Case Study

Vodafone Tests Quantum-Safe Business Network with Upgraded Smartphones

vodafone

SANDBOXAQ

Partner

Vodafone Group

www.vodafone.com

Industry

Telecommunications

Organization Size

104,000+

Products & Services

Voice, messaging, and data services across fixed and mobile networks.

Country

United Kingdom

Working to protect customers, governments, and society from Store Now, Decrypt Later (SNDL) attacks by testing new cryptography algorithms

Millions of times a day, people trust technology to keep their data safe. Emails, messaging apps, online banking, internet shopping and secure links for governments and large businesses — they all rely on public-key cryptography to establish secure communication channels and protect sensitive data.

The security of these public-key methods relies on the difficulty of solving certain mathematical problems. However, the emergence of fault-tolerant quantum computers, able to undertake far more complex processing tasks than a traditional computer, poses a risk. This step-change in processing power has the potential to crack today's codes, decimating the trust and security on which current technology is built.

The quantum risk is part of the ever-evolving security threat landscape that Vodafone is working on with technology partners and industry body, the GSMA. Together, they are exploring quantum-safe defenses to help protect customers, governments, and society at large from any future threat.

Emma Smith, Vodafone's Cyber Security Director, explained: "On one hand quantum computing has the potential to rapidly solve ultra-complex problems in key areas such as healthcare, but on the other it could undermine today's cryptography.

© SandboxAQ. Vodafone Group

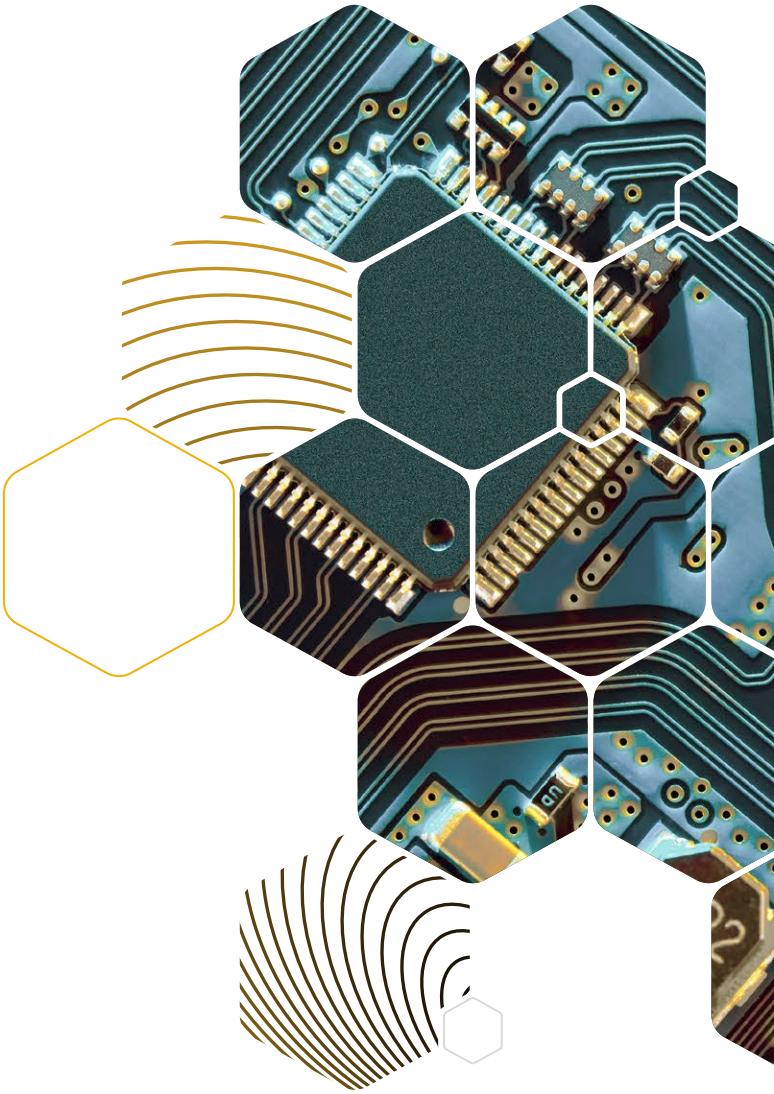
"This is why we are playing an active role in the transition to a quantum safe world. We are exploring and trialing new algorithms to provide protection for our customers against possible quantum-empowered attackers in the future."

Vodafone and Sandbox AQ test upgraded smartphones on business network

Among a raft of initiatives designed to anticipate and safeguard against future threats, Vodafone joined forces with SandboxAQ (a spin-off from Alphabet) to conduct a proof-of-concept test for a quantum safe Virtual Private Network (VPN) — a type of network used by millions of workers to securely access company systems via their devices.

The test was conducted using standard smartphones, connected to the VPN, that had been specifically adapted by Vodafone/SandboxAQ using cryptography algorithms from The National Institute of Standards and Technology (NIST). NIST is part of the U.S. Department of Commerce, and it has developed a framework of standards for national or corporate cyber security practices.

Adapting a standard smartphone for the test allowed Vodafone/SandboxAQ to evaluate the latest NIST standards in a real-life telecommunications scenario.



© SandboxAQ. Vodafone Group

> Although cryptographically relevant quantum computers may remain some years off, the threat posed by quantum-empowered attackers is already here today.
>
> **Luke Ibbetson,** Head of Research and Development

Store Now, Decrypt Later

Governments are adopting NIST standards as part of their planning to mitigate the potential risk Quantum Computing poses today. One of those risks is SNDL.

Vodafone's Head of Research and Development Luke Ibbetson said: "The Store Now, Decrypt Later attack involves adversaries stealing encrypted data now so they can decrypt it in the future with a quantum computer. Although cryptographically relevant quantum computers may remain some years off, the threat posed by quantum-empowered attackers is already here today."

According to some online reports, threat actors may already be harvesting data in anticipation of the quantum computing revolution. Although there is no hard evidence that long-lived sensitive data, such as government records, corporate intellectual property, and even individual biodata, may already be at risk, Vodafone has started work on this now by testing new cryptography in partnership with key industry players.

While it's true this will not protect vulnerable data which may have been already harvested and stored for future decryption, Vodafone believes in taking the necessary steps now to mitigate as much risk as possible going forward. Its goal is to work in tandem with partners to migrate data in an orderly fashion to suitable, post quantum cryptographic methods now to protect customers, governments, and society from future SNDL attacks.

© SandboxAQ. Vodafone Group

Protection Against Quantum-empowered Attackers

Known as post-quantum cryptography (PQC), these algorithms leverage new mathematics and methods to offer quantum safety and are the subject of ongoing standardisation processes. Vodafone has taken a leading role in the GSMA's newly established Post-Quantum Telco Network (PQTN) task force to help develop industry-wide strategies and planning to address the quantum threat. One of the first outputs from this task force was the publication of a white paper in early 2023, discussing the quantum threat and outlining the telco-specific implications. In this context, Vodafone is working with a variety of technology partners, from specialist startups in quantum technologies to established industry leaders.

Quantum-Safe Virtual Private Network

In addition, Vodafone is exploring the performance characteristics of the post-quantum algorithms. Different types of post-quantum cryptography can have varying performance

© SandboxAQ. Vodafone Group

Vodafone established its first ever quantum-safe VPN, using new technology and customised SandboxAQ software

characteristics, which may impact existing communications processes such as voice calls or web browsing and telecommunications infrastructure.

To better understand these performance characteristics, Vodafone continues to work on several real-life scenarios such as the one with SandboxAQ.

The Vodafone-SandboxAQ quantum-safe VPN project assessed the impact of PQC algorithms on this key telecommunications service, without compromising the customer experience. During the project, Vodafone established its first ever quantum-safe VPN, using new technology and customised SandboxAQ software for quantum-safe internet protocols and analytics.

Vodafone engineers conducted a series of experiments to test several scenarios, including connecting the modified smartphones to a server and site-to-site connections to replicate a link between head office and local branches.

Post-Quantum Cryptographic Smartphones

Luke added: “The experiments involved the assessment of both synthetic traffic and real data sessions made by internal volunteers from several countries in which we operate, together with the project team.

“We tested the impact of post-quantum cryptography on activities many of us do every day. These included web browsing, social media and chat application use, video and audio streaming, and mobile gaming using PQC-enabled mobile handsets, helping to test network performance and assess the user experience.”

Useful Insights

Multiple PQC algorithms were tested, revealing strengths and weaknesses of the distinct PQC algorithm classes. Thorough testing demonstrated that

© SandboxAQ. Vodafone Group

hybrid cryptographic approaches, composed of classical and best-fit PQC algorithms, had minimal impact on the quality of service, while still achieving post-quantum security.

Moreover, the best-fit PQC algorithms selected for standardization by (NIST) were found to perform well in the telecommunications setting. These PQC algorithms had relatively little impact on the quality of service for users of both smartphones and fixed broadband services. The findings support the use of hybrid classical/PQC algorithms for the security processes that use a cryptographic key exchange, protecting against SNDL attacks and providing useful insights around implementing PQC algorithms in vital telecommunications infrastructure.

A second group of PQC algorithms, namely for digital signatures, is being considered by NIST in a new standardisation process, beginning June 2023. The Vodafone and SandboxAQ project findings demonstrate that, in the meantime, traditional digital signature algorithms can be used in concert with hybrid key-exchange mechanisms in a VPN (and related contexts such as quantum-safe software-defined wide area networks) to ensure protection against a SNDL attack.

© SandboxAQ. Vodafone Group

Post-quantum cryptography offers protection against quantum threats such as SNDL and future attacks on the cryptography used to secure many types of communication. However, the transition to implement PQC will take time and resources. We think it's important to start acting now. Vodafone continues to actively test new solutions with companies such as SandboxAQ and combine its work with broader industry groups to address the need for global standards to protect society worldwide.

Global team of 900 cyber security experts

"The cyber risk remains volatile. Every day our global team of 900 cyber security experts draw on their rich technical skills, inquisitiveness, and motivation to protect our customers and society at large," Emma Smith said.

"We work on everything from the cyber security of our networks, and securing both business and consumer products and services, to collaborating with standard bodies on critical topics such as PQC implementation."

Vodafone's scale means it benefits from global collaboration, technology sharing and deep expertise, and ultimately having greater visibility of emerging threats. It also means Vodafone is in a prime position to leverage the huge potential benefits of quantum technology, for example, to provide improved network optimisation that existing computers will never achieve alone. This will allow it to save energy, reduce costs and give customer great connectivity in more places.

© SandboxAQ. Vodafone Group