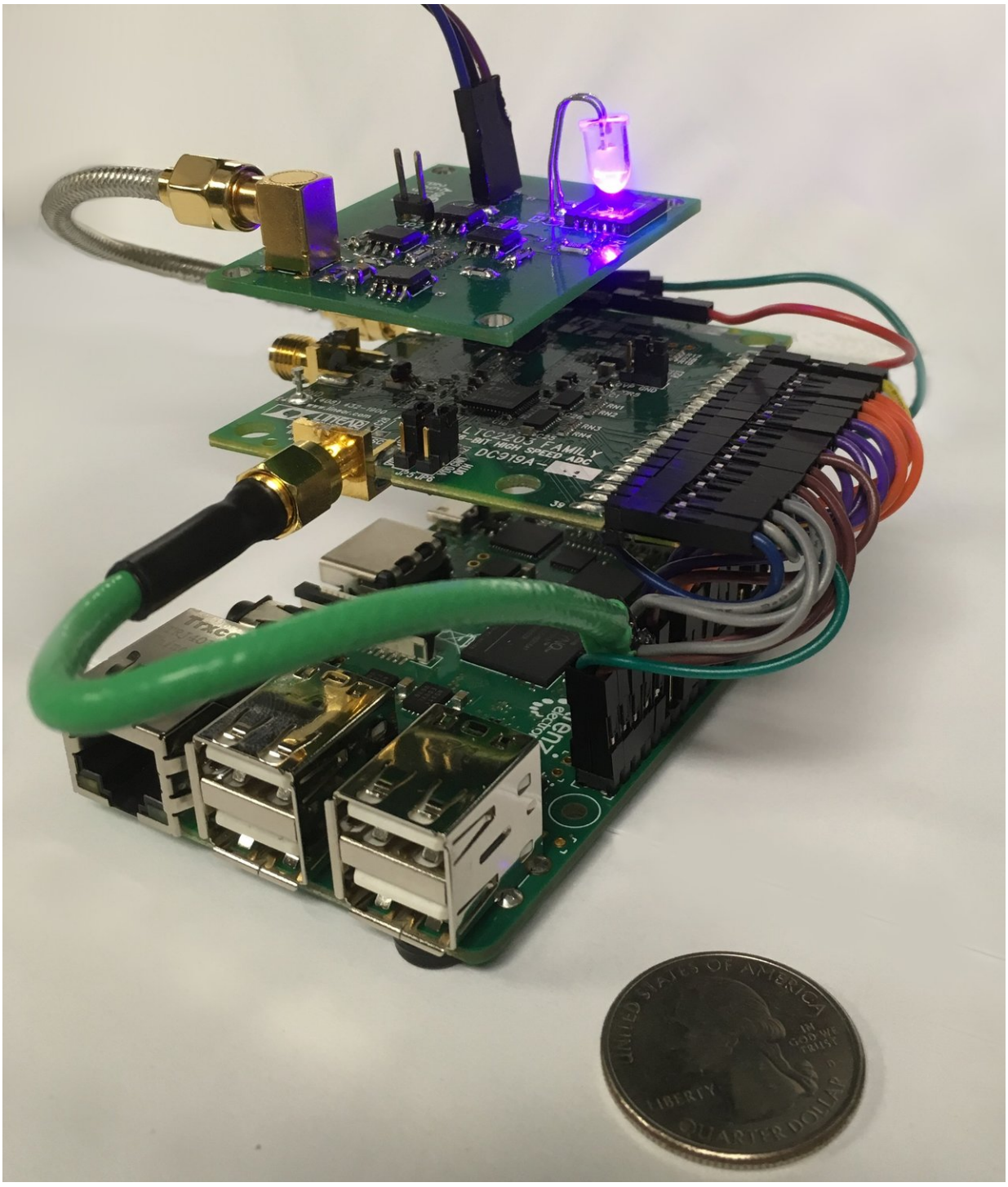
Qrypt licenses ORNL's quantum random number generator to fortify encryption methods

August 27 2018, by Sara Shoemaker



Development of ORNL's quantum random number generator began with basic components including an LED light, the source from which a field of quadrillions of photons are produced. The device can detect and measure the quantum statistics of photons present in the field and use each one as the basis

for creating truly unique encryption keys that are impossible to decipher or predict. Credit: Brian Williams/Oak Ridge National Laboratory, U.S. Dept. of Energy

Qrypt, Inc., has exclusively licensed a novel cyber security technology from the Department of Energy's Oak Ridge National Laboratory, promising a stronger defense against cyberattacks including those posed by quantum computing.

Qrypt will incorporate ORNL's quantum random number generator, or QRNG, into the company's existing encryption platform, using inherent quantum randomness to create unique and unpredictable encryption keys enabling virtually impenetrable communications.

The advent of quantum computing offers a fundamentally new approach to solving some of the world's most difficult and pressing problems. However, quantum computing will also render current encryption methods obsolete and require a reimagined, quantum-based approach to protecting data.

"The cryptography we have developed is based on true quantum sources of entropy and is mathematically proven to be unbreakable—even in theory," said Denis Mandich, Qrypt's chief technology officer at the company's New York City office.

"Until recently, this class of technology was unavailable at the scale required to encrypt Internet-sized datasets," Mandich said. "Simply relying on increasing the complexity of cryptographic algorithms has again proven to be a failing bet."

ORNL's research is integral to Qrypt's hybrid approach: combining

quantum physics hardware with post-quantum cryptographic algorithms and software. "We anticipate a long and productive partnership with one of the nation's premier labs as we continue to develop secure computing technologies," he added.

One method for successful, failsafe encryption will come from encoding messages with encryption keys that are truly random. That is, there is no realistic chance the exact key sequence used could be generated more than once.

ORNL's Michelle Buchanan, left, and Qrypt founder and CEO Kevin Chalker signed a licensing agreement for novel cyber security technology that promises a stronger defense against cyberattacks including those posed by quantum computing. Credit: Carlos Jones/Oak Ridge National Laboratory, U.S. Dept. of Energy

To harness quantum's perfect randomness, ORNL coinventor Raphael Pooser and his colleagues from the lab's quantum sensing, computing, and communications teams developed a quantum random number generator that detects the presence and characteristics of electro-magnetic waves, called photons, streaming from a light source.

"A field of quadrillions of photons are produced and pass through a beam splitter," Pooser said. "Different from other QRNG technologies, our method does not require that we wait for a single photon to appear, but allows us to use the collective statistics of large numbers of them."

The ORNL device can detect and measure the quantum statistics of photons present in the field and use each one as the basis for creating truly unique encryption keys that are impossible to decipher or predict.

"While true and quantum random number generators have been available for years, they were impractical to incorporate into server size appliances and their output was always very limited," Mandich said.

ORNL's scientific achievement can be proven based on quantum entropy, a purely probabilistic effect, he said.

"Many competing technologies advertise true randomness and pass modern statistical testing, yet there is no guarantee they do not have a pattern discoverable in the future," said Mandich.

"Historically, patterns, predictability and repetition are a critical flaw for many crypto systems, allowing them to fall to basic cryptanalysis," he added.

Qrypt will incorporate ORNL's technology into a suite of quantum-resistant encryption techniques and technologies, including a card or chip enabling quick encryption of vast datasets. Data protected by this

technology will be secure against attack by quantum computers or any future computational device and developments in the mathematics of cryptanalysis.

Provided by Oak Ridge National Laboratory