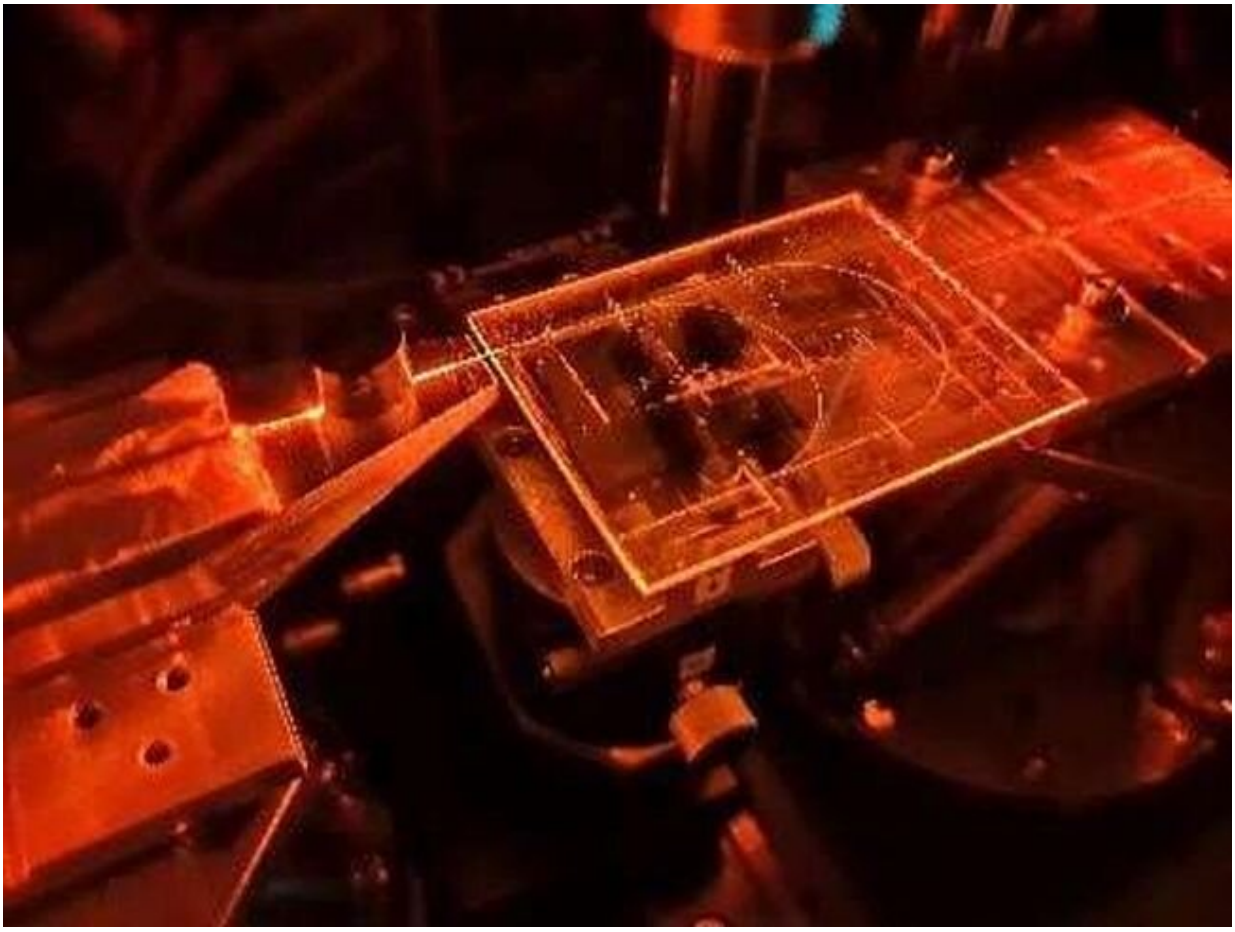
Chip-based quantum key distribution achieves higher transmission speeds

May 25 2023



The silica-based QKD receiver shown consists of a photonic integrated circuit and two external single-photon detectors. Credit: Simone Atzeni, CNR-IFN

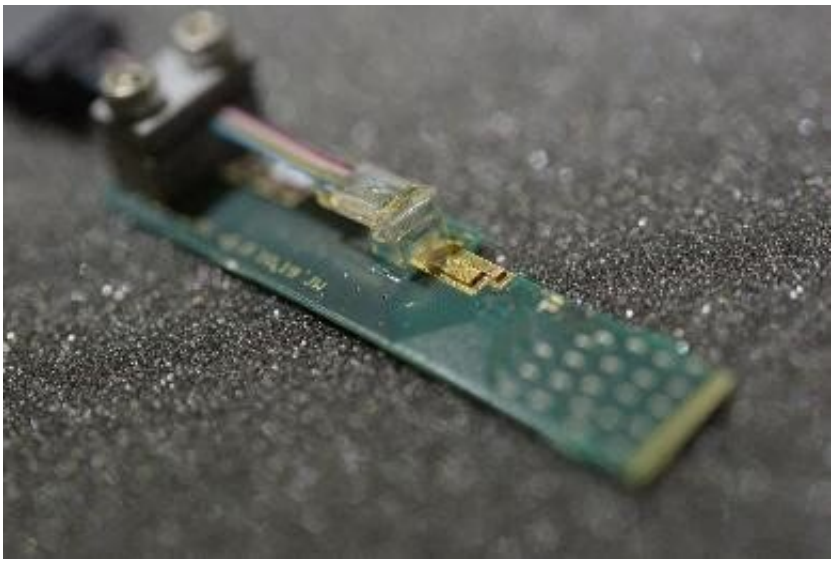
Researchers have developed a quantum key distribution (QKD) system based on integrated photonics that can transmit secure keys at unprecedented speeds. The proof-of-principle experiments represent an important step toward real-world application of this highly secure communication method.

QKD is a well-established method of providing secret keys for secure communication between distant parties. By using the quantum properties of light to generate secure random keys for encrypting and decrypting data, its security is based on the laws of physics, rather than computational complexity like today's communication protocols.

"A key goal for QKD technology is the ability to simply integrate it into a real-world communications network," said research team member Rebecka Sax from the University of Geneva in Switzerland. "An important and necessary step toward this goal is the use of integrated photonics, which allows optical systems to be manufactured using the same semiconductor technology used to make silicon computer chips."

In an article in *Photonics Research*, researchers led by University of Geneva's Hugo Zbinden describe their new QKD system, in which all components are integrated onto chips except the laser and detectors. This comes with many advantages such as compactness, low cost and ease of mass production.

"Although QKD can provide security for sensitive applications such as banking, health and defense, it is not yet a widespread technology," said Sax. "This work justifies the technology maturity and helps address the technicalities around implementing it via optical integrated circuits, which would allow integration in networks and in other applications."



Researchers have developed a quantum key distribution (QKD) system based on silicon photonics that can transmit secure keys at unprecedented speeds. The QKD transmitter (pictured) combines a photonic and electric integrated circuit with an external diode laser. Credit: Rebecka Sax, University of Geneva

Building a faster chip-based system

In previous work, the researchers developed a three-state time-bin QKD protocol that was carried out with standard fiber-based components to achieve QKD transmission at record high speeds.

"Our goal in this new work was to implement the same protocol using integrated photonics," said Sax. "The compactness, robustness and ease of manipulation of an integrated photonic system—with less components to verify when implementing or to troubleshoot in a network—improves the position of QKD as a technology for secure communication."

QKD systems use a transmitter to send the encoded photons and a receiver to detect them. In the new work, the University of Geneva researchers collaborated with silicon photonics company Sicoya GmbH

in Berlin, Germany, and quantum cybersecurity company ID Quantique in Geneva to develop a silicon photonics transmitter that combines a photonic integrated circuit with an external diode laser.

The QKD receiver was made of silica and consisted of a photonic integrated circuit and two external single-photon detectors. Roberto Osellame's group at the CNR Institute for Photonics and Nanotechnology in Milano, Italy, used femtosecond laser micromachining to fabricate the receiver.

"For the transmitter, using an external laser with a photonic and electronic integrated circuit made it possible to accurately produce and encode photons at a record speed of up 2.5 GHz," said Sax. "For the receiver, a low-loss and polarization independent photonic integrated circuit and a set of external detectors allowed passive and simple detection of the transmitted photons. Connecting these two components with a standard single-mode fiber enabled high-speed production of secret keys."

Low-loss, high-speed transmission

After thoroughly characterizing the integrated transmitter and receiver, the researchers used it to perform a secret key exchange using different simulated fiber distances and with a 150-km long single-mode fiber and single-photon avalanche photodiodes, which are well-suited for practical implementations.

They also performed experiments using single-photon superconducting nanowire detectors, which enabled a quantum bit error rate as low as 0.8%. The receiver not only featured polarization independence, which is complicated to achieve using integrated photonics, but also presented extremely low loss, around 3 dB.

"In terms of secret key rate production and quantum bit error rates, these new experiments produced results that are similar to those of previous experiments performed using fiber-based components," said Sax. "However, the QKD system is much simpler and more practical than the previous experimental setups, thus displaying the feasibility of using this protocol with integrated circuits."

The researchers are now working to house the system parts in a simple rack enclosure that would allow QKD to be implemented in a network system.

More information: Rebecka Sax et al, High-speed integrated QKD system, *Photonics Research* (2023). DOI: 10.1364/PRJ.481475

Provided by Optica