

Pulses of light to encrypt data and protect security of cryptocurrencies

January 11 2018



Organic-molecule enhanced frequency comb. A single input laser (left) enters the spherical frequency comb generator that includes a single layer of organic molecules (4-diethylamino(styryl)pyridinium, DASP). The light orbits inside the sphere over 10,000x in a few nanoseconds, interacting with the molecules during each orbit and resulting in the generation of the frequency comb. Credit: Vinh Diep and Alexa Hudnut

Data travels through thousands of miles of fiber optic cables underneath the world's oceans—via pulses of light. And according to experts, the data in these cables is at great risk of being intercepted. However, a newly designed frequency comb—recently developed by researchers at the USC Viterbi School of Engineering might be an effective tool for data encryption.

Researchers Andrea M. Armani, Xiaoqin Shen, Rigoberto Castro Beltran, Vinh M. Diep, and Soheil Soltani have invented a new method to create a [frequency](#) comb—a tool that increases the potential applications of lasers by converting a single wavelength into multiple wavelengths, effectively creating tens to hundreds of lasers from a single laser. The new frequency comb is the size of a human hair compared with traditional frequency combs that can be as large as an apartment refrigerator. More importantly, the newly generated comb requires 1000x less power to operate, allowing for mobile applications.

The current state of the art relies on material systems traditionally used in microelectronics, such as silicon. By replacing these [materials](#) with carbon-based or organic molecules, the research team led by post-doctoral pursued a fundamentally different approach. Attaching only a single layer of a 25-atom organic molecule to the surface of a laser, frequency combs were demonstrated with 1000x reduction in power.

Professor Armani, the Ray Irani Chair in Engineering and Material Sciences at the USC Viterbi School of Engineering, likens the change from conventional silicon to organic materials as analogous to the change of "gas to electric." At the most basic level, the process that enables the comb to be generated is distinctly different in the two material classes.

"Organic optical materials have already transformed the electronics industry, leading to lighter, lower power TVs and cellphone displays, but previous attempts to directly interface these materials with lasers

stumbled," said Armani, "We solved the interface challenge. Because our approach can be applied to a wide range of organic materials and laser types, the future possibilities are very exciting."

Opportunity for Optical Encryption of Data

The first applications of frequency combs focused on detecting trace amounts of chemicals and high precision time-keeping. However, recently, a new application of great significance to society has emerged: quantum cryptography.

Terms like cybersecurity and quantum encryption used to be the plot lines of action thrillers and Bond movies, but with the advent of cryptocurrencies and IoT, the awareness of cybersecurity has moved from the silver screen to the mainstream. How can frequency combs contribute? The answer lies in how data is transmitted and how quantum cryptography works.

When a data signal is traveling to its destination, it is packaged like a letter in a locked envelope. Just like any lock, some are easier to crack than others, and current encryption efforts have focused on creating increasingly complex and dynamic locks. However, one fundamental limitation with many current approaches is that it is not possible to detect when an encryption has failed.

Quantum encryption presents an alternative approach. Not only can more complex keys be implemented, but intrusions are immediately apparent through changes in the transmitted data signal.

While many strategies are being pursued to enable quantum cryptography, one of the leading contenders is based on a phenomenon called photon entanglement. Entangled pairs of photons must be created at exactly the same time with exactly the same properties. Sound

impossible? Enter frequency combs.

The first step in forming the frequency comb occurs when the primary laser generates a secondary pair of wavelengths. However, because of energy conservation, one wavelength must have higher energy and one wavelength must have lower energy. Additionally, the energies must sum to be exactly equal to the primary [laser](#), and the two new wavelengths must appear at exactly the same time. Thus, frequency comb generators can be viewed as entangled photon generators.

While reducing the size and power requirements of the [frequency comb](#) were key technical hurdles, there are many integration and manufacturing challenges remaining before [quantum cryptography](#) on portable platforms will be commonplace.

Armani, a faculty member in the new USC Michelson Center for Convergent Bioscience, indicated that in addition to the important role that [quantum encryption](#) could play in securing our healthcare information in the future, frequency combs are also being used to improve the detection of cancer biomarkers.

The full study "Low threshold parametric oscillation in organically modified microcavities" is available in *Science Advances*.

More information: Xiaoqin Shen et al. Low-threshold parametric oscillation in organically modified microcavities, *Science Advances* (2018). [DOI: 10.1126/sciadv.aao4507](https://doi.org/10.1126/sciadv.aao4507)

Provided by University of Southern California

Citation: Pulses of light to encrypt data and protect security of cryptocurrencies (2018, January

11) retrieved 23 April 2024 from <https://phys.org/news/2018-01-pulses-encrypt-cryptocurrencies.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.