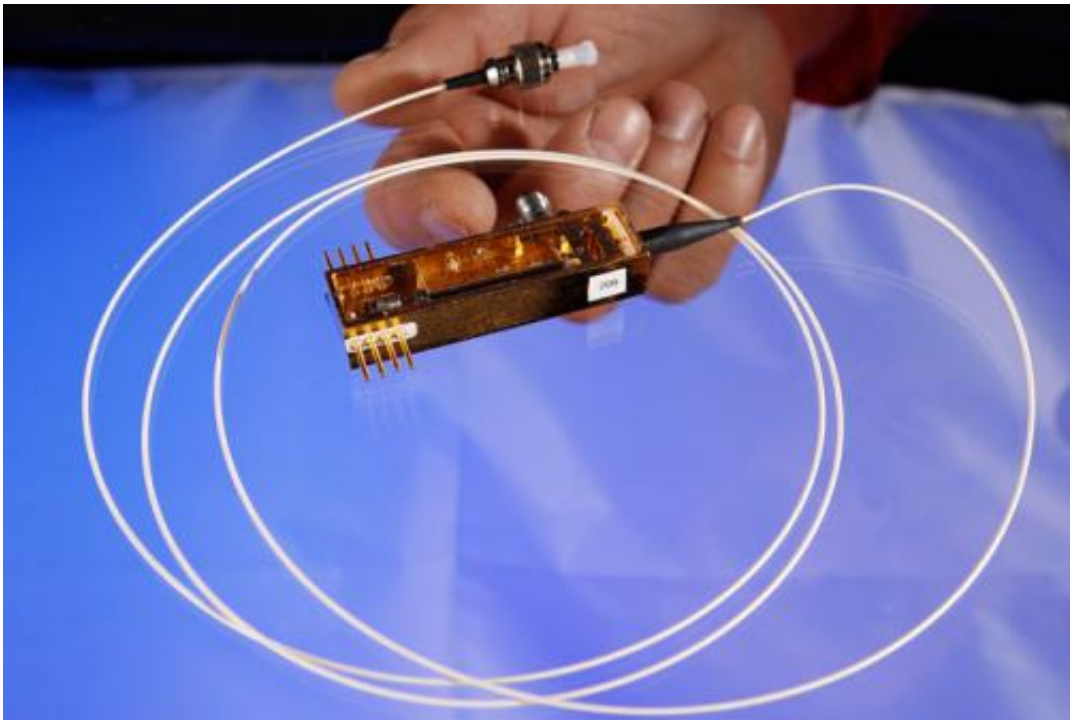
Quantum key distribution technology: Secure computing for the 'Everyman'

September 3 2014, by James E. Rickman



This small device developed at Los Alamos National Laboratory uses the truly random spin of light particles as defined by laws of quantum mechanics to generate a random number for use in a cryptographic key that can be used to securely transmit information between two parties. Quantum key distribution represents a foolproof cryptography method that may now become available to the general public, thanks to a licensing agreement between Los Alamos and Whitewood Encryption Systems, LLC. Los Alamos scientist developed their particular method for quantum cryptography after two decades of rigorous testing inside of the nation's premier national security science laboratory.

The largest information technology agreement ever signed by Los Alamos National Laboratory brings the potential for truly secure data encryption to the marketplace after nearly 20 years of development at the nation's premier national-security science laboratory.

"Quantum systems represent the best hope for truly secure data encryption because they store or transmit information in ways that are unbreakable by conventional cryptographic methods," said Duncan McBranch, Chief Technology Officer at Los Alamos National Laboratory. "This licensing agreement with Whitewood Encryption Systems, Inc. is historic in that it takes our groundbreaking technical work that was developed over two decades into commercial encryption applications."

By harnessing the quantum properties of light for generating random numbers, and creating cryptographic keys with lightning speed, the technology enables a completely new commercial platform for real-time encryption at high data rates. For the first time, ordinary citizens and companies will be able to use cryptographic systems that have only been the subject of experiments in the world's most advanced physics and computing laboratories for real-world applications.

If implemented on a wide scale, quantum key distribution technology could ensure truly secure commerce, banking, communications and data transfer.

The technology at the heart of the agreement is a compact random-number-generation technology that creates cryptographic keys based on the truly random polarization state of light particles known as photons. Because the randomness of photon polarization is based on quantum mechanics, an adversary cannot predict the outcome of this random number generator. This represents a vast improvement over current "random-number" generators that are based on mathematical formulas

that can be broken by a computer with sufficient speed and power.

Moreover, any attempt by a third party to eavesdrop on the secure communications between quantum key holders disrupts the quantum system itself, so communication can be aborted and the snooper detected before any data is stolen.

The Los Alamos technology is simple and compact enough that it could be made into a unit comparable to a computer thumb drive or compact data-card reader. Units could be manufactured at extremely low cost, putting them within easy retail range of ordinary electronics consumers.

Whitewood Encryption Systems, Inc. of Boston, Mass., is a wholly owned subsidiary of Allied Minds. The agreement provides exclusive license for several Los Alamos-created quantum-encryption patents in exchange for consideration in the form of licensing fees.

"Whitewood aims to address one of the most difficult problems in securing modern communications: scalability—meeting the need for low-cost, low-latency, high-security systems that can effectively service increasingly complex data security needs," said John Serafini, Vice President at Allied Minds. "Whitewood's foundation in quantum mechanics makes it uniquely suited to satisfy demand for the encryption of data both at rest as well as in transit, and in the mass quantity and high-throughput requirements of today's digital environment."

Provided by Los Alamos National Laboratory