Quantum encryption technology developed at LANL reinvents cybersecurity for electrical grids

Los Alamos National Laboratory

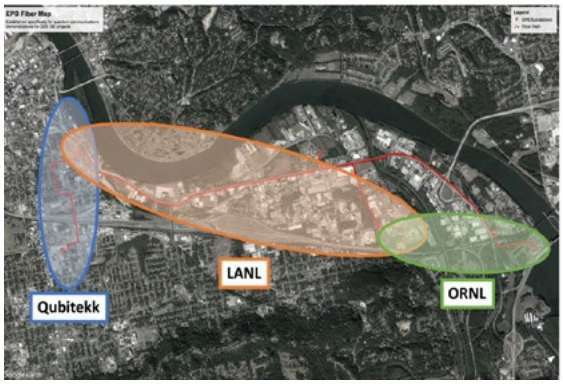
As hackers' growing access to advanced computing technology threatens conventional encryption systems, scientists from Los Alamos National Laboratory (LANL) are using quantum principles to give electrical grids extra protection against cyberattacks that can leave millions without power.

National security, economic productivity, and human health can be imperiled when an electrical grid is compromised. Scientists in the field of cryptography have developed highly complex, mathematically based security code problems to protect these critical infrastructure operations. However, as computing power steadily increases, so does the chance that adversaries will decode these complex encryptions.

Current encryption systems rely on computational difficulty, such as factoring a large number, for defense against eavesdropping, impersonation, or other types of malicious actions. But these systems are becoming more vulnerable as hackers gain access to advances in computing power, efficient algorithms, and artificial intelligence. This concern is particularly relevant to critical infrastructure, such as electrical grids, which cannot be quickly updated or patched to accommodate every new security vulnerability.

Scientists at LANL are seeking to escape this ongoing attack-defend cycle by developing a new method for protecting information called Quantum Ensured Defense (QED). Instead of mathematical complexity, this method uses physics—specifically, the unusual behavior of the quantum realm.

Currently, information that is sent through the internet is passed through the optical fibers as pulses of photons from a transmitter on one end to a receiver at the other. QED uses these same principles and goes further by making the light pulses so dim that they contain on average a single particle of light, or photon. These photons are used to create cryptographic "keys" which can be used to "lock" control signals into secret codes—a process called quantum key distribution (QKD).



Above: Back-to-back operation of three quantum communication systems, each operating on different physical principles during the successful field demonstration with Oak Ridge National Lab, Qubitekk Inc., and EPB in Chattanooga, Tennessee. Red line indicates layout of optical fibers on EPB's metroscale commercial system.

Scientists know the information is protected for three reasons: a photon cannot be cut in half; a photon cannot be accurately copied; and a photon cannot even be measured without changing it in some way.

Los Alamos researchers partnered with Oak Ridge National Laboratory, QKD developer and manufacturer Qubitekk, and the Electric Power Board (EPB) of Chattanooga, Tennessee, to bring this futuristic idea of quantum-ensured security to an actual electric grid. Together they tested a network of three different QKD systems (see figure) on EPB's optical fiber network, which included the grid's communications center and substations. The field tests successfully demonstrated the interoperability of these diverse QKD systems' keys, without the need for a complete system overhaul.

In the near future, LANL will be seeking a cooperative research and development agreement (CRADA) partner to further develop this technology for its unique applications. Many of the technologies that have been developed for electrical grids could be adapted to protect other types of infrastructure under computer control that are subject to hacking.