T-QUAKE Quantum Mechanical Microchip

Principal application

The quantum world defies intuition. One of its axioms, the Heisenberg Uncertainty Principle, states that any attempt to measure the position or momentum of a quantum object changes the object itself. Historically, this principle was viewed as a hindrance by scientists trying to examine quantum particles. But the same quantum effects that make them difficult to measure have long been of interest to the cryptography and intelligence communities. Theoretically, quantum-encrypted information cannot be intercepted without detection, because any attempt to measure the particles that make up a quantum-encrypted message alters their quantum characteristics, alerting the intended sender and receiver of the breach. Further, quantum-encrypted signals cannot be decoded by powerful future (perhaps quantum) computers, as is feared for the RSA encryption protocol now widely used for secure transactions in the banking, internet, and national security domains. For these reasons, quantum cryptography is seen as a promising alternative for sending and receiving private cryptographic keys.

But practical, day-to-day quantum encryption has remained elusive due to the extreme technical challenges, high costs, and large size of the technologies required to send and receive quantum signals. Previously, quantum transmission and reception had been demonstrated at the bench-top scale using laboratory systems that cost hundreds of thousands of dollars.

Now a Sandia research team has developed and demonstrated the first microfabricated quantum transmitter/receiver. Called T-QUAKE (Transceiver for Quantum Keys and Encryption), the system miniaturizes all of the components necessary to securely encode, transmit, receive, and decode quantum photonic signals onto a single microchip, in effect creating an ultra-secure cryptographic network node for any secure communication or network application. T-QUAKE accomplishes what bench-scale quantum encryption systems do but at one millionth the scale, on a chip roughly 3 mm x 5 mm and weighing less than an ounce.

Because of the ability to mass fabricate microchips using traditional CMOS techniques, T-QUAKE also dramatically reduces costs. Current quantum communication laboratory systems have a price point greater than $100,000 for one transmitter-receiver system. We estimate that Sandia's chips could cost less than $5,000 per transceiver in existing, high-consequence cyber and physical security markets and less than $100 per transceiver when mass produced for future commercial electronics markets, transforming quantum communications from the national laboratory research realm to the military-industrial domain and, soon, consumer laptops and mobile phones.

In the near-term, a quantum cryptographic transceiver would be extremely valuable in high consequence information-sharing environments such as for cyber intrusion detection and military communications. Early adopters will likely use the keys produced by the chips with existing encryption techniques, providing an additional layer of security. Over the long term, such a chip could become part of any highly secure networked system, such as for digital banking and ATM machines, enhanced-privacy internet communications and transactions, and hand-held and mobile phone communications. In addition, the chip could become a key component of physical security and anti-tampering applications, such as automobile anti-theft devices, seals for manufacturer warranty verification, and remote user authentication.

NNSA National Nuclear Security Administration

U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-4224 O

Sandia National Laboratories