**Application for QICS PhD project**
**'Secure Network of Quantum Sensors'**

## Context

Two of the main areas of quantum technologies are communication and sensing. In communication, by exchanging quantum systems and sharing entanglement we have security and efficiency that cannot be achieved classically. In sensing, using quantum probes allows for precision and sensitivity beyond any possible measurement based on classical physics.
As we move towards a quantum internet, where quantum devices of different sizes and applications are connected through classical and quantum channels, it is natural to consider the possibility of merging the incredible benefits of quantum sensing and communication. Indeed in an 'internet of quantum things' combining security, efficiency with the super classical measurements, for example ensuring sensing data is secure and trusted, would appear to suggest much possibility for great advantage.

We imagine a network of sensors, of all different kinds, with different applications, connected by quantum and classical channels, and we want to push the limits of what can be done, by incorporating cutting edge quantum cryptographic techniques and ideas. Networking quantum sensors is already understood to offer many benefits. Entangling sensors allows sensing global fields or features over a network (such as total or average field strength), with applications for novel synchronisation of clocks and telescope alignments to name a few. Clearly any additional security and efficiency is greatly beneficial here. Even without entangling the sensors themselves, the capacity to delegate sensing, or securely communicate the results in a trusted, possibly anonymous, way has many promising applications. One could imagine many sensors deployed across a network (for example of cars, or medical devices), that wish to securely share sensitive data locally collected.

Previous works looking at combining quantum security with quantum sensing, though inspiring, have often lacked cryptographic rigour, leaving them open to security loopholes. In a recent work [1], we make the first steps to address these issues, developing formal notions of security for sensing, and provide new, secure, protocols for delegated (two party) quantum sensing.

## Objectives

In this project we will develop a formal framework for secure sensing in networks, combining rigorous cryptographic techniques with sensing. Building on the work of [1], we will enable more involved network sensing scenarios (multiparty, multiparameter, various levels of trust and mistrust), and develop towards near term practical implementations.

- Develop a formal framework for security for networks of quantum sensors
- Develop proposals for proof of principle experiments demonstrating quantum advantage in networks of sensors

## Methods

The student will address two main questions in this thesis. On the one hand they will build on the cryptographic framework initiated in [1] to involve more useful, concrete, applications, including directions such as secure multiparty computations and anonymity in networks of sensors. The student will benefit from the expertise in the LIP6 group in this direction, but also links to the CS community in LIP6 in IOT which will help guide understanding of real world use cases, as well as our participation in international projects for future quantum

internet, in particular the EU flagship project Quantum Internet Alliance. We strongly believe that secure networks or sensors will be an exciting candidate for real world use cases of the future quantum internet.
On the other hand the student will pursue the implementation of proof of principle demonstrations of networks of quantum sensors. Here we build on the LIP6 experience in taking protocols from theory to practice, e.g. [3]. The student will explore different possibilities, but a concrete example we expect to work will be on the optical implementation of GHZ states and their application for secure sensing, in set ups similar to that of [3].

The initial plan for the thesis duration is as follows
T1: Formal framework for secure networks of quantum sensors (integration of secure multiparty computation with sensing networks, including delegation, anonymity, untrusted channels and devices) [M0-12]
T2: Adaptation to variety of sensing technologies (optics, NV centres, cooled atoms…) [M12-24]
T3: Proposal for proof of principle experiments demonstrating quantum advantage. Clear projects in mind within LIP6, in particular for using optical GHZ states [M24-36].

**Expected results**
We expect to publish several articles during the thesis which present a formal security framework, broadly applicable, as well as concrete examples. When possible we will pursue experimental implementation. We will also work with internet-of-things experts in LIP6 to maximise possible acceptance and applicability for future technologies.

**Supervisors and related publications**
The main supervisor will be Damian Markham, the co-supervisor will be Eleni Diamanti, both from the LIP6 QI team.
Both Markham and Diamanti have experience supervising PhDs and bring different expertise to the project. Markham is a theoretician, who developed the first rigorous proofs for secure networks of quantum sensors ([1]) and has a strong background in quantum cryptography and protocol development (e.g. [2]). Diamanti is an expert in implementing quantum cryptographic protocols. Markham and Diamanti have a strong history collaborating in the development and implementation of novel quantum protocols proving quantum advantage, for example in [3]. This project will continue this work in the novel direction of integrating quantum sensors and quantum cryptography.

[1] Nathan Shettell, Elham Kashefi and Damian Markham, A cryptographic approach to quantum metrology, Phys. Rev. A 105, L010401 (2022)
[2] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, E. Kashefi, Quantum certification and benchmarking, Nature Reviews Physics 2, 382-390 (2020)
[3] McCutcheon W, Pappa A, Bell BA, Mcmillan A, Chailloux A, Lawson T, Mafu M, Markham D, Diamanti E, Kerenidis I, Rarity JG. Experimental verification of multipartite entanglement in quantum networks, Nature communications, 7(1):1-8 (2016).

**Candidate**
The candidate will have a background in physics and or computer science. Familiarity with quantum information is an advantage, as is some knowledge of cryptography and or quantum optics.