# On the Radar: Quantum Xchange provides a quantum-proof cryptography solution

Preparing for a new world of cryptography as we get closer to Q-day

Publication Date: 28 Jun 2018 | Product code: INT003-000142

Roy Illsley

# Summary

## Catalyst

The quantum computing advances made over the past couple of years (IBM has a 50-qubit and Google a 72-qubit quantum computer) have led to the pronouncement of "Q-day" – the day a quantum computer will be able to break any current encryption in seconds. The National Institute of Standards and Technology (NIST) is working on an algorithmic approach to developing the next generation of encryption, but will not announce any possible solution until 2023 at the earliest. This report explores how a new and different approach of quantum key exchange can provide a quantum-resistant security solution today.

## Key messages

- Quantum Xchange provides a secure way to protect data in a post-quantum computer era.
- Quantum Xchange uses trusted nodes to extend the range of a dark fiber network so that it can transmit a photon over 100km.
- Quantum Xchange plans to launch its service in New York in 2018 and extend it in key geographic locations.

## Ovum view

The post-quantum computer challenge is to find a solution that a quantum computer cannot decrypt. The current encryption algorithms are based on prime factors, which is precisely the sort of problem a quantum computer is ideal to solve. This has led to the concern that a threat (e.g., individual hacker, terrorist group, or rogue nation) with access to a powerful enough quantum computer could render current-day encryption obsolete.

While quantum computing is still a research project, working quantum computers are being made available by Microsoft, Google, and IBM for developers to work on generating the applications needed to make quantum computing a commercial prospect. Quantum Xchange has developed a solution based on quantum key distribution (QKD) that it claims is unbreakable.

# Recommendations for enterprises

## Why put Quantum Xchange on your radar?

The fact that a 100-qubit working quantum computer will be available, even if only in a research lab, by 2019 demonstrates that it is not a question of if, but when, current encryption will be broken in seconds. Quantum Xchange has developed a QKD solution using dark fiber transmission that will operate at distances greater than 100km. Its solution provides a secure solution to encrypting data at rest or in transit, and its offering will be available as a service, but does require the purchase of specialist hardware. However, the current encryption technologies used by an organization can be used in conjunction with Quantum Xchange.

# Highlights

The Quantum Xchange solution uses photons of light to transmit key data, and uses this key to encrypt the information. The limitation is on the transmission of the photons it uses to send the keys; the photons can be sent over distances greater than 100km.

The premise behind the QKD approach is based on Heisenberg's uncertainty principle, which states that the very act of observation affects the observed. This can be roughly translated as: if a photon (consider it a carrier of the key information) is observed by a third party (somebody has intercepted the key), then this will alter the velocity of the photon, which means the recipient knows the transmission has been observed (somebody has attempted to read the encryption key). The quantum key encryption means that even though the message has been observed, the act of decrypting it is impossible as QKD protocols are used for transmitting the keys for encrypting data, and these do not follow classical mathematical algorithms. QKD security relies on the laws of quantum mechanics, and more specifically on the fact that it is impossible to gain information about non-orthogonal quantum states without disturbing these states – Heisenberg's uncertainty principle. This property can be used to establish a random key between two users, commonly called Alice and Bob, and guarantee that the key is perfectly secret from any third party eavesdropping on the line, commonly called Eve.

# Background

Quantum Xchange was publicly launched in April 2018; it is headquartered in Bethesda, Maryland, and backed by New Technology Ventures. Quantum Xchange developed the trusted node technology that can extend the QKD range to over 100km. Quantum Xchange was founded by serial entrepreneur John Prisco, who is the current president and CEO.

# Current position

The Quantum Xchange solution of QKD is based on four core components that can extend the range of transmission to greater than 100km.

## Quantum key distribution network

Quantum Xchange is planning its first network to match the financial markets in New York connecting the Wall Street offices with the New Jersey-based back-office operations for the banks. The quantum keys are transmitted via the quantum key network based on fiber-optic cables and using photons as the vehicle for transmission. The encrypted data is sent over the existing network, but unlike traditional encryption, the keys cannot be broken as they are randomly generated secret keys that are only known by the sender and receiver in a point-to-point communication.

## The hardware

To make the QKD network secure requires that a pair of hardware components, rack mounted, are required at the "transmit" and "receive" points of the network. The hardware is used to join the encrypted data, using current RSA technology, with Q key via an exclusive (XOR) gate. The XOR gate implements an exclusive "or"; that is, a true output results if one, and only one, of the inputs to the gate is true.

### Delivered as a service

The dark fiber network is operated by Quantum Xchange as a service provider, and the quantum keys are multiplexed over this network to reduce operating costs. The encrypted data is transmitted over the customer's existing network separate from the dark fiber. The customer has a one-off installation fee, effectively paying for the hardware, then paying a monthly subscription for unlimited use of the keys based on different lengths of contract from one to five years.

### Trusted node system

Due to the limited amount of energy a photon has, the distances that can support photon transmission are relatively short, and introducing intermediate nodes can make the entire chain susceptible to attack. Quantum Xchange has developed a trusted node network where each node has a quantum key controller and quantum key engine to ensure the transmission remains secure and extends the key distribution length beyond 100km and enables nationwide coverage.

# Data sheet

## Key facts

**Table 1: Data sheet: Quantum Xchange**

| | | | |
|---|---|---|---|
| **Product name** | Quantum Xchange | **Product classification** | Encryption |
| **Version number** | | **Release date** | 2018 |
| **Industries covered** | All | **Geographies covered** | US, with Canada, UK, EMEA, and Australia targets for expansion next |
| **Relevant company sizes** | All | **Licensing options** | Subscription |
| **URL** | www.quantumxc.com | **Routes to market** | Mixed |
| **Company headquarters** | Bethesda, Maryland, US | **Number of employees** | 20 |

Source: Ovum

# Appendix

## On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

## Author

Roy Illsley, Principal Analyst, Infrastructure Solutions

roy.illsley@ovum.com

## Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

## Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

## CONTACT US

ovum.informa.com

askananalyst@ovum.com

## INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo