Quintessence Labs

WHITE PAPER

Living in a Quantum-Safe World

With Quantum Computers on the horizon, QuintessenceLabs is taking a three-pillar approach to support organizations seeking to build quantum safety.

Overview

Computing technology is advancing rapidly, with the full potential of quantum computing on the horizon. Leveraging the power of quantum physics, quantum computers will be able to handle highly complex calculations in a fraction of the time required by today's best supercomputers.

While exciting, this future has its dark side. Given the speed and power of quantum computers, and their ability to solve the mathematically complex problems on which some of our security systems are based -- particularly key exchange protocols -- cybersecurity experts have raised the alert that they will easily defeat the defenses used to secure our data today. The implications are huge, and the race is on to devise, mature and deploy cybersecurity measures that can be a match to a quantum attack. The question then is, how can today's businesses make their security infrastructures safe for "post-quantum" world?

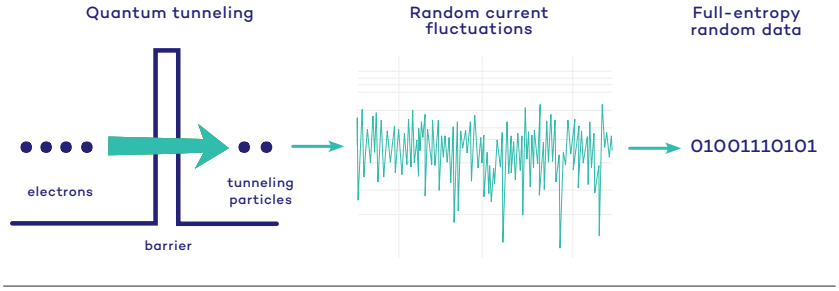
At QuintessenceLabs, we are taking a three-pillar approach to quantum safety to help enterprises lay strong foundations for the quantum future.

1. Use True Random Numbers

Cybersecurity starts with strong encryption keys, and being quantum-safe means protecting data with keys that are as strong as possible. These should ideally be "full entropy", or truly random keys. Traditional deterministic RNGs may not have sufficient entropy to remain secure when under a quantum attack. Integrating full entropy keys into your security architecture is an important first step to building quantum safety.

Fortunately, this technology is readily available and can be easily integrated. For example, QuintessenceLabs' qStream generates random data by measuring quantum tunneling noise. Quantum tunneling is a phenomenon in which a particle travels across a barrier that—according to classical mechanics—it should not be able to cross.

Inside the QRNG, a voltage is applied to a forward-biased diode junction. The diode contains a barrier through which charge carriers can "tunnel" even if they lack the energy to overcome the barrier according to Newtonian physics. The number of particles that will tunnel through in a given instant in time cannot be predicted, making the process an ideal source for random data.



Quantum tunneling delivers the highest quality entropy at high speeds

Quantum tunneling creates random fluctuations in the current flowing through the diode. These fluctuations are measured, digitized and digitally processed to generate ultra-high bandwidth random numbers. Full-entropy data is generated at 1Gb/second, suitable for use in any cryptographic application.

This type of capability will be necessary regardless of the encryption type used – whether symmetric encryption with longer keys, which will likely remain resilient to quantum attacks, or when deploying new quantum-resistant algorithms, which are currently being investigated.

2. Integrate New Encryption Algorithms in a Crypto-agile Environment

Cybersecurity relies on several industry-standard encryption algorithms such as RSA, AES, and ECC, each proven to perform to a certain level of protection and with different target uses. Symmetric encryption algorithms used to protect data at rest, such as AES, are expected to remain secure in a quantum world as long as longer, full entropy keys are used. However, asymmetric algorithms used for key exchange, such as integer factorization (RSA), discrete logarithm (DH, and DSA), and elliptic curve (ECC) will no longer be safe, since quantum computers will be able to break the type of math used to secure them. One response to this involves implementing post-quantum algorithms, which will use mathematical structures such as lattice-type algorithms that are resistant to quantum attacks.

NIST is currently managing a program to evaluate the best protocols and plans to publish standards on this topic. The standards are not expected to appear in a draft form until 2022 at the soonest. Be warned that they will typically require significantly larger keys than used today, and will take more processing time. Furthermore, there is always the possibility that new routes of quantum attacks are discovered that the new algorithms will be vulnerable to, requiring ongoing adjustments.

Whatever form these protocols take, they will need to be embedded into an overall security structure that can manage keys and policies effectively, as today. An important part of building quantum safety is to ensure that the key management solutions that you are deploying today have the built-in flexibility to manage different types of keys and integrate these new solutions as they become available, this capability is commonly known as "crypto-agility". Crypto-agility is the second pillar in QuintessenceLabs' approach, and is an important and integral part of QuintessenceLabs' qCrypt product suite.

3. Protect Key Exchange using Key Wrapping & Quantum Key Distribution

Secure key management requires replication nodes – additional servers with the ability to replicate copies of keys should part of the system fail for any reason. The transfer of data between replicating nodes typically happens over a mutually authenticated TLS connection, which includes using RSA or ECC asymmetric encryption for the initial key exchange handshake. This part of the TLS connection will be vulnerable to quantum attacks. Symmetric key wrapping can protect this: a true random number can be used to make a symmetric key that "wraps" a payload (the RSA/AES key or another object), resulting in an extra-protected TLS transfer.

Some key management solutions, including QuintessenceLabs' qCrypt, already include this symmetric key wrapping as part of their standard offering, protecting this in-network key exchange from current and future quantum threats.

More broadly, quantum key distribution (QKD) technology can be integrated into the security architecture to enable the secure exchange of keys without relying on quantum resistant algorithms. Instead, the laws of physics are harnessed to protect the key exchange, delivering the best future proof security for the most sensitive communications links. This type of technology can even support one-time pad (OTP) encryption, using high speed true random from a quantum source as the encryption "pad."

The security threat of quantum computers is very real, and actions need to be taken soon both to protect sensitive data from future attacks, and more immediately, to secure it from harvesting attacks that intercept it and store it for later decryption by a quantum computer. The good news is that multiple facets of quantum resistant cybersecurity are already available -- and thoughtful, systematic implementation of our three pillars can effectively keep an organization's business strong and operating for the long term.

Get in Touch

QuintessenceLabs has formed proven partnerships with a variety of enterprises, where our quantum-based encryption and key management solutions have effectively strengthened the data protection across entire organizations. We secure data so you can focus on what you do your best. Send us a message at **quintessencelabs.com** for sales information or to request a demo.

©2019 QuintessenceLabs. All rights reserved.

Quintessence Labs

AUSTRALIA
Unit 1, Lower Ground
15 Denison St
Deakin, ACT 2600
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com

Document ID: 3785