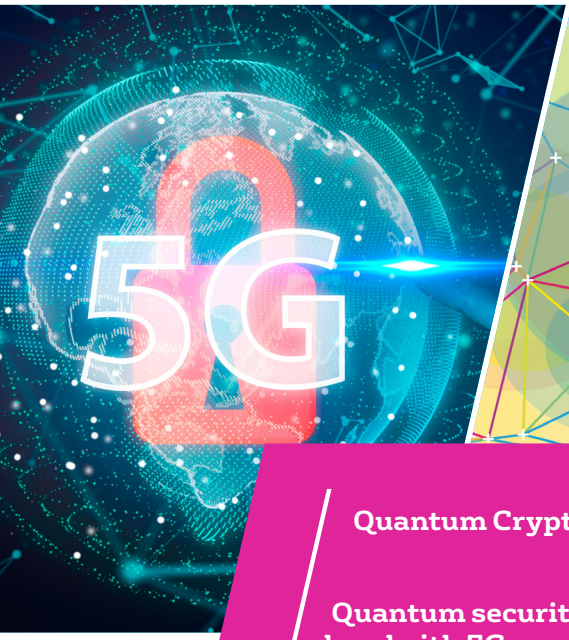
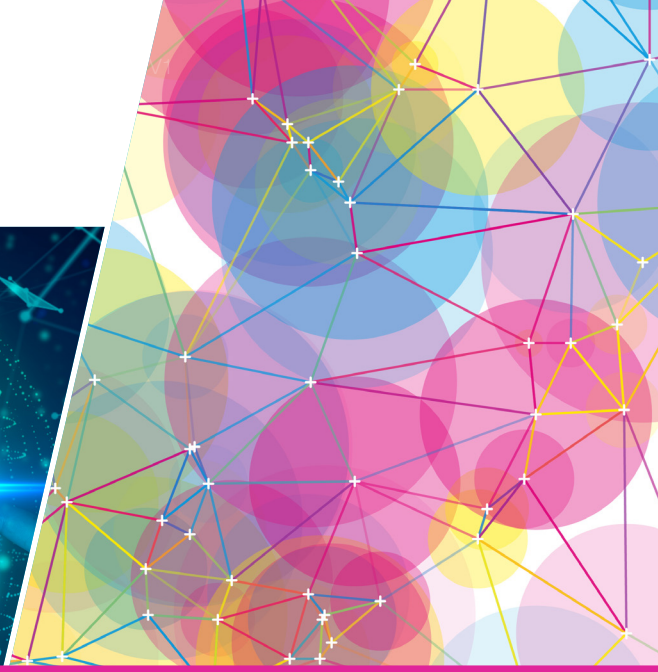
University of BRISTOL





Quantum Cryptography for ultimate 5G security

Quantum security for ultra low latency and high bandwith 5G services

Securing multi operator virtualised network services

Quantum Secured 5G Network

Addressing 5G Security with Quantum Cryptography

About

There are widely reported concerns on security vulnerability of 5G networks which are predicted to transform the telecommunications industry in the next ten years.
New research by the High Performance Network Research Group at the Smart Internet Lab has demonstrated a ground-breaking solution for securing future critical communications infrastructures, including emerging 5G networks.
The proposed solution will enable 5G network operators to offer ultimately secure 5G services while guaranteeing ultra-low-latency and high-bandwidth communications. This is due to the novel combination of quantum and infrastructure virtualisation technologies.
The proposed quantum secured 5G virtualisation platform is capable of working across multiple 5G operators' networks (i.e. EE, O2, Vodafone etc.). It uses advanced and standard compliant virtualisation technology for creating on-demand complex and collaborative 5G network services across operators' domains, while utilising quantum cryptography and optical interconnection infrastructure to secure services and guarantee 5G Key Performance Indicators (3GPP KPIs).

Let's Get Technical

Recent advances in software engineering and commodity computing technologies have revolutionised the telecommunications industry in the past ten years. Entire classes of network communication services that have traditionally been carried out by proprietary, dedicated hardware, are now virtualised and hosted in commodity computing servers. This is commonly referred to as "Network Softwareisation".
The move of critical network communication functions into software, distributed across the internet however, imposes significant security risk for telecommunications networks and specifically for 5G networks that rely entirely on such software architecture. Any malicious attempt to tamper with these virtualised network functions can potentially put the whole internet and its users at risk.
The new research addresses this problem with a new, fully programmable network virtualisation platform leveraging on quantum technologies for securing function virtualisation and service orchestration.
The proposed solution leverage on state-of-the-art key 5G technologies such as:

- Network Function Virtualisation (NFV)
- Software Defined Network (SDN)
- Quantum Mesh Networking
- Quantum Key Distribution (QKD)

Smart Internet Lab

The Smart Internet Lab at the University of Bristol has been recognised as the top Higher Education Institution within the UK as a concentrated 5G hub of estabilised collaborative relationships between national and international institutions, authorities and industry.

5G Research

We are world leaders in fibre, wireless, and 5G convergence research. We have created a unique 5G Trial Testbed for a Smart City, Campus, Region and the Telecom Industry.

EPSRC
Engineering and Physical Sciences Research Council

Department for Digital, Culture Media & Sport

European Commission | Horizon 2020 European Union funding for Research & Innovation

QUANTUM COMMUNICATIONS HUB

UNIQORN

Ultimately secure and programable 5G network