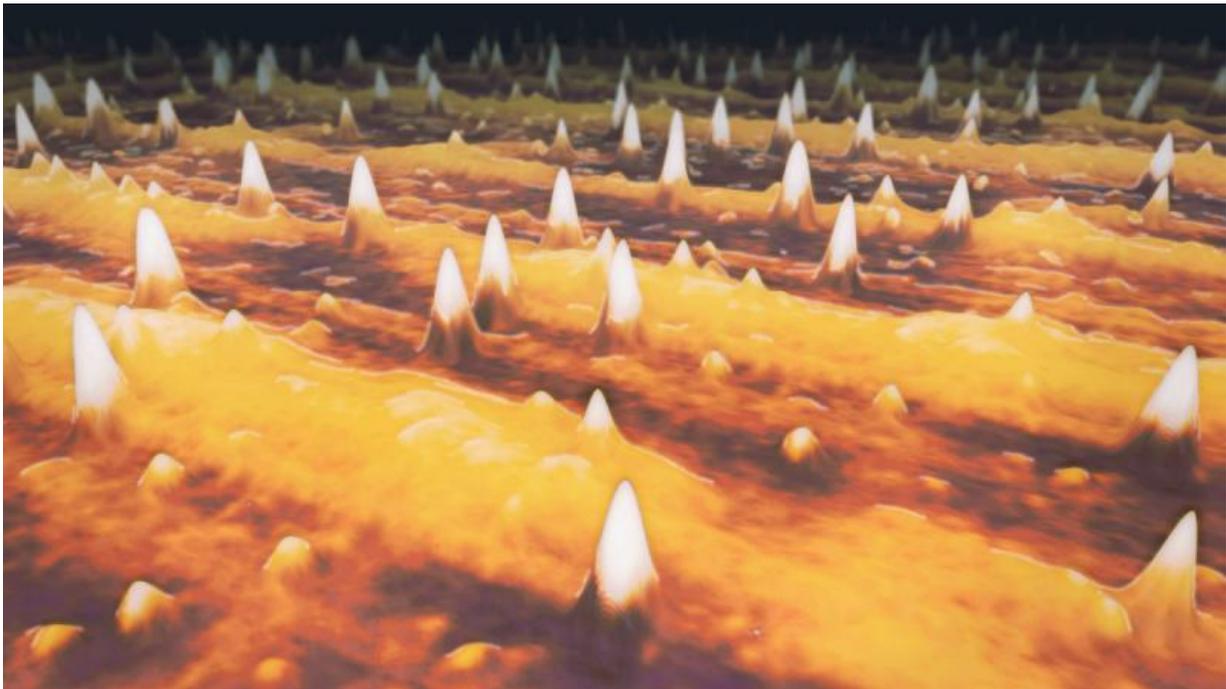


Artificial atoms shed light on the future of security

November 8 2016



Stylized depiction of quantum dots on a semiconductor surface based on an atomic-force microscope image. Credit: Joint Quantum Institute

From credit card numbers to bank account information, we transmit sensitive digital information over the internet every day. Since the 1990s, though, researchers have known that quantum computers threaten to disrupt the security of these transactions.

That's because [quantum physics](#) predicts that these computers could do some calculations far faster than their conventional counterparts. This would let a quantum computer crack a common internet security system called public key cryptography.

This system lets two computers establish private connections hidden from potential hackers. In public key cryptography, every device hands out copies of its own public key, which is a piece of digital information. Any other device can use that public key to scramble a message and send it back to the first device. The first device is the only one that has another piece of information, its private key, which it uses to decrypt the message. Two computers can use this method to create a secure channel and send information back and forth.

A quantum computer could quickly calculate another device's private key and read its messages, putting every future communication at risk. But many scientists are studying how quantum physics can fight back and help create safer [communication lines](#).

One promising method is quantum key distribution, which allows two parties to directly establish a secure channel with a single secret key. One way to generate the key is to use pairs of entangled photons—particles of light with a shared quantum connection. The entanglement guarantees that no one else can know the key, and if someone tries to eavesdrop, both parties will be tipped off.

Tobias Huber, a recently arrived JQI Experimental Postdoctoral Fellow, has been investigating how to reliably generate the entangled photons necessary for this secure communication. Huber is a graduate of the University of Innsbruck in Austria, where he was supervised by Gregor Weihs. They have frequently collaborated with JQI Fellow Glenn Solomon, who spent a semester at Innsbruck as a Fulbright Scholar. Over the past couple of years, they have been studying a particular source of

entangled photons, called quantum dots.

A quantum dot is a tiny area in a semiconductor, just nanometers wide, that is embedded in another semiconductor. This small region behaves like an artificial atom. Just like in an atom, electrons in a quantum dot occupy certain discrete energy levels. If the quantum dot absorbs a photon of the right color, an electron can jump to a higher energy level. When it does, it leaves behind an open slot at the lower energy, which physicists call a hole. Eventually, the electron will decay to its original energy, emitting a photon and filling in the hole. The intermediate combination of the excited electron and the hole is called an exciton, and two excited electrons and two holes are called a biexciton. A biexciton will decay in a cascade, emitting a pair of photons.

Huber, Weihs, Solomon and several colleagues have developed a way to directly excite biexcitons in quantum dots using a sequence of laser pulses. The pulses make it possible to encode information in the pair of emitted photons, creating a connection between them known as time-bin entanglement. It's the best type of entanglement for transmitting quantum information through optical fibers because it doesn't degrade as easily as other types over long distances. Huber and his colleagues are the first to directly produce time-bin entangled photons from quantum dots.

In their latest work, published in *Optics Express*, they investigated how the presence of material imperfections surrounding the quantum dots influences this entanglement generation. Imperfections have their own electron energy levels and can steal an electron from a dot or donate an electron to fill a hole. Either way, the impurity prevents an exciton from decaying and emitting a photon, decreasing the number of photons that are ultimately released. To combat this loss, the team used a second laser to fill up the electron levels of the impurities and showed that this increased the number of photons released without compromising the

entanglement between them.

The team says the new work is a step in the right direction to make quantum dots a viable source of entangled photons. Parametric down-conversion, a competitor that uses crystals to split the energy of one photon into two, occasionally produces two pairs of entangled photons instead of one. This could allow an eavesdropper to read an encrypted message without being detected. The absence of this drawback makes [quantum dots](#) an excellent candidate for producing [entangled photons](#) for quantum key distribution.

The advent of quantum computing brings new security challenges, but tools like [quantum key distribution](#) are taking those challenges head-on. It's possible that, one day, we could have not only quantum computers, but quantum-secure communication lines, free from prying eyes.

More information: Tobias Huber et al. Effects of photo-neutralization on the emission properties of quantum dots, *Optics Express* (2016). [DOI: 10.1364/OE.24.021794](#)

Provided by Joint Quantum Institute

Citation: Artificial atoms shed light on the future of security (2016, November 8) retrieved 26 April 2024 from <https://phys.org/news/2016-11-artificial-atoms-future.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.