Whitewood Announces the Awarding of a U.S. Patent for Quantum Key Management

January 25, 2017

Whitewood, a developer of solutions focused on improving the use of cryptography, is pleased to announce that the U.S. Patent and Trademark Office (USPTO) granted a new patent entitled, *Quantum Key Management*. The patent, designated number 9,509,506, addresses the critical issue of identifying, authenticating, verifying, and exchanging secret cryptographic keys when employing quantum communications techniques designed to address the emerging threat of quantum computers.

The security systems that we use today such as internet encryption, credit card payments, email encryption, secure content sharing and even bitcoin are designed to span large groups of users and devices comprising many senders and receivers, as well as buyers and sellers. These systems employ a security architecture called public key infrastructure (PKI) to establish a framework for managing keys and identities, and to define a trust model that underpins transactions and instructions in a way that can be verified and validated. The much-anticipated arrival of quantum computers introduces the potentially devastating threat that these PKI-

based systems can be compromised. Quantum computers have the potential to expose secret keys in a PKI and shatter the security they provide.

Established technologies such as quantum key distribution (QKD) have the potential to provide a method for exchanging keys securely even in the presence of an attacker with a quantum computer, but are limited to fixed, point-to-point connections and represent only a small fraction of the capabilities required by a PKI-based architecture. Products that make use of the new Quantum Key Management (QKM) patent would be able to address many of the practical and architectural limitations of deploying QKD.

The patent covers innovations that enable the low-level quantum-safe capabilities of QKD to be deployed in a way that aligns with existing PKI-based architectures and can scale to large distributed systems. This patented hybrid approach combines QKD and a quantum identification protocol that uses a hash-based signature scheme to create a system that spans many users and devices and yet avoids the need to rely on QKD connections between each of them. The patent also includes innovations for the secure enrollment of users with a registration authority, as well as credential checking and revocation.

This invention originated in research conducted at Los Alamos, and was part of a wide-ranging effort to address the quantum threat. Two of the three inventors named on the patent are Jane Nordholt and Richard Hughes, who co-founded and co-led the Quantum Communications team at Los Alamos for nearly two decades before retiring to become consulting physicists for Whitewood.

“We are proud that Los Alamos has once again been recognized as a center for innovation in this critical area,” said Duncan McBranch, Chief Technology Officer at Los Alamos. “This and our other inventions in quantum science move beyond pure research to teach how viable quantum systems can be designed and built. Quantum technologies will be powerful future security tools and our goal is to make that future real today.”

This new patent forms part of a portfolio of Los Alamos intellectual property that was exclusively licensed by Whitewood to commercialize quantum-based technologies and address current and future needs for secure cryptography. Other Nordholt and Hughes patents in the portfolio include:

- An advanced method for correcting the unwanted polarization effects encountered in today’s optical fiber networks;
- The miniaturization of QKD technology components for use on existing optical fiber networks and from satellite to ground;
- Technologies that dramatically increase the scalability of multi-node networks that employ quantum-based key management techniques.

“The timing of the arrival of quantum computing has been hotly debated for years, but with the stakes so high it is important that organizations assess their current crypto systems and take action to evolve to a quantum-safe posture,” said Richard Moulds, Vice President of Strategy at Whitewood. “Transitioning to quantum-safe algorithms or technologies such as QKD is potentially very disruptive. The ability to adopt the hybrid QKM approach described in this new patent could greatly simplify that transition.”

QKM builds on existing Whitewood products that include quantum-powered random number generators (QRNG) and entropy management systems. Whitewood’s first product, the award-winning Entropy Engine™ QRNG, was launched in 2015, and last year the company made it possible for customers to address the threat of entropy starvation with Whitewood’s

netRandom product suite, which provides access to high-quality true random numbers across an entire data center and application infrastructure.

Read more about Quantum Key Management.

RICHARD P. FEYNMAN CENTER FOR INNOVATION

www.lanl.gov/feynmancenter | (505) 667-9090 | feynmancenter@lanl.gov