Department	School of Computing
Supervisors	Baraq Ghaleb, Zakwan Jaroucheh, Bill Buchanan
Project Title	Fast and Secure Muti-party Comutation 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

Perspective applicants are encouraged to contact the Supervisor before submitting their applications. Applications should make it clear the project you are applying for and the name of the supervisors.

Academic qualifications

A first degree (at least a 2.1) ideally in Computer Science with a good fundamental knowledge of Cryptography.

English language requirement

IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. Full details of the University's policy are available online.

Essential attributes:

- Experience of fundamental of cryptography related research
- Competent in programming and math related concetps
- 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

Indicative Bibliography	1. Archer, David W., et al. "From keys to databases—real-world applications of secure multi-party computation." The Computer Journal 61.12 (2018): 1749-1771.

	2. R. Gennaro and S. Goldfeder. Fast Multiparty Threshold ECDSA with Fast Trustless Setup. In ACM CCS 2018 (this proceedings). 3. Canetti, R., Makriyannis, N. and Peled, U. (1970) UC non-interactive, proactive, THRESHOLD ECDSA, Cryptology ePrint Archive. Available at: https://eprint.iacr.org/2020/492. 4. https://blog.taurushq.com/first-open-source-implementation-of-mpc-cmp/ 5. https://www.fireblocks.com/what-is-mpc/
Enquiries	For informal enquiries about this PhD project, please contact Dr. Baraq Ghaleb at b.ghaleb@napier.ac.uk
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process