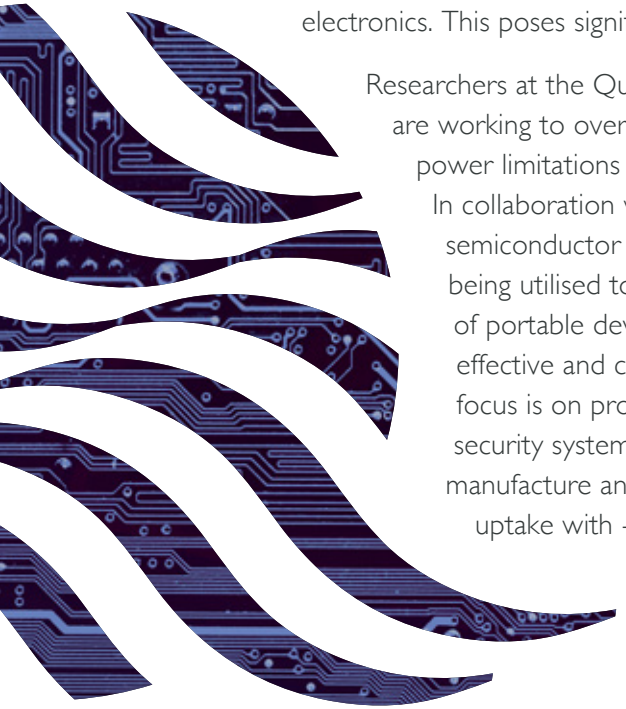
Chip-scale Quantum Key Distribution

Threats to current conventional encryption techniques created by major advances in quantum computing are widely acknowledged as both real and forthcoming. Quantum Key Distribution (QKD) is a mature quantum technology which underpins secure communications and other transactions through the secure distribution of cryptographic keys. QKD is future-proofed against threats created by advances in other new quantum technologies, and is based on the manipulation and communication of quantum optical signals.

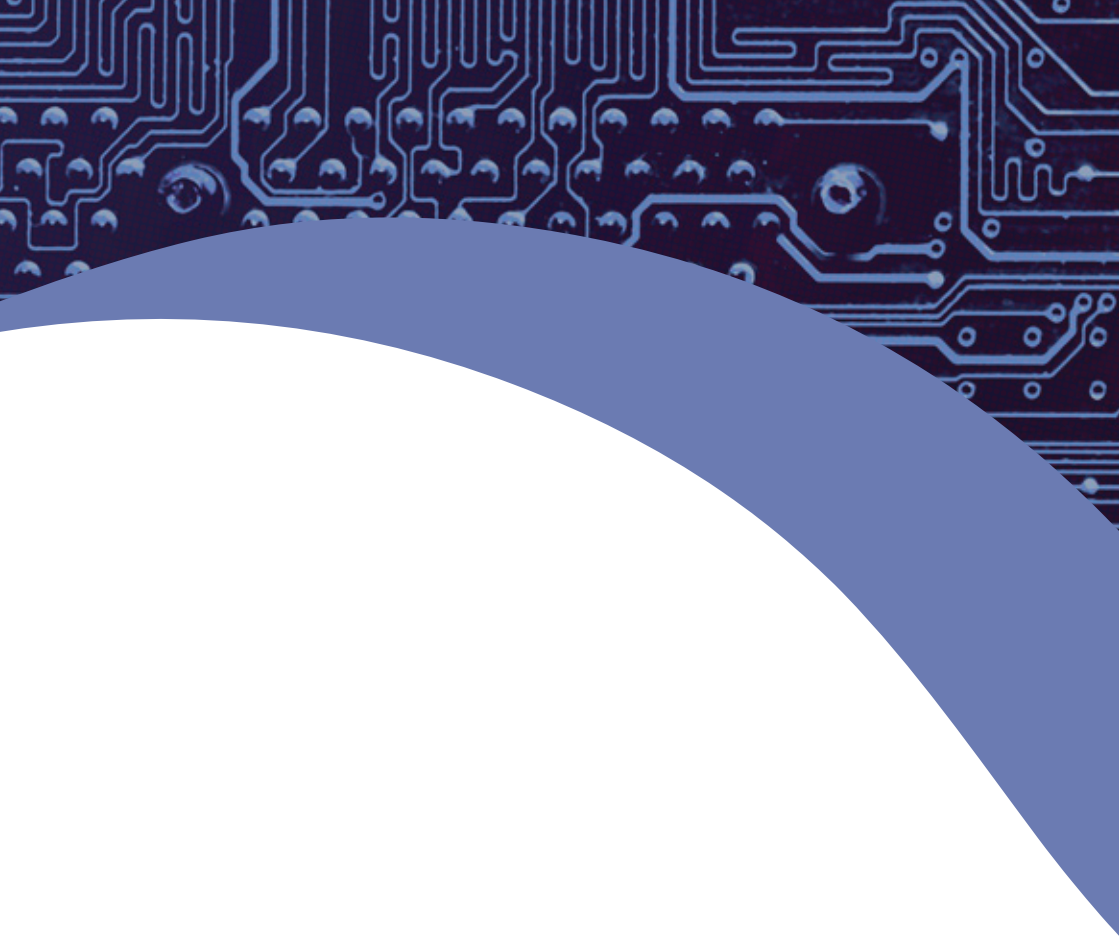
All our existing IT, particularly consumer devices, rely heavily upon sub-microscopic components, integrated in vast numbers on semiconductor chips. Such miniaturisation offers distinct advantages in portability, ease of manufacture, reduced costs and integration of multiple capabilities. It follows then that in order for quantum-enabled secure communications devices to enter mass market deployment, quantum optics must also be miniaturised to chip-scale and integrated alongside conventional electronics. This poses significant engineering challenges.



Researchers at the Quantum Communications Hub are working to overcome the size, weight and power limitations of existing QKD devices. In collaboration with industry, existing semiconductor fabrication infrastructure is being utilised to produce a new generation of portable devices which are robust, cost-effective and commercially viable. The focus is on producing quantum enhanced security systems in a form suitable for mass manufacture and thus widespread industrial uptake with - importantly - significant scope for integration with conventional technologies.

Quantum Communications Hub researchers at the University of Bristol have successfully trialled the world's first chip-to-chip QKD system, which enables cryptographic keys to be securely exchanged. Tiny microchip circuits control, communicate and detect quantum states of light, at scales that pave the way for QKD to be integrated within conventional consumer devices. Further advances include: migration onto silicon photonics; new integrated quantum network switching (University of Cambridge); and a novel hybrid classical-quantum transmitter design with major potential for integration with existing telecommunications infrastructure (University of York). Drivers for all our work include increasing the communication rates of devices and network compatibility.

The Quantum Communications Hub has helped create an R&D ecosystem for the development and eventual rollout of integrated quantum photonic platforms for secure data networking. This ecosystem is clearly going from strength to strength – there is now an Innovate UK Industrial Strategy Challenge Fund (ISCF) project AQuaSeC pushing towards commercialisation, and Hub-supported start-ups such as KETS and Nu Quantum are now respectively producing systems and components. The establishment of a supply chain for chip-based quantum security solutions is beginning. All this enables future Hub work to focus on innovation at low technology readiness levels. So we are now working on chip-based "next generation" systems and protocols, such as floodlight QKD, measurement-device-independent QKD and hybrid classical-quantum systems – developing these to feed into the growing ecosystem of companies and ISCF projects.



If you would like to hear more about the Hub's work on miniaturising QKD devices, please contact us via enquiries@quantumcommshub.net

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

UKRI Engineering and Physical Sciences Research Council