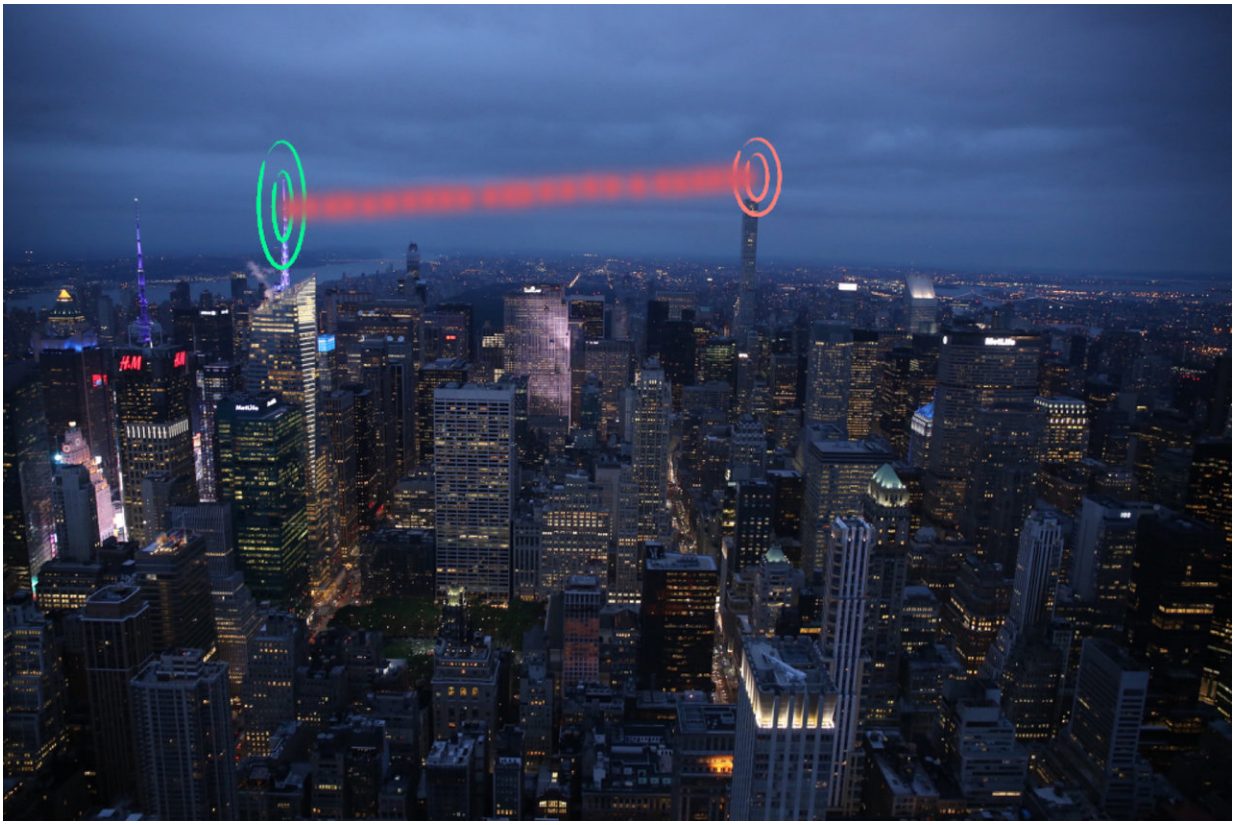
High-speed quantum encryption may help secure the future internet

November 24 2017



Depiction of the proposed system in a metropolitan city where quantum-secure information is transferred between two quantum nodes. Credit: Agheal Abedzahdeh (Duke University)

Recent advances in quantum computers may soon give hackers access to machines powerful enough to crack even the toughest of standard

internet security codes. With these codes broken, all of our online data—from medical records to bank transactions—could be vulnerable to attack.

To fight back against the future threat, researchers are wielding the same strange properties that drive quantum computers to create theoretically hack-proof forms of quantum data encryption.

And now, these quantum encryption techniques may be one step closer to wide-scale use thanks to a new system developed by scientists at Duke University, The Ohio State University and Oak Ridge National Laboratory. Their system is capable of creating and distributing encryption codes at megabit-per-second rates, which is five to 10 times faster than existing methods and on par with current internet speeds when running several systems in parallel.

The researchers demonstrate that the technique is secure from common attacks, even in the face of equipment flaws that could open up leaks.

"We are now likely to have a functioning quantum computer that might be able to start breaking the existing cryptographic codes in the near future," said Daniel Gauthier, a professor of physics at The Ohio State University. "We really need to be thinking hard now of different techniques that we could use for trying to secure the internet."

The results appear online Nov. 24 in *Science Advances*.

To a hacker, our online purchases, bank transactions and medical records all look like gibberish due to ciphers called encryption keys. Personal information sent over the web is first scrambled using one of these keys, and then unscrambled by the receiver using the same key.

For this system to work, both parties must have access to the same key,

and it must be kept secret. Quantum key distribution (QKD) takes advantage of one of the fundamental properties of quantum mechanics—measuring tiny bits of matter like electrons or photons automatically changes their properties—to exchange keys in a way that immediately alerts both parties to the existence of a security breach.

Though QKD was first theorized in 1984 and implemented shortly thereafter, the technologies to support its wide-scale use are only now coming online. Companies in Europe now sell laser-based systems for QKD, and in a highly-publicized event last summer, China used a satellite to send a quantum key to two land-based stations located 1200 km apart.

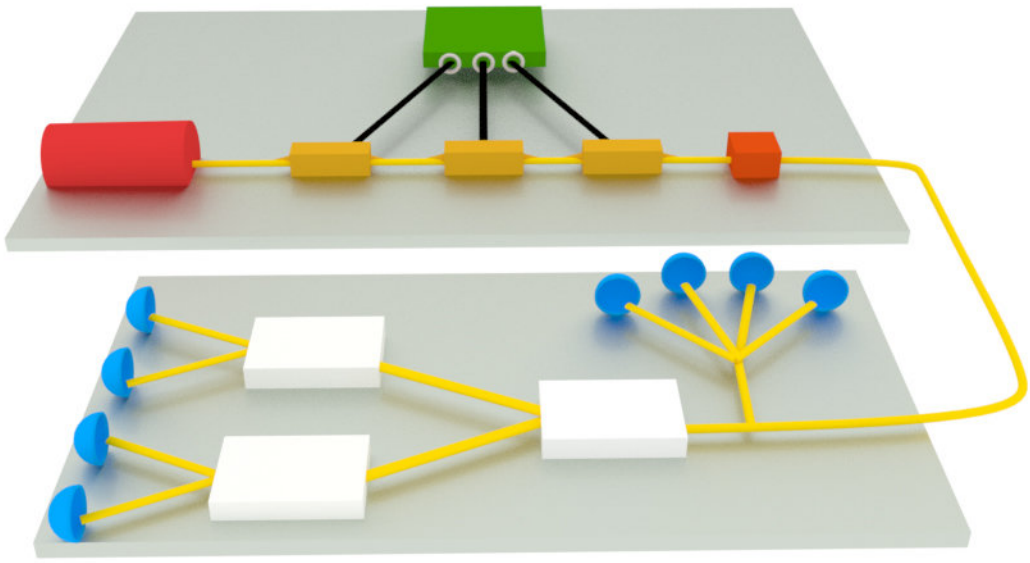


Illustration of a high-dimensional quantum communication device capable of streaming encrypted video. Credit: Agheal Abedzahdeh (Duke University)

The problem with many of these systems, said Nurul Taimur Islam, a graduate student in physics at Duke, is that they can only transmit keys at relatively low rates—between tens to hundreds of kilobits per second—which are too slow for most practical uses on the internet.

"At these rates, quantum-secure encryption systems cannot support some basic daily tasks, such as hosting an encrypted telephone call or video streaming," Islam said.

Like many QKD systems, Islam's key transmitter uses a weakened laser to encode information on individual photons of light. But they found a way to pack more information onto each photon, making their technique faster.

By adjusting the time at which the photon is released, and a property of the photon called the phase, their system can encode two bits of information per photon instead of one. This trick, paired with high-speed detectors developed by Clinton Cahall, graduate student in electrical and computer engineering, and Jungsang Kim, professor of electrical and computer engineering at Duke, powers their system to transmit keys five to 10 times faster than other methods.

"It was changing these additional properties of the photon that allowed us to almost double the secure key rate that we were able to obtain if we hadn't done that," said Gauthier, who began the work as a professor of physics at Duke before moving to OSU.

In a perfect world, QKD would be perfectly secure. Any attempt to hack a key exchange would leave errors on the transmission that could be easily spotted by the receiver. But real-world implementations of QKD require imperfect equipment, and these imperfections open up leaks that hackers can exploit.

The researchers carefully characterized the limitations of each piece of equipment they used. They then worked with Charles Lim, currently a professor of electrical and computer engineering at the National University of Singapore, to incorporate these experimental flaws into the theory.

"We wanted to identify every experimental flaw in the system, and include these flaws in the theory so that we could ensure our system is secure and there is no potential side-channel attack," Islam said.

Though their transmitter requires some specialty parts, all of the components are currently available commercially. Encryption keys encoded in photons of light can be sent over existing optical fiber lines that burrow under cities, making it relatively straightforward to integrate their transmitter and receiver into the current internet infrastructure.

"All of this equipment, apart from the single-photon detectors, exist in the telecommunications industry, and with some engineering we could probably fit the entire transmitter and receiver in a box as big as a computer CPU," Islam said.

More information: "Provably secure and high-rate quantum key distribution with time-bin qudits" *Science Advances* (2017). DOI: 10.1126/sciadv.1701491
advances.sciencemag.org/content/3/11/e1701491

Provided by Duke University