REPORT REPRINT

QuintessenceLabs 'tunnels' into the quantum key opportunity

MARCH 21 2019

By Owen Rogers

The Australia-based startup is using quantum tunneling to create uncrackable codes. At its core, QLabs was built around innovations in quantum key distribution.

Summary

QuintessenceLabs (QLabs) is employing 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.

451 TAKE

QLabs is showing that microscopic entities can have a macro impact on technology. It has a compelling offering with regards to its key management, random number generation and hardware security module (HSM). But the vendor is on track to have a commercial offering that allows keys to be transmitted through free space with certainty that they have not been intercepted. It is early days, however, and huge steps need to be made around education and justification of quantum technology's deployment to make it mainstream.

Context

Founded in 2008, QuintessenceLabs has about 60 employees across its headquarters in Canberra as well as offices in Brisbane and San Jose. It has raised about $21m in funding from investors that include Australian bank Westpac. Plans for a UK sales and support operation are also underway.

In parallel with qOptica, the company has developed the use of quantum tunneling to create random numbers for use in encryption purposes in its qStream offering and 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. An HSM ensures secure key storage. Encryption is only as good as the random numbers used to generate the keys. Pseudo-random numbers (perhaps constructed from the time) may be predicted by a hacker if the time is known, which makes the key more vulnerable. The startup's method is truly random and should be unpredictable to any malicious entity. It sells the technology as an appliance, with subscription support, and claims that its key manager with a quantum random number generator (QRNG) embedded in it is about the same price as similar devices without a QRNG.

The blue-sky opportunity is qOptica. Our primer on quantum security showed how keys can be distributed using quantum particles, such that if they are intercepted, the receiver is made aware. QLabs is halfway through a three-year proof of concept (POC) with the Australian government to do exactly this, using fiber optics as the medium. A free-space version (which transmits data via high-powered lasers) is also underway. The company employs momentum and phase spin as the quantum encoding mechanism, which it claims reduces costs through the deployment of off-the-shelf components.

QLabs is also working with the ITU-T as part of industry consortium the Quantum Alliance Invitation 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 longer 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.

Quantum tunneling

In our primer on quantum computing, we referred to Schrödinger's Cat: when trapped in a box at the mercy of radioactive decay, we can't tell the state of the cat (alive or dead) until we open the box and measure it. Thus, we can say that the cat is in a state of superimposition. It is both – and neither – alive and dead.

In fact, we can go a step further and say that the cat's state is subject to a waveform of different probabilities. In our cat example, the waveform consists of two states, both with a probability of 50%, but – depending on the scenario – the waveform could consist of any number of states with any number of probabilities. The waveform 'collapses' to a definite state when we measure it.

This is where it starts to become a bit bizarre. Now imagine a quantum particle in a sealed, boxed space. It is constantly moving – we can't measure precisely where it is, we can just measure the probability of it being somewhere in that space. In a really big box, the chance of the particle being at a specific location would be pretty tiny. Thus, the waveform of probabilities would be huge, representing all of the places in the box it could be, and the probability of it being at each of those places. What is the probability of the quantum particle being outside the boxed space? Rationally, you would think zero – it can't escape the box space. But because the waveform captures all of the possibilities, there is a chance – a tiny chance – that the particle will appear outside the box. The particle 'tunnels' through the box wall, but it's probably fairer to say that it 'borrows' energy and spontaneously appears outside the box.

This is the mechanism that QuintessenceLabs uses to create random numbers. In a diode, an electronic component that restricts current flow to a single direction, electrons shouldn't be able to flow backward. But occasionally, an electron can appear in the wrong direction because the waveform dictates that there is a tiny probability that the electron will jump the barrier in the diode. When exactly this jump happens is totally random, based on the uncertainty in the laws of physics. Thus, it is a perfect method of generating random numbers that are impossible to predict, unlike pseudo-random numbers based on things such as time.

Competition

QuintessenceLabs rivals such as ID Quantique, Quantum Exchange (which is building a QKD network under the Hudson River in New York City), MagiQ Technologies, Sequrenet and SecureRF currently employ quantum technologies in the secure communications arena, but QKD is generally still an area of research by the likes of Toshiba, Mitsubishi, NEC, NTT, Huawei and IBM. Partnerships with telcos such as BT, Telefonica and UPM demonstrate the commercial interest.

The US Defense Advanced Research Projects Agency (DARPA) has run a 10-node QKD network since 2004, and the EU has its SECOQC project, which links six sites over a fiber network. China is getting in on the act as well, operating a satellite-based quantum channel from China to Vienna with a link of 4,700 miles using its QUESS space mission. A fiber-optic network provides the validation, and the project is aiming for a global QKD network enabled by 10 satellites by 2030.

The highest bandwidth currently achieved by a QKD network is 1Mbps over 12 miles of optical fiber and 10Kbps over 62km of fiber. Signal noise is a major problem, which reduces the distance achievable. Repeaters that resend the signal at regular intervals are one solution, but they aren't ready for widespread deployment today.

SWOT Analysis

STRENGTHS

QLabs is trialing QKD technology with the Australian government, and has established a niche with its quantum key management.

WEAKNESSES

It's early days, and there are huge challenges of education. QLabs should consider how it can materially demonstrate that the value of quantum number generation is better than 'pseudo-random is good enough.'

OPPORTUNITIES

The company hasn't rested on its laurels and has an active POC in place. When quantum technology becomes more desired by enterprises and governments, it will be in a good position to capitalize.

THREATS

Quantum solves some problems in data security, but poorly implemented crypto and human error will continue to be challenging.