REPORT REPRINT

There's nothing random about QuintessenceLabs' strategy

FEBRUARY 04 2020

By Owen Rogers

QuintessenceLabs employs quantum tunneling to create uncrackable random codes for use in its range of key management offerings. It continues with its partnerships and proofs of concept to make QKD mainstream, but is also addressing security concerns with the launch of a quantum entropy enhancer.

Introduction

QuintessenceLabs (QLabs) employs quantum tunneling to create uncrackable codes for use in its range of key management offerings. It continues to move quantum key distribution toward the mainstream with its partnerships and proofs of concept, and is addressing security concerns with the launch of a quantum entropy enhancer and its existing key management portfolio.

451 TAKE

QLabs is showing that microscopic entities can have a macro impact on technology. It has a compelling offering with its key management, random number generation and hardware security module. With the addition of a quantum entropy enhancer, the company is taking advantage of quantum effects today, with the commercial potential for organizations to transmit keys through free space with certainty that they have not been intercepted via its quantum key distribution technology. It is still early, however, and huge steps need to be made around education and justification of quantum technology's deployment to make it mainstream.

Details

Founded in 2008, QuintessenceLabs has about 60 employees across its headquarters in Canberra, as well as offices in Brisbane, Australia, and San Jose. It has raised about $21m in funding from investors such as Australian bank Westpac. The company also has a UK support operation.

QuintessenceLabs employs quantum tunneling to create uncrackable codes for use in its range of key management offerings. At its core, the Australia-based startup was built around innovations in quantum key distribution (QKD) in the form of its qOptica product. In parallel, the company has developed the use of quantum tunneling to create random numbers for use in encryption purposes in its qStream offering, as well as a key management system called qCrypt. QLabs' qCrypt is an interoperable key and policy manager, and qStream is the random number generator based on this quantum tunneling process.

Over the past six months, QLabs claims increasing interest as a result of increased media coverage of innovations in quantum computing. This tallies with the experience of our Quantum Center of Excellence analysts. Announcements from IBM, Microsoft, Google and Amazon appear to have brought quantum computing into focus with enterprises that now see it as less of an R&D project firmly embedded in universities, and more of an opportunity – and threat – waiting around the corner. QKD provides one method of defense against quantum computers being used to hack encryption keys.

QLabs' new focus in this regard is to provide enterprises with key management capabilities that can be easily extended in the future to manage quantum-resistant algorithms as they become available (as quantum computing becomes more mainstream). Both qCrypt and qStream provide this key management capability, with the option of deploying QKD in the form of qOptica.

QLabs recently launched a quantum entropy enhancer called qRand. Entropy essentially refers to the 'randomness' of data. When generating keys, we want the keys generated to be unpredictable – if an external party can guess the key, perhaps based on past keys or a data source that was used to produce the random data, then the whole system breaks down. A secret key that a hacker can guess or predict isn't so secret. Generating truly random numbers is surprisingly difficult, and the algorithms used to generate them can fall into patterns of predictability or even fail to generate numbers altogether, which can slow performance.

QRand monitors a stream of pseudorandom numbers and determines the entropy. If the entropy drops below a threshold, it populates the stream with further random numbers generated from a quantum tunneling process embedded in its qStream product. The company has won a deal with a major US-based financial institution to deploy qRand and qStream.

QLabs is also working with the ITU-T as part of industry consortium Quantum Alliance to establish standards for QKD to encourage interoperability, and it is investigating encryption algorithms that are resistant to quantum computing attacks. The company believes that, in the long term, all random numbers will be generated deploying quantum technology. Partners include PKWARE, VMware, NetDocuments and AppViewX. Industry segments targeted include banking and financial services, government, defense, and cloud. It will be participating in the World Economic Forum in New York in May.

In 2019, the company deployed a QKD network to the Australian Department of Defence and provided the key management capabilities to secure a QKD video conference connection with BT and Tech Mahindra. In 2020 it expects to have three QKD proofs of concept in place. It is also partnering with a third-party QKD provider to deliver a high-entropy QKD network to a continental space agency.