Department	School of Computing
Supervisors	Bill Buchanan, Jawad Ahmad
Project Title	Post-Quantum Cryptography Infrastructure for Trust and Homomorphic Encryption within Health Care

PROJECT DESCRIPTION

Context: All existing public key methods, such as RSA and ECC (Elliptic Curve Cryptography) will be broken with the usage of quantum computers. These methods will be replaced by post quantum cryptography (PQC) methods for digital signing, such as for lattice-based and hash-based signatures. Unfortunately, most of our trusted infastructures for the PKI (Public Key Infrastructure) and blockchain are based on either RSA and ECC, and thus need to be replaced. These PQC methods often have additional features that enable enhanced privacy, such as in the implementation of homomorphic encryption (and which allows for the processing of encryption data).

Focus: This research aims to provide a replacement framework for the integration of PQC methods, and build identity systems and sharing systems in health care which support quantum robustness [1, 2]. This will likely to be applied into a key application area, such as replacing existing blockchain infastructures, self-soveign identity systems, and in trusted information sharing in health care [3]. A particular focus of the work is on improving the performance of existing post-quantum cryptography methods for their performance, and with a trade-off against overall security [4], and in the application of homomorphic encryption for privacy-aware processing of health care data [5]. The work has more of a focus on the application into a specific domain, rather than the formal methods involved in PQC.

Why undertake this PhD? The work will be undertaken with the Blockpass ID Lab at Edinburgh Napier and which is the first research lab in the world to focus on identity and trust, and is advancing in many areas of privacy-aware systems. This lab is led by Prof Bill Buchanan and who has a long track record of success in creating highly successful spin-out companies (Zonefox, Symphonic and Cyan Forensics), and in commercialising reseach work. Overall, the PhD research work has the potential to build into a licencing or spin-out opportunity, and will likely integration with health care providers.

Academic qualifications

A first degree (at least a 2.1) ideally in Computer Science-related or Electronic Engineering with a good fundamental knowledge of software development.

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 cybersecurity and computer science.
- Competent in software development
- Knowledge of encryption.
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

An interest in cryptography.

Indicative Bibliography	[1] Saha, R., Kumar, G., Devgun, T., Buchanan, W., Thomas, R., Alazab, M., ... & Rodrigues, J. (2021). A Blockchain Framework in Post-Quantum Decentralization. *IEEE Transactions on Services Computing*. [2] Banupriya, S., Kottursamy, K., & Bashir, A. K. (2021). Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in public blockchain. *Peer-to-Peer Networking and Applications*, *14*(5), 2813-2825. [3] Xu, G., Xu, S., Cao, Y., Yun, F., Cui, Y., Yu, Y., & Xiao, K. (2022). PPSEB: A Postquantum Public-Key Searchable Encryption Scheme on Blockchain for E-Healthcare Scenarios. *Security and Communication Networks*, *2022*. [4] Aumasson, J. P. (2019). Too much crypto. *Cryptology ePrint Archive*. [5] Munjal, K., & Bhatia, R. (2022). A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex & Intelligent Systems*, 1-28.
Enquiries	For informal enquiries about this PhD project, please contact Bill Buchanan (b.buchanan@napier.ac.uk)
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process