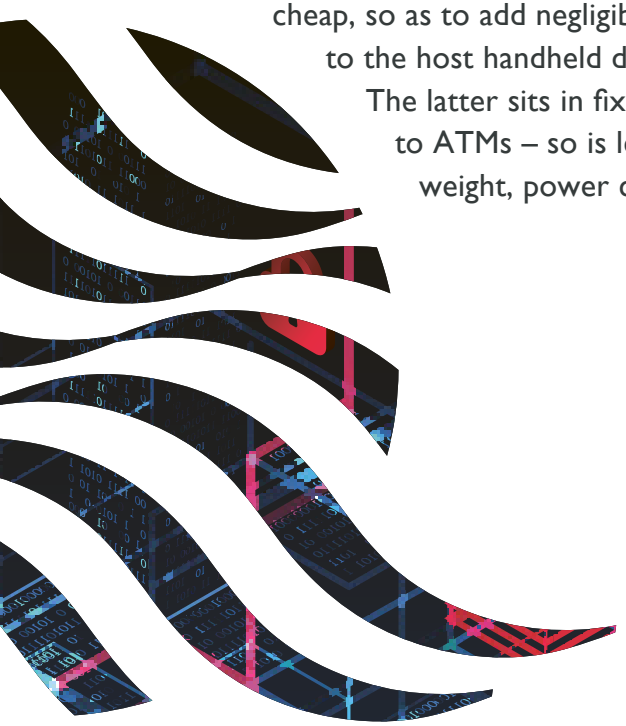
QUANTUM COMMUNICATIONS HUB

Consumer Quantum Key Distribution

Much of the journey of digital communications happens in underground fibre. However, for consumers, information flow often takes the form of a short journey between the end of a fibre network and a handheld device. So for quantum communications to be commercialised for mass consumer use, we need to distribute quantum keys – for secure communications and other transactions – to personal handheld devices, through free-space (i.e. without fibre).

Free-space quantum key distribution (QKD) between prototype handheld devices and a wall mounted terminal (the so-called "quantum ATM") has been demonstrated by Quantum Communications Hub researchers, based at the University of Bristol, paving the way for short-range consumer QKD. The system under development comprises a miniature transmitter that docks to a larger receiver. The former must be very cheap, so as to add negligible manufacturing cost to the host handheld device, such as a phone. The latter sits in fixed terminals – analogous to ATMs – so is less restricted in size, weight, power consumption and cost.



The first Quantum Communications Hub consumer QKD design used a card slot-inspired system, to demonstrate suitable quantum transmission and operation. However, the system is now being advanced to include hand tracking functionality, to remove the requirement for any physical contact between the transmitter and receiver. This new functionality targets practical "contactless QKD" transactions, comparable to current personal contactless technologies. A significant challenge with this technology is achieving precise tracking of hand movements, whilst maintaining a wide field-of-view. Hub researchers at the Universities of Bristol and Oxford are collaborating to develop a novel beam-steering and tracking system to address this challenge.

The aim of consumer QKD systems is to securely establish quantum keys between a mobile user and an institution, or service provider. These keys then enable consumers to interact with enhanced security over the standard internet, e.g. with financial or health institutions. This same technology could similarly enable ultra-secure sensitive interactions between users and government services, for example, e-voting. With a trusted service provider sharing keys securely with multiple users, the provider can then facilitate shared keys between specific individuals, for personal communications.

The commercial trajectory for this QKD technology is the seamless integration of miniature transmitters into future mobile phones. These will communicate over LiFi (similar to WiFi, but using light instead of radio waves) to a fixed receiver (similar to a router) – and so connect into high performance secure quantum networks, allowing consumers to benefit with cost effective hardware. Combining this QKD technology with new quantum-resistant conventional cryptography will enable straightforward connection of new devices to existing, dynamically changing networks. All this will truly bring QKD to consumers, providing them with the enhancement of quantum security for their personal devices – in a transparent and user-friendly package.

If you would like to hear more about the Hub's work developing handheld consumer QKD technologies and merging these with quantum-resistant cryptography, please contact us via enquiries@quantumcommshub.net

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

UKRI Engineering and Physical Sciences Research Council