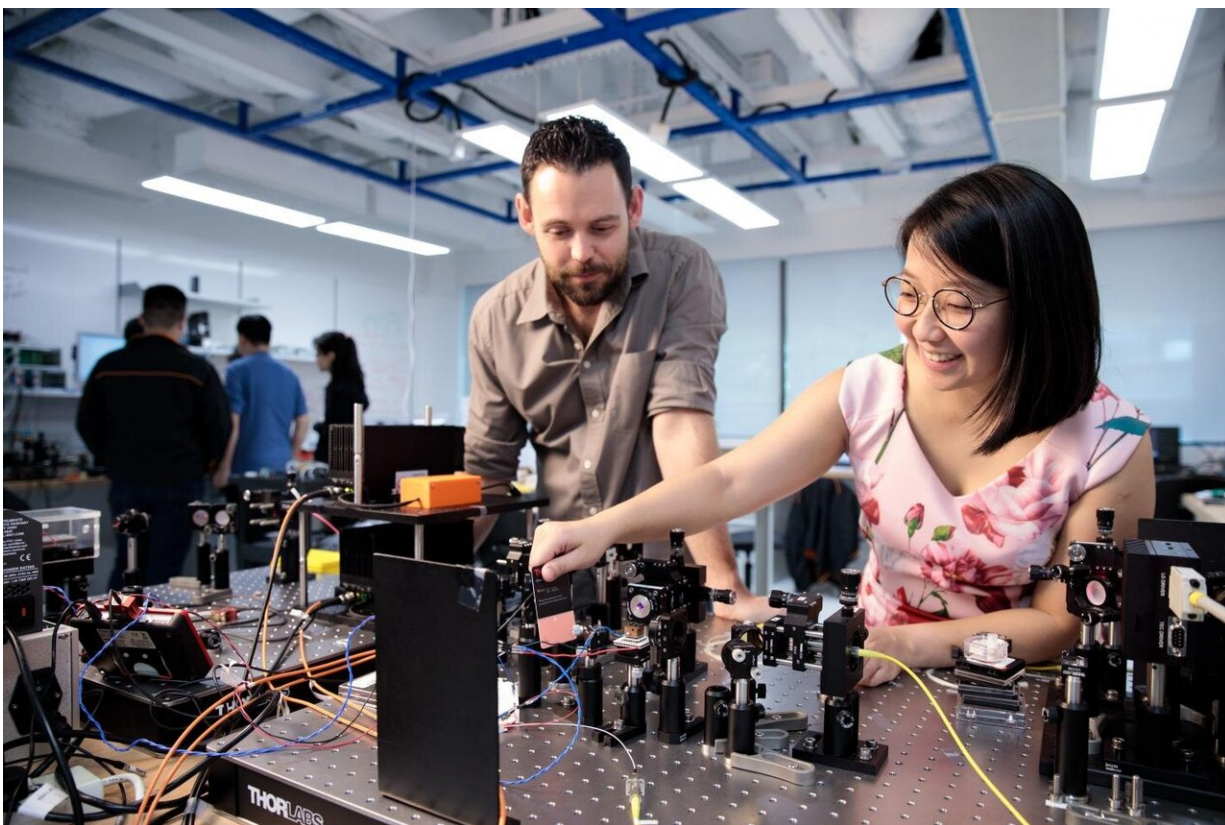


Photons trained for optical fibre obstacle course will deliver stronger cyber security

April 5 2019



Pictured here (from left) are Senior Research Fellow James Grieve of the Centre for Quantum Technologies at NUS and Dr. Amelia Tan, Senior R&D Researcher of Trustwave, Singtel's cyber security subsidiary. Credit: National University of Singapore

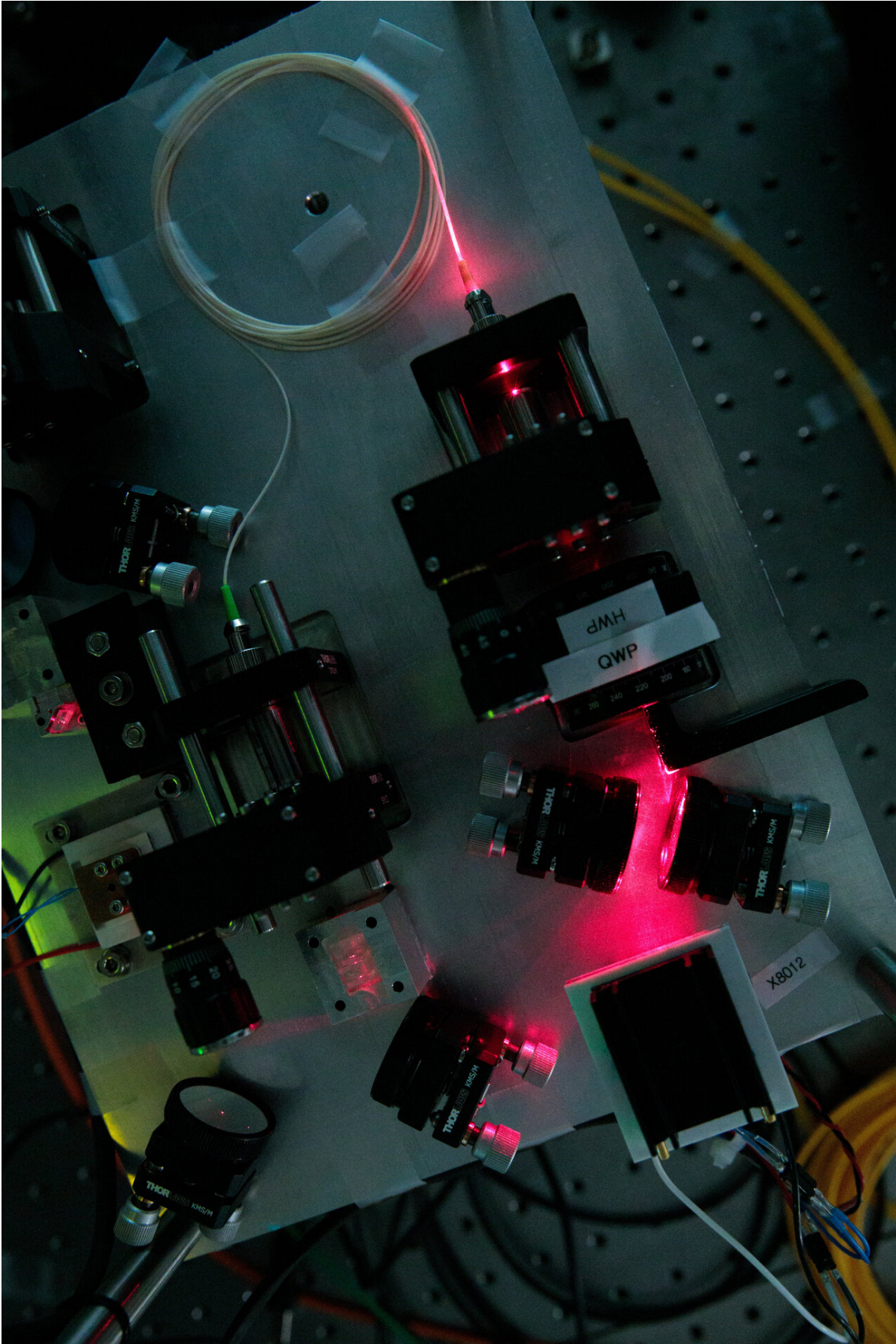
Beneath many cities are complex networks of optical fibres that carry

data, encoded in pulses of light, to offices and homes. Researchers from the National University of Singapore (NUS) and Singtel, Asia's leading communications technology group, have demonstrated a technique that will help pairs of light particles smoothly navigate these networks, a breakthrough that will enable stronger cyber security. The demonstration was performed over 10 km of Singtel's fibre network. This project, conducted in Singapore, is driven by the NUS-Singtel Cyber Security Research & Development Laboratory, a public-private partnership supported by the National Research Foundation, Prime Minister's Office, Singapore. It relies on the expertise from the Centre for Quantum Technologies (CQT) at NUS.

This new approach supports the deployment of a technology known as quantum [key distribution](#) (QKD). Transmitted over [fibre](#) networks, it uses signals sent in particles of light known as photons. Detection of individual photons creates [encryption keys](#) for secure communication. Data encrypted with such keys is resistant to all computational hacks.

QKD trials are being conducted worldwide as governments and companies recognise the need to strengthen their cyber security. The QKD trials carried out by the NUS-Singtel team use pairs of photons that are connected by the quantum property of entanglement. Most QKD schemes require that the sender and receiver of a secret message exchange photons directly or trust the source of their keys. With this alternative approach, it is possible to check the security of a key provided by a third party supplier.

It works like this: the supplier would create a pair of photons, then split them up, sending one each to the two parties that want to communicate securely. The entanglement means that when the parties measure their photons, they get matching results, either a 0 or 1. Doing this for many photons leaves each party with identical patterns of 0s and 1s, giving them a key to lock and unlock a message.



Pictured here is a device developed in the NUS-Singtel Cyber Security R&D Lab that creates particles of light, known as photons, that are connected by the quantum property of entanglement. Credit: National University of Singapore

Typically, each photon encounters a different obstacle course of spliced fibre segments and junction boxes. On their paths, the photons also suffer dispersion, where they effectively spread out. This affects the operators' ability to track the photons.

The new trick, published on 4 April in the scientific journal *Applied Physics Letters*, keeps the entangled photons in sync as they travel different paths through the network. This is important because they are identified by the gap between their arrival times at the detector. "Timing information is what allows us to link pairs of detection events together. Preserving this correlation will help us to create encryption keys faster," says James Grieve, a researcher on the team.

The technique works by carefully designing the [photon](#) source to create pairs of light particles with colours either side of a known feature of optical fibre called the 'zero-dispersion wavelength'. Normally, in [optical fibres](#) bluer light would arrive faster than redder light, spreading out the photons' arrival times. Working around the zero-dispersion point makes it possible to match the speeds through the photons' time-energy entanglement. Then the timing is preserved.

Associate Professor Alexander Ling, a Principal Investigator at CQT, led this work for the NUS-Singtel lab. He said, "Before these results, it was not known if the multi-segment nature of deployed fibre would enable high precision dispersion cancellation, because the segments don't

generally have identical zero dispersion wavelengths."

In showing it can work, the team boosts expectations for QKD over commercial fibre. The entangled photons could find other applications, too. For example, the photons in each pair are created within femtoseconds of each other. Their coordinated arrival times might synchronise clocks for time-critical operations such as financial trading.

More information: James A. Grieve et al, Characterizing nonlocal dispersion compensation in deployed telecommunications fiber, *Applied Physics Letters* (2019). DOI: [10.1063/1.5088830](https://doi.org/10.1063/1.5088830) . Preprint available at: arxiv.org/abs/1901.02204

Provided by Centre for Quantum Technologies at the National University of Singapore

Citation: Photons trained for optical fibre obstacle course will deliver stronger cyber security (2019, April 5) retrieved 19 April 2024 from <https://phys.org/news/2019-04-photons-optical-fibre-obstacle-stronger.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.