No images? Click here

Welcome to the EPSRC Quantum Communications Hub Newsletter!

Hi there, welcome to the first EPSRC Quantum Communications Hub Quarterly Newsletter. Here you can keep up to date with the latest news, events and opportunities associated with the Hub!

EPSRC Quantum Communications Hub 2.0 Launch

Please see a video address from Hub Director, Prof Tim Spiller, below. The video was released in place of the Phase 2.0 Launch Event which unfortunately had to be cancelled due to the current Covid-19 pandemic. In the video, Tim outlines the main achievements of the Hub during Phase 1.0 and the plans for Phase 2.0.

Watch video

National Cyber Security Centre White Paper

The National Cyber Security Centre (NCSC) has published a new white paper on quantum security technologies, which discusses both quantum key distribution (QKD) and quantum random number generators (QRNGs).

The paper acknowledges that QKD mitigates against security issues of traditional public key cryptography by utilising fundamental quantum mechanics, as opposed to hardness of mathematical problems. The latter could be vulnerable to attacks by future large-scale quantum computers for example through Shor's algorithm. The paper recognises that QKD enables two parties to be able to share a secret key, where the key cannot be observed by an eavesdropper without the parties being aware. However, it also highlights that QKD does not provide initial authentication, meaning it could be vulnerable to physical man-in-the-middle attacks. The paper recommends that QKD should be deployed in conjunction with routine cryptographic mechanisms, which ensure authentication, and that further research is required to understand how QKD can be integrated into systems of classical components. It concludes that: "**NCSC does not endorse the use of QKD for any government or military applications**, and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors." *(sic)*

With regard to QRNGs, the paper recognises that these are able to produce random numbers at very high speeds and in their ideal state, can produce truly unpredictable numbers. However, it comments that this unpredictability is hard to realise due to noise from the classical circuitry required and the use of classical circuitry can leave the QRNGs open to implementation level attacks, similar to those experienced by classical RNGs. It is noted that the NCSC will continue to support research surrounding QRNGs.

In the Quantum Communications Hub we are pleased to see that NCSC continues to engage in the important sector of quantum security technologies, and have revised their previous position with respect to the use of QKD in business-critical networks. However, it is also important to highlight the progress that has been made with quantum security technology research and development over the past few years and the planned work going forward in the UK National Quantum Technologies Programme.

Clearly, one of the main concerns remaining with regards to QKD is authentication. The limitations of QKD in general and the issue of authentication, in particular, have long been identified by the community and highlighted as such in specialist publications. Indeed, a combination of both quantum-based and post-quantum infrastructure solutions has been long advocated as the most effective against the threats posed by the advance of quantum computing, both in technical references and trade and public engagement press. Examples of such, co-authored by Hub investigators/partners, include:

- the European Telecommunications Standards Institute's white paper 'Implementation Security of Quantum Cryptography'

- an article written by Hub Director, Prof Tim Spiller, and Dr Christoper Chunnilall from the National Physical Laboratory, for Laser World Focus, 'Quantum Photonics: Ensuring quantum-secured communications'
- an article written by Hub Director, Prof Tim Spiller, for the IMPACT publication 'Making tomorrow's world secure today'
- and an article written by Hub Director, Prof Tim Spiller, for the Royal Signals Journal, 'Quantum Communications Technologies'.

Hybrid solutions of quantum-based and post-quantum technologies are a key aspect of the work which will be undertaken by the Hub in the second phase of the National Programme.

In response to the white paper, Hub Director, Professor Tim Spiller made the following statement:

"Whilst I welcome the shift in NCSC's position with respect to the use of QKD in business-critical networks, I think it is also important to highlight the progress that has been made with quantum security technology R&D over the past few years.

With respect to QKD, the requirement for authentication is well-appreciated. A very appealing solution will be to use quantum-safe asymmetric (public key) algorithms to authenticate QKD between transmitters (Alices) and receivers (Bobs) that have never met before. Even in a dynamic and evolving network scenario, this can provide long term quantum-safe keys through QKD, underpinned by an authentication algorithm that is only required to be quantum-safe at the specific time of use. The Quantum Communications Hub and other projects in the UK National Quantum Technologies Programme are already working on these hybrid solutions, and the standards to underpin them.

With respect to QRNGs, their significant appeal is the true unpredictability of their randomness. For this, it is clearly crucial to assure the "quantumness" of the source of entropy that underpins the randomness. Over the last few years the Quantum Communications Hub has been establishing the principles and processes for assuring the quantumness underpinning current QRNGs working closely with the UK's national metrology institution, the National Physical Laboratory, and in collaboration with industrial partners. We will be continuing this multi-disciplinary strand of work over the next five years (phase 2) of the Hub, alongside our drive towards future device-independent assurance. Such new QRNGs, alongside other quantum security technologies based on entanglement, will offer an even broader spectrum of assured security solutions in the future."

Hub investigators are keen to work together with NCSC (as per the recommendations of the UK Government Blackett review) and our many industry partners to run a number of field trials across the UK's Quantum Network, seeking to establish the most quantum secure solutions for our national infrastructure both in ICT and other sectors.

Interim Leadership Team for National Quantum Computing Centre announced

An interim leadership team, bringing together expertise and experience from across the UK's quantum technology sector, has been appointed to drive the development of the UK's National Quantum Computing Centre.

The centre, which is being created as part of the second phase of the UK's National Quantum Technologies Programme, will enable the UK to be a world-leader in quantum computing, bringing together academia, business and government to address key challenges of this disruptive new technology.

The leadership team will be responsible for designing the building and engaging with government, academia and industry in order to build a community which will work to enhance the UK's capabilities in quantum computing.

Members of the leadership team are:

- Professor Simon Benjamin, Professor of Quantum Technologies at the University of Oxford
- Dr Michael Cuthbert, Business Development Director and Quantum Technologies Sector Lead at Oxford Instruments
- Dr Simon Plant, Innovation Lead for Quantum Technologies at Innovate UK
- Ash Vadgama, Principal Computational Scientist at AWE PLC

Read more

Conference for Undergraduate Women in Physics 2020

The Quantum Communications Hub was proud to support the Conference for Undergraduate Women in Physics 2020, held at the University of York between 12th and 15th March 2020. The event brought together over 100 people who identify as women and had a programme packed with interesting and inspiring activities including excursions, workshops, keynote talks and panel discussions. Keynote talks were given by Prof Daniela Bortoletto, Prof Petra Rudolf, Sue Nelson and Dame Jocelyn Bell Burnell. Excursions included trips to the Advanced Manufacturing Research Centre at the University of Sheffield and the York Plasma Institute, and workshops included 'Unconscious Bias' and 'Engaging with the media' plus many more. Delegates also had the opportunity to attend academic and industry panel discussions. The academic panel featured Prof Marialuisa Aliotta, Dr Kate Lancaster, Prof Petra Rudolf and Prof Sarah Thompson, chaired

by Dr Marina Petri. The industry panel included Dr Heather Barton (EDF Energy), Sarah Dempsey (Peratech Holdco Limited), Leah Morgan (UK Atomic Energy Authority (UKAEA), Xanthe Jackson (BAE Systems) & Suzy Beanland (Darktrace), chaired by Beth Medley of the White Rose Industrial Academy.

**With credit to Paul Shields, University of York, for the photographs.*

QuantIC Accelerated Development Fund to Support Quantum Projects Now Open

QuantIC, the UK Quantum Technology Hub in Quantum Enhanced Imaging has announced a new £2m funding call to support universities accelerate innovation in quantum imaging in alignment with industry priorities and societal needs.

The Accelerated Development Fund (ADF) comprises of a total budget of £2M will be spread over two calls and will be designed to bring new research ideas into QuantIC. These university led projects will address a demonstrable industrial or societal need and will feed the pipeline of technology to be translated into industrial applications and commercial opportunities.

Key dates:

- **06.04.20** - Call opens
- **24.05.20** - Expression of interest deadline
- **01.09.20** - Application deadline

For full details including call guidance and application process, please go to the QuantIC website.

QUANTIC
The UK Quantum Technology Hub in Quantum Enhanced Imaging

UK-Canada Call for Joint Projects on Quantum Technologies

Innovate UK and the Natural Sciences and Engineering Research Council of Canada (NSERC) are partnering to launch a call for research proposals on quantum technologies. The call builds on complementary interests and research expertise in this area in the UK and Canada. This call will allow for the collaboration between leading-edge scientists and potential innovative users, from industry and/or government sectors, to accelerate the development of quantum technologies.

Read more

Knowledge Transfer Network Quantum Technologies Special Interest Group

The Quantum Technologies Special Interest Group (QT SIG) will help to maximise the return from the UK Government's substantial, multi-million investment since 2013 to commercialise quantum technology. The SIG is a delivery partner in the UK National Quantum Technology Programme and supports and connects researchers, technology developers and users to link markets and suppliers to create a self-sustaining and profitable world-class UK quantum technology sector. Visiting the link below will enable you to view SIG News, Events and Reports, along with signing up to the SIG newsletter.

QT SIG Webpage

Knowledge Transfer Network Quantum Technologies Global Expert Mission to the USA

A report on the KTN Quantum Technologies Global Expert Mission to the USA, in November 2019, has been published.

The report includes information and insights gathered by the delegation during the mission, which was part of Innovate UK's Global Mission Programme. The Programme aims to support the UK's Industrial Strategy's ambition for the UK to be the international partner of choice for science and innovation. The Global Missions led by the KTN play an important role in encouraging collaborations, which are crucial to meeting the UK's Industrial Strategy's Grand Challenges.

Read the report

Knowledge Transfer Network

Events

EPIC World Industrial Quantum Photonics Technology Summit

3-4 September 2020, University of Glasgow, UK

The purpose of the EPIC Industrial Quantum Photonics Technology Summit is to bring together the companies in the supply chain towards the commercialization of upcoming products resulting of the current R&D initiatives. The event includes sessions on: the quantum industrial revolution; quantum communication and QKD; quantum clocks technology and applications; quantum sensing and metrology; quantum imaging; quantum computing and also includes networking opportunities.

More info

Quantum Communications Hub
Information Centre, Market Square
(Department of Physics)
University of York
York YO10 5DD

enquiries@quantumcommshub.net