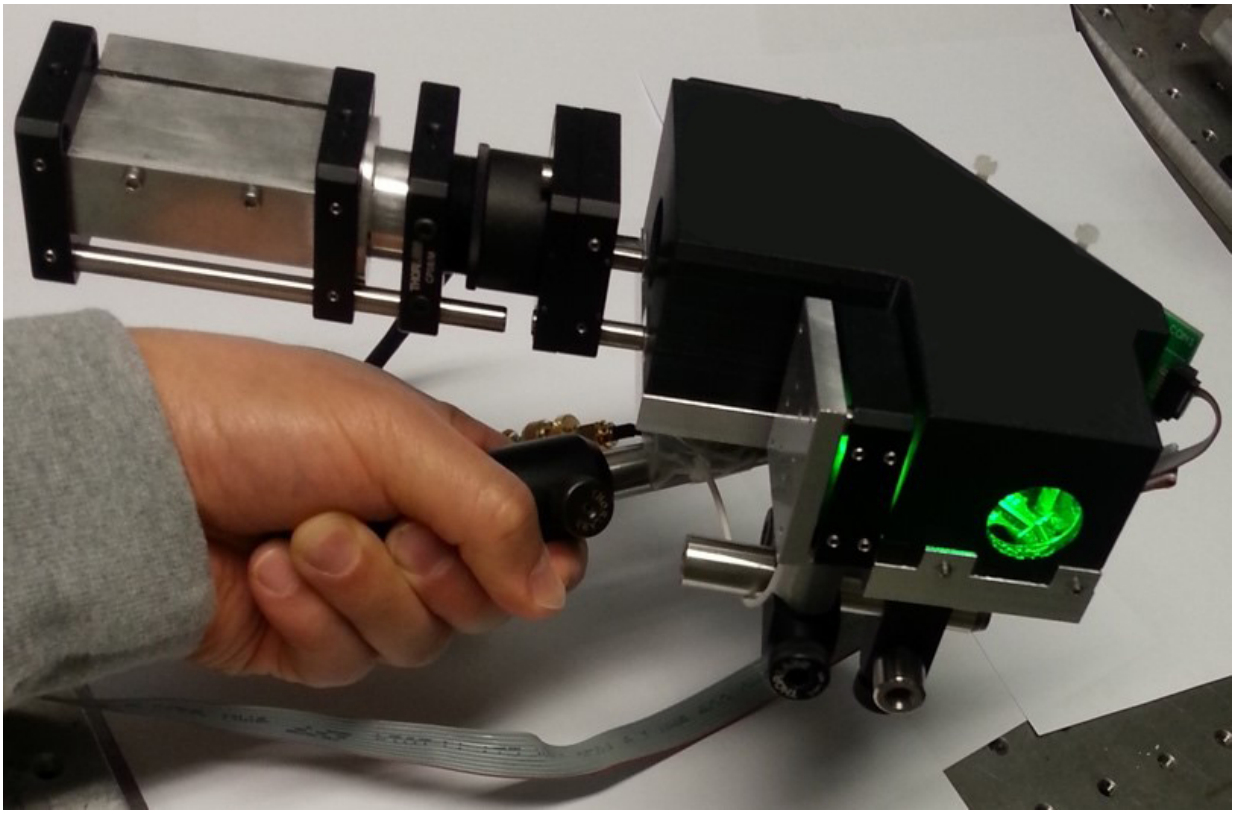
Quantum key system could make mobile transactions far more secure

March 15 2017



This handheld device for transmitting and receiving quantum cryptographic keys was built from off-the-shelf components. The device could be miniaturized for use in a mobile device. Credit: Iris Choi, Oxford University

With the growing popularity of mobile phone apps to pay for purchases at cash registers and gas pumps, users would like to know their personal

financial information is safe from cyber-attacks. For the first time, researchers have demonstrated a prototype device that can send unbreakable secret keys from a handheld device to a terminal.

In The Optical Society (OSA) journal *Optics Express*, researchers lay out a scheme for transmitting quantum keys at a high enough data rate to ensure data security while compensating for the inevitable movement of the human hand. Their prototype system uses ultra-fast LEDs and moveable mirrors to send a secret key at a rate of more than 30 kilobytes per second over a distance of 0.5 meters.

"The idea is that this gadget would be a mobile object that talks to something that is fixed," said Iris Choi of Oxford University, one of the paper's authors. If integrated into a cell phone, for example, the device could allow secure links to near-field communications mobile payment systems and indoor Wi-Fi networks. It also could improve the security of ATMs and help prevent ATM skimming attacks, which are estimated to cost the industry more than $2 billion annually.

Keys made from light

The technology is a quantum key distribution system. Quantum key distribution relies on characteristics of a single photon to provide a bit—a 1 or a 0—to build up a cryptographic key that can encrypt and decrypt information. Quantum keys are considered secure because if someone intercepts the quantum bits and then passes them on, the very act of measuring them will alter them.

"When an eavesdropper attempts to tap into the channel, it will change the content of the key," Choi said. "We're not saying this technology can prevent being eavesdropped on, but if you do eavesdrop, we know you're there."

The system contains six resonant-cavity LEDs, which provide overlapping spectra of light. Each of the six is filtered into a different polarization, split into pairs to represent 1s and 0s—horizontal or vertical, diagonal or anti-diagonal, circular left or circular right. The circularly polarized LEDs provide the bits for the key, while the other pairs are used to measure the security of the channel and provide error correction. Every four nanoseconds, one of the channels produces a one-nanosecond pulse in a random pattern. On the other end, six polarized receivers pick up the light from their matching LEDs and convert the photons into the key.

It's important not to let a potential adversary know which channel has which polarization, because that would reveal which bits were being sent, but there will always be some slight variation in the wavelength emitted by each LED, which could serve to identify them and give a hacker a way to break the code. The researchers solved this problem by equipping both the transmitter and the receiver with filters that select only a portion of the light, so they all shine with the exact same color, regardless of which polarization they produce.

Steering the beam

A quantum key must be long enough to ensure that an adversary cannot hack it simply by guessing randomly. This requires the system to transmit a large number of bits in less than a second. Achieving such a high data transmission rate in turn requires that most of the photons get to where they're supposed to go.

As a result, Choi said, the prototype's most important innovation is the steering system. Even someone trying to hold perfectly still has some motion in his hand. The research team measured this motion by looking at how the spot of a laser pointer jittered as a person tried to hold it steady. They then optimized design elements of the beam-steering

system, such as bandwidth and field of view, to compensate for this hand movement.

To help the detector properly align with the transmitter and further correct for hand movement, both the receiver and the transmitter contain a bright LED with a different color than the quantum key distribution LED that acts as a beacon. A position sensing detector on the other side measures the precise location of the beacon and moves a microelectromechanical systems (MEMS) mirror to align the incoming light with the fiber optics of the detector.

The team tested their idea with a handheld prototype made from off-the-shelf equipment. Choi said the design likely could be easily miniaturized in order to turn the system into a practical component for a mobile phone from brands such as Nokia, which participated in the research. Improving the protocol while keeping the same hardware could also increase the transmission rate, and other changes could be made to let the device work over longer distances to, for instance, connect with a Wi-Fi hub.

More information: H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, D. O'Brien, D. Bitauld, "Handheld free space quantum key distribution with dynamic motion compensation," *Opt. Express*., Volume 25, Issue 6, 6784-6795 (2017). DOI: 10.1364/OE.25.006784

Provided by Optical Society of America

Citation: Quantum key system could make mobile transactions far more secure (2017, March 15) retrieved 25 April 2024 from https://phys.org/news/2017-03-quantum-key-mobile-transactions.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.