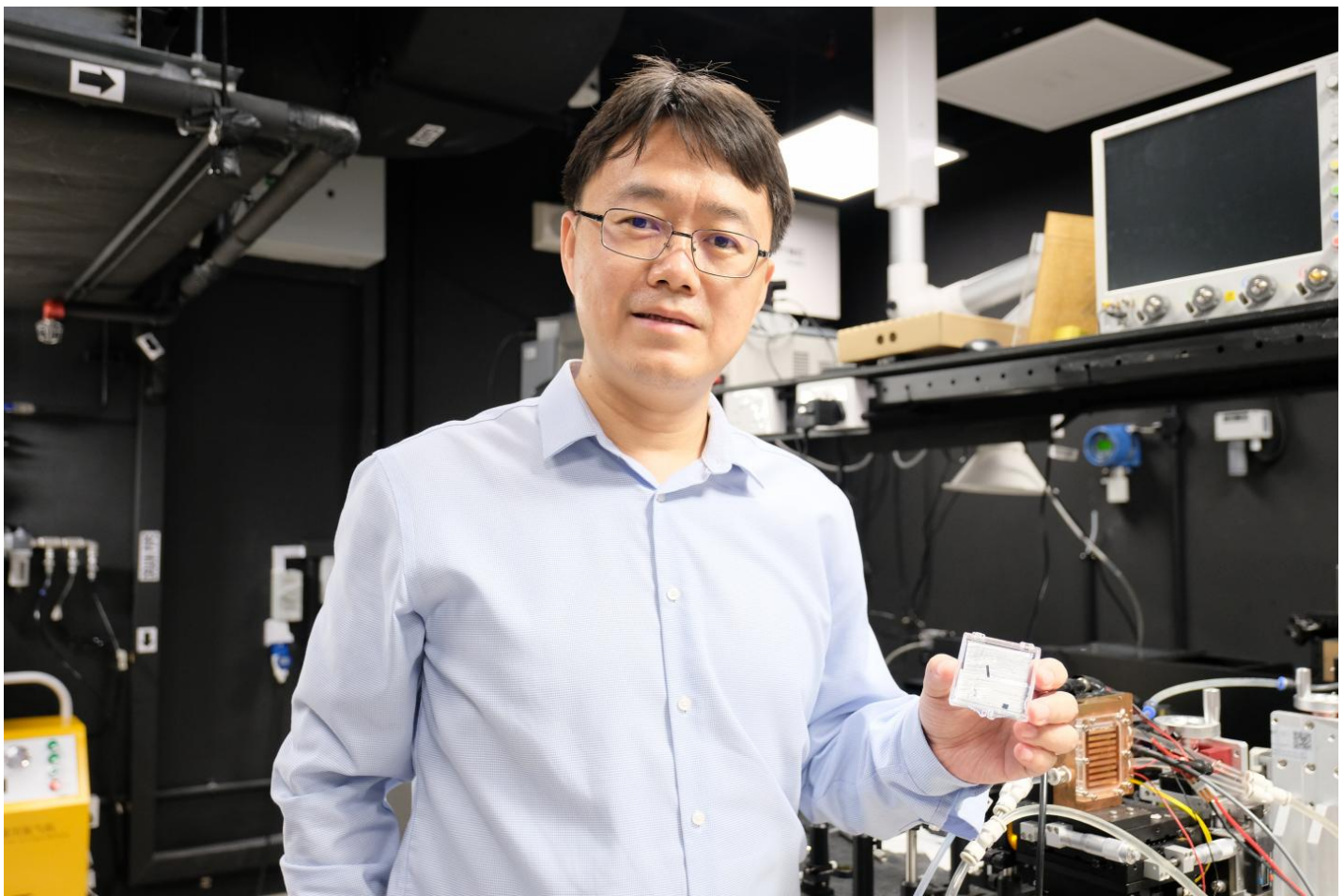


Home > SCIENCE NEWS > Mathematics >

NTU Scientists Develop Laser System That Generates Random Numbers At Ultrafast Speeds

On Feb 25, 2021

MATHEMATICS



Credit: NTU Singapore

An international team of scientists has developed a system that can generate random numbers over a hundred times faster than current technologies, paving the way towards faster, cheaper, and more secure data encryption in today's digitally connected world.

The random generator system was jointly developed by researchers from Nanyang Technological University, Singapore (NTU Singapore), Yale University, and Trinity College Dublin, and made in NTU.

Random numbers are used for a variety of purposes, such as generating data encryption keys and one-time passwords (OTPs) in everyday processes such online banking and e-commerce to shore up their security.

The system uses a laser with a special hourglass-shaped cavity to generate random patterns, which are formed by light rays reflecting and interacting with each other within the cavity. By reading the patterns, the system generates many series of random numbers at the same time (see Image 1).

The researchers found that like snowflakes, no two number sequences generated using the system were the same, due to the unpredictable nature of how the light rays reflect and interact with each other in the cavity.

The laser used in the system is about one millimeter long, smaller than most other lasers. It is also energy efficient and can be operated with any household power socket, as it only requires a one-ampere (1A) current.

In their study published in one of the world's leading scientific journals *Science* on 26 February 2021, the researchers verified the effectiveness of their random number generator using two tests, including one published by the US National Institute of Standards and Technology.

The research team has proven that the NTU-made random number generator which is faster and more secure than existing comparable technologies, could help safeguard users' data in a world that is steadily relying more on Internet transactions (see Image 2).

Professor Wang Qijie from NTU's School of Electrical and Electronic Engineering & School of Physical and Mathematical Science, as well as The Photonics Institute, who led the NTU team involved in the international research, said, "Current random number generators run by computers are cheap and effective. However, they are vulnerable to attacks, as hackers could predict future number sequences if they discover the algorithm used to generate the numbers. Our system is safer as it uses an unpredictable method to generate numbers, making it impossible for even those with the same device to replicate."

Dr Zeng Yongquan, a Research Fellow from NTU's School of Physical and Mathematical Sciences, who co-designed the laser system, said: "Our system surpasses current random number generators, as the method can simultaneously generate many more random sequences of information at an even faster rate."

The team's laser system can also generate about 250 terabytes of random bits per second – more than a hundred times faster than current computer-based random number generators.

At its speed, the system would only take about 12 seconds to generate a body of random numbers equivalent to the size of information in the largest library in the world – the US Library of Congress.

Elaborating on the future of the system, the team is working on making the technology ready for practical use, by incorporating the laser into a compact chip that enables the random numbers generated to be fed directly into a computer.

###