of the project include (but are not limited to):

- Improving the performance and usability of multi-party computation protocols
- Designing new multi-party computation protocols and/or use cases

References:

Candidate characteristics

Education:

A first-class honours degree, or a distinction at master level, or equivalent achievements in Computer Science

Subject knowledge:

- Cyber Security

Essential attributes:

- Experience in fundamental of cryptography related research
- Competent in programming and math-related concepts
- Knowledge of multi-party computation, homomorphic encryption and zero-knowledge proof
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management