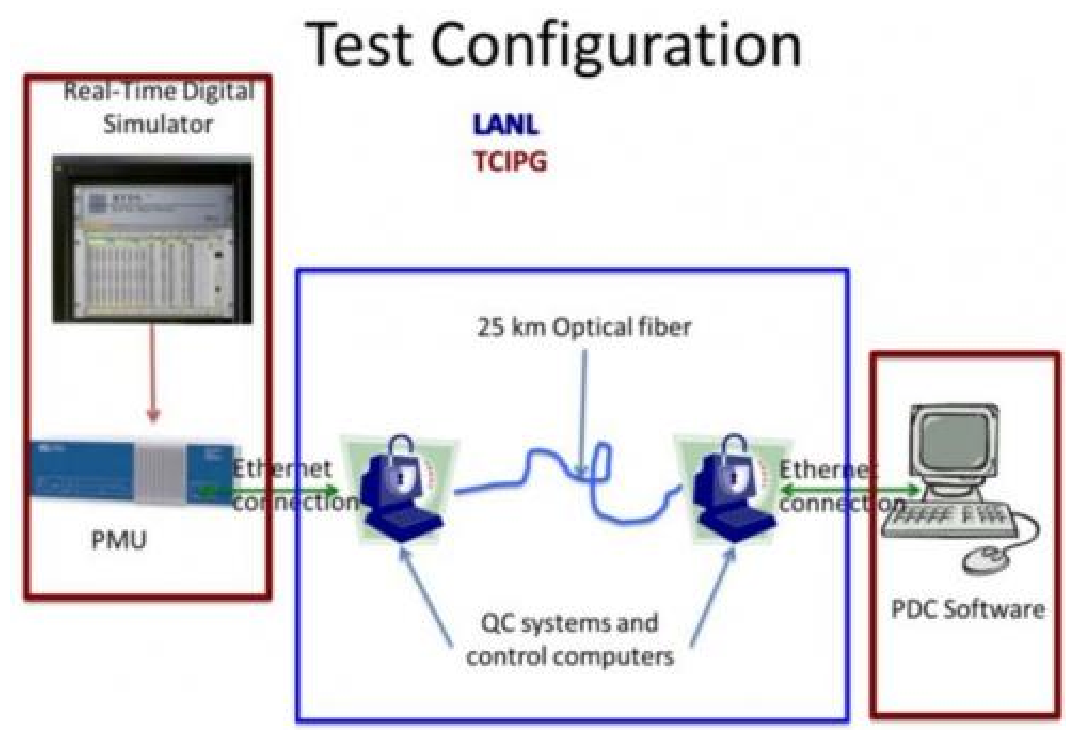
Los Alamos reveals it's been running quantum network for two and a half years

May 7 2013, by Bob Yirka



Test configuration using the Los Alamos (LANL) QSC system to secure PMU control commands and data. The TCIPG test bed provided a real-time digital (power) simulator, PMU, and PDC software to control and display data from the PMU. Credit: arXiv:1305.0305 [quant-ph]

(Phys.org) —In a recent paper available on *arXiv*, a team of researchers at New Mexico's Los Alamos National Laboratory has revealed they've been running a quantum network for 2 1/2 years. The network is hub-and-spoke based, the team reports, and allows for perfectly secure messaging except at the hub.

Quantum networks are the Holy Grail for security experts—because messages cannot be read without changing them, it is impossible for them to be intercepted without being detected. But that same technology that allows for such perfect security also prevents it from being implemented in network systems. In order for messages to be routed, the address must be read, thus altering the message. The researchers at Los Alamos report they've worked around this problem by implementing the network as a hub-and-spoke system.

In this approach, all nodes on the network are connected directly to the hub. The hub reads the message (causing it to be changed), then repackages it and sends it securely to the node whose address was found in the original message. This makes the network secure at all points except at the hub.

Using a hub-and-spoke approach has two deficiencies for general purpose use. The first is the inherent weakness at the hub—if it were to be breached, the whole network would be compromised. The second is scalability—at some point, the number of nodes connected to the central hub becomes unwieldy, making further growth impossible. The researchers at Los Alamos say they've reduced the scalability problem by giving each node on the network a quantum transmitter, but not a photon detector. This makes adding nodes a very cheap proposition—those at Los Alamos, the researchers say, aren't much bigger than a box of matches.

Impressive as it is, the network at Los Alamos is more of a work-around than solution to the problem of building quantum networks for general purpose use. A solution requires that someone figures out a way to route quantum messages without destroying their integrity. Until that happens, this new approach appears to be a good stand-in, as it's clearly far more secure than traditional network systems.

More information: Network-Centric Quantum Communications with Application to Critical Infrastructure Protection, arXiv:1305.0305 [quant-ph] arxiv.org/abs/1305.0305

Abstract
Network-centric quantum communications (NQC) - a new, scalable instantiation of quantum cryptography providing key management with forward security for lightweight encryption, authentication and digital signatures in optical networks - is briefly described. Results from a multi-node experimental test-bed utilizing integrated photonics quantum communications components, known as QKarDs, include: quantum identification; verifiable quantum secret sharing; multi-party authenticated key establishment, including group keying; and single-fiber quantum-secured communications that can be applied as a security retrofit/upgrade to existing optical fiber installations. A demonstration that NQC meets the challenging simultaneous latency and security requirements of electric grid control communications, which cannot be met without compromises using conventional cryptography, is described.

via ArxivBlog

Citation: Los Alamos reveals it's been running quantum network for two and a half years (2013, May 7) retrieved 19 April 2024 from https://phys.org/news/2013-05-los-alamos-reveals-quantum-network.html