FEATURE

Does quantum cryptology offer hack-proof security?

New quantum cryptology research could result in systems that are impossible to hack. But good luck trying to explain it to your boss.

By JD Sartain | Follow
CIO | Sep 9, 2015 4:58 AM PT

Untangling hyper-entangled twisted light.

Photons in the form of a bi-photon frequency comb.

Quantum-powered random numbers generated by an entropy engine that exploits quantum mechanics.

Quantum cryptology may be the hottest topic in security these days, but it sure reads like a lot of sci-fi jargon. But what does it mean?

Bruce Potter, CTO of the KEYW Corporation, defined it to a room full of privacy professionals this past July at the Black Hat conference. He explained that with so much concern regarding the quality of our protective encryption capabilities, this is still a complicated and misunderstood process. Quantum cryptology (and its crypto components) is a mind-bending concept that baffles even the most experienced scientists. Those who try to understand what's going on are stymied by the diversity, age and code complexity of the various software components. And, while cryptographic core algorithms have been well-studied, other components in enterprise cryptosystems are less understood. It's no wonder this field of science incites so much controversy.

According to Toshiba, it means a stable, unbreakable encryption method that uses photons (or light particles) transferred through a custom-made, fiber-optic cable that's completely independent of the Internet. And, it's hack-proof because any attempts to eavesdrop (intercept, copy, wiretap, etc.) such a transmission alters the quantum state – that is, scrambles the encoded data – and is immediately detectable.

Hirokazu Tsukimoto, a spokesman at Toshiba, says quantum cryptographic communication uses quantum physics to ensure that genomic data encrypted with digital keys remains undisclosed. Bits are transmitted by individual photons, which cannot be manipulated without leaving remnants of the intrusion. "Toshiba has developed the world's fastest quantum key distribution prototype based on a *self-differencing circuit* for single photon detection," says Tsukimoto. "Field trials begin this month to evaluate the prototype for commercial use in five years. Further development includes large-scale quantum cryptography networks."

Meanwhile, however, other quantum cryptographic research is sprouting up in universities and corporations all over the planet. UCLA, MIT, Columbia, Duke, University of Maryland (UM), University of Rochester (UR), University of Glasgow (UG), National Institute of Standards and Technology (NIST), Los Alamos National Laboratory (LANL), and Whitewood Encryption Systems (WES), to list some of the notable ones, are all working frantically to improve, perfect and expedite this technology.

Hyperentanglement

UCLA's engineering research team has discovered that photon pairs can be divided, then entangled into multiple dimensions by using the photons' energy and spin properties. Each additional dimension doubles the photon's data capacity, which means photon pairs can hold 32 times more data than they could using the standard quantum encoding methods.

[Related: IBM researchers make quantum computing breakthroughs]

"We show that an optical frequency comb can be generated at single photon level," says Zhenda Xie, associate professor and research scientist at UCLA. "Essentially, we're leveraging wavelength division multiplexing concepts at the quantum level."

"Our goal is to advance quantum hyperentanglement for high-speed, unbreakable, secure communications," says Chee Wei Wong, Sc.D., associate professor of electrical engineering. "This is an enhancement package to dramatically speed up the current Quantum Key Distribution (QKD) rate, so our breakthrough leverages on the current QKD technologies, some of which are already implemented and released."

Wong explains that this technology is currently only relevant for transmitting medical databases, finance trading and banking information, government database communications and military communications in the field and war theatre. In other words, UCLA's quantum hyperentanglement research is just for communications, *not* for protecting data files and records at the source, like all those databases that were recently breached.

"The next step for us," says Wong, "is to demonstrate even more quantum bits encoded in the hyperentanglement approach. Currently, each photon carries about five quantum bits, at about 2^5 = 32 (2 to the 5th power), which is 32 times higher than the current unbreakable data rates. As the next step, we would also like to see information encoding on our physical system. Yes, in the absence of a quantum computer, this quantum physics-based communication approach is known to be unbreakable."

Twisted light

A research team at the University of Rochester is working with Duke University and the University of Glasgow on another new technique. This one uses twisted light to enhance the data capacity of each photon. The current process uses one of the four polarization orientations (e.g., horizontal, vertical, diagonal and anti-diagonal), which yields only one qubit per photon.

University of Rochester PhD student Mohammad Mirhosseini and colleagues used the orbital angular momentum (OAM) of light and the azimuthal angular position (ANG) of photons to encode the qubits, which doubled the capacity to 2.05. Basically, light has energy defined by its frequency and momentum defined by its wavelength. The orbital angular momentum is the wavefront of a beam of light that's coiling around its propagation axis. The electric field spirals around like a corkscrew; hence, twisted light. The quantum number describes how sharp the spiral is, while the sign reveals the direction of the spiral.

[Related: Los Alamos National Lab's R&D fueling new quantum-crypto firm]

Using the "twisted light" technology, the team encoded a seven-dimensional alphabet and confirmed that the new system can generate and detect information at 4 kHz speeds with 93 percent accuracy. According to Mirhosseini, future plans include enhancing the transmission rates to GHz levels for communications/telecom applications and to extend the encoding to 4.17 bits per photon.

Entropy engine

Whitewood Encryption Systems and Los Alamos National Laboratory are also collaborating on another area of quantum cryptology research and development: the Entropy Engine, which is a random number generator (RNG) that harvests entropy from a quantum field. LANL claims the RNG is so efficient, it can fit on a USB key drive at an exceptionally low cost.

"Security is a multi-faceted discipline representing multiple attack vectors and a constantly shifting set of targets for an agile and equipped attacker," says Richard Moulds, vice president of Product Strategy and Development at Whitewood Encryption Systems. "We believe that attacks against random number sources and key management systems are on the rise and represent a highly attractive target for would-be hackers."

According to Moulds, the Entropy Engine exploits quantum mechanics in an effort to provide pure entropy in the form of random data at high speeds (200 Mbps), and addresses the fundamental issue of all cryptosystems: predictability. Future plans include integrating this source of random data into a host of other applications. For example, Whitewood plans to expand its focus on a wider range of commercial and open-source or mainstream cryptographic applications.

"Our goal is to enable as broad a suite of applications as possible and take advantage of this high-quality, high-performance source of random data," says Moulds. "At the Black Hat show, Whitewood released an open-source plugin for OpenSSL to improve the monitoring and management of entropy consumption."

JD Sartain

J.D. Sartain is a freelance journalist from Boston.

The hottest security certifications, most in-demand skills

View 1 Comment