FUJITSU | Cambridge Quantum

Quantum resilience on software-based networks

Can software networks be protected in a post-quantum world?

Quantum computer attacks on encrypted data is a serious future threat that concerns all information processing systems, including the supporting networks that are critical to system connectivity and interoperability. Networks use cryptography and encryption for protecting their data, which must remain resilient against targeted quantum attacks. SD-WAN software-defined network capability has a pivotal role in supporting information systems that operate in cloud, with a large attack surface, including quantum. SD-WAN must be protected and assured in the post-quantum world, but are there any risks to their integration with Quantum Security Technologies?

The National Institute of Standards and Technology (NIST) and National Cyber Security Centre (NCSC) are the US and UK Government-leading organisations providing advice and guidance on the quantum threats and approaches for responding to these threats through papers and publications on their websites.

On 11 November in 2020, NCSC updated its 2016 whitepaper 'Preparing for Quantum-Safe Cryptography' with the latest guidance on mitigations to the threat of quantum computing advances to cryptography. NCSC's 24 March 2020 whitepaper 'Quantum Security Technologies' has stated the potential vulnerabilities of traditional public key cryptography algorithms to a future large-scale quantum computer, and the need for new approaches that eliminate these vulnerabilities.

In the US, NIST has been running a competition to identify the best quantum-proof encryption algorithm from using a number of different approaches. The competition has identified the following three 'families' of quantum-proof approaches and final submissions are undergoing further evaluation:

- **Lattice** – using geometric structures represented as mathematical arrays
- **Code-based** – using error-correcting codes
- **Multivariate** – a system of quadratic polynomial equations

The NCSC 'Quantum Security Technologies' paper also contains a positioning statement on the use of Quantum Random Number Generators (QRNGs), which generate random numbers that at ideal state are unpredictable, and construct entropy using quantum mechanical effects. The NCSC paper explains why commercial QRNGs have failed to provide value in terms of unpredictability, mainly due to the impact of electronic noise pollution on the quantum state and randomness.

The paper has encouraged further research in the following areas that includes the challenge of QRNG integration with larger systems:

- Modelling and evidencing real-world properties of physical QRNGs
- Engineering and integration of QRNGs into larger systems
- Understanding changes in behaviour of QRNGs under various physical stresses and through aging
- Vulnerability research to explore new technical risks

Fujitsu and Cambridge Quantum collaborate on QRNG Integration Research

Fujitsu is a global leading supplier of IT infrastructure, hosted applications and networking services. SD-WAN technology is strategic for hosted IT services on cloud, by enabling application-defined networking solutions to optimise performance and has other benefits such as edge routing and built-in security. The security enhancements for resilience against quantum attacks on SD-WAN solutions is therefore a major concern for Fujitsu, and has been instrumental to collaborations with Cambridge Quantum on a joint response to the NCSC's QRNG integration research challenge using the Fujitsu SDWAN system configuration.

Cambridge Quantum is a global leader in quantum software and quantum algorithms, enabling clients to achieve the most out of rapidly evolving quantum computing hardware. Cambridge Quantum's Quantum Origin key generation platform is based on the world's only source of verifiable quantum entropy. Unlike the QRNG solutions discussed in the NCSC paper, Quantum Origin creates cryptographic keys using quantum entropy unpolluted by electronic noise.

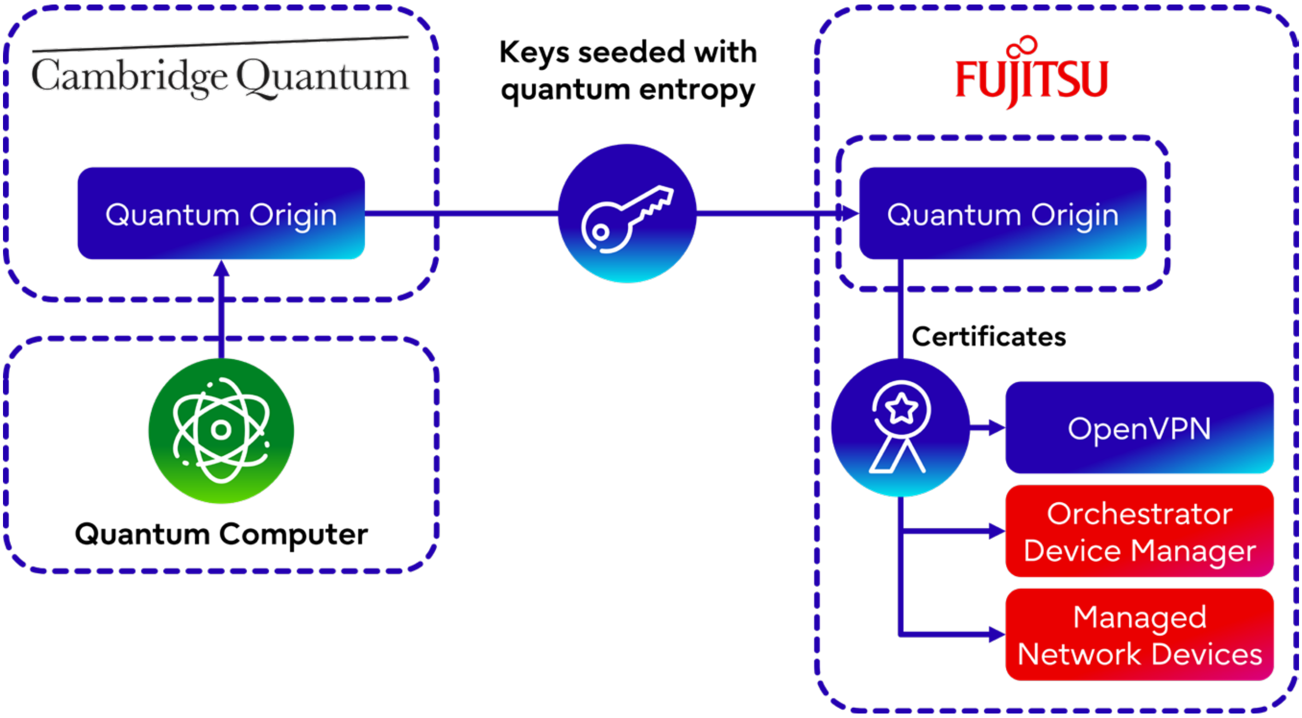
Fujitsu and Cambridge Quantum demonstrate QRNG Integration on the Fujitsu SD-WAN Solution

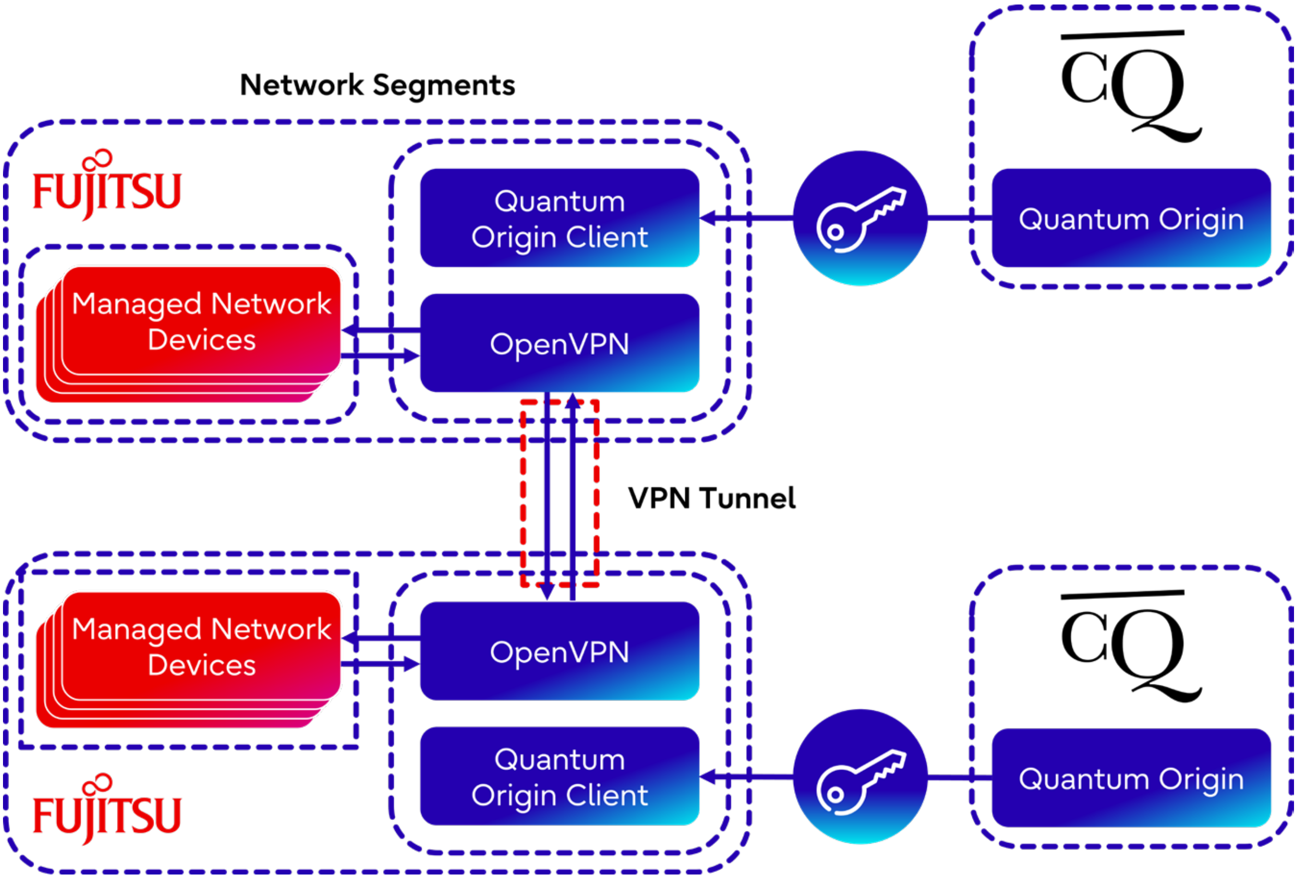
Fujitsu and Cambridge Quantum have recently completed their collaborations on a Proof of Concept (PoC) investigation for the integration of Cambridge Quantum's Quantum Origin key generation platform with the Fujitsu SD-WAN solution configuration.

The PoC demonstrates the successful integration of Fujitsu's SD-WAN solution configuration with the cloud-hosted Quantum Origin platform, responsible for generating keys using NIST and NCSC-approved classical cryptographic algorithms seeded with verifiable quantum entropy.

The following diagram is a high-level illustration of the integration architecture and the functional components provided by each company.

For the purpose of integration, the Fujitsu SD-WAN configuration has been adapted by replacing the native VPN with OpenVPN software. Specifically, the SD-WAN OpenVPN implementation uses OpenSSL, which obtains the keys seeded with quantum entropy over a simple web API distribution service from Quantum Origin. The keys are used in the generation of certificates in the OpenVPN and other Fujitsu SD-WAN network components. The following diagram shows the OpenVPN tunnel providing SD-WAN secure communications, based on the certificates generated using the Quantum Origin keys.





What are our future aims?

The PoC for quantum resilience is limited in scope to the network-centric security context of SD-WAN, and QRNG integration on classical cryptographic algorithms. The wider security contexts of Quantum resilience for custom applications and services data form the future aims for scenario-driven application-based PoCs. The future aims of quantum security technologies will be guided by NIST's recommendations on new solution methods, with new cryptographic algorithms that are not expected before 2022.

About the authors

Dr. Houtan Houshmand is the CTO Research Lead at Fujitsu. Houtan has 35 years of experience in IT architecture and systems design and over 13 years of research collaborations within a number of consortia. Houtan has been the technical lead and contributor to a wide range of research projects on the themes of Situational Awareness, Operational Logistics Decision Support, Information-Knowledge Management Systems and Enterprise Architecture capabilities. His specialisations and interests are in multi-modal agent-based systems with neuro-symbolic AI knowledge representations and ML in graph networks including Reinforcement Learning, Data Centric Security (DCS), logic-based reasoning and probabilistic decision models, synthetic environment modelling and simulation driven optimisations. Houtan is a Fujitsu Distinguished Engineer and holds a PhD in Computer Networks Modelling and Performance Analysis from the University of Manchester.

Duncan Jones is Head of Quantum Cybersecurity at Cambridge Quantum. He leads a team developing advanced cybersecurity products based on quantum technology, which deliver value today. Duncan has 14 years' experience in cybersecurity and has held senior technical and product-focused roles in companies such as Thales, Arm and Worldpay.

For more details and insights on the PoC and our wider initiatives on quantum resilience, please contact us.

Why Fujitsu in Defence & National Security

Our world is being disrupted. But together with you, Fujitsu's ambition is to build a brighter, more sustainable future for us all.

We want to work together to navigate this digital disruption collaboratively, and explore solutions to the evolving threats we face today. Together, we can exploit technology that will drive high-impact improvement, transform our digital future, and help to make us more sustainable in every way.

We can do this by harnessing technologies such as AI, machine learning, digital twin, quantum, and high-performance computing. Our vision uses the power of everyone, bringing together our integration capabilities and knowledge in managed services with cognitive and advanced technologies that will drive your digital transformation. By elevating people higher up the value chain allows the smartest ideas to emerge to tackle tomorrow's big challenges today – whatever they may be.

With our technological inspiration and business vision from Japan, we touch the lives of millions of people around the world every day. For over 60 years, we've been working at the highest levels of security demanded by militaries, governments, and industry to ensure the UK's most critical infrastructure operates smoothly, 24/7.

We've continually had to adapt to a changing world, and we will keep evolving in the face of future threats. We are diverse, creative, talented, and different. And we are committed to building new possibilities for everyone. By connecting people, technology and ideas, we are making the world more sustainable by building trust in society through innovation.

Contact
+44 (0) 870 242 7998
ask.fujitsu@fujitsu.com
Ref: 4196
uk.fujitsu.com