

Department	School of Computing
Supervisors	Luigi La Spada, Bill Buchanan
Project Title	Quantum Metasurfaces for Cybersecurity Applications

PROJECT DESCRIPTION

For information security, software algorithms or hardware protocols are generally adopted. Software algorithms use pseudo-random numbers generated from one-way mathematical functions. Hardware protocols use physically unclonable functions (PUFs) that exploit, for example, manufacturing process variations in the physical microstructures of integrated circuits. Both solutions (software and hardware) are robust for classical computers but vulnerable in the age of quantum computers.

In this project, with the aim of developing secure cryptographic systems, we would like to use artificially engineered 2D structures, called quantum metasurfaces. More specifically, we propose the design and implementation of an optical cryptographic surface based on quantum metasurfaces, where optical PUFs are embedded in optical diffusion films, with micro/nano architectures, inspired by biological tissues. This will allow obtaining a structure with unique randomness. Such a structure is difficult to decode and at the same time, it is high entropy, non-volatile, reconfigurable, ultra-low power, low cost, and environmentally friendly.

The resulting new cryptographic systems can currently be integrated with existing communication protocols and networks and used with quantum computers in the future.

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 Electrical/Electronic Engineering or Computer Science with a good fundamental knowledge of Electromagnetics and Cybersecurity.

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 Electromagnetics and Cybersecurity
- Competent in sensors and networks design and security
- Knowledge of digital signals processing and public-key cryptography
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

Electromagnetic waves and materials
Applied cryptography

Indicative Bibliography	<p>_ L La Spada et al., Curvilinear metasurfaces for surface wave manipulation, Nature Scientific reports 9 (1), 1-10, 2019</p> <p>_ Buchanan, et al. Post Quantum Cryptography Analysis of TLS Tunneling on a Constrained Device, 2022</p>
Enquiries	For informal enquiries about this PhD project, please contact i.laspada@napier.ac.uk
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process