New Laser Number Generator System Could Enable More Secure Data Encryption

Written by AZoOptics Feb 26 2021

A new system created by an international group of researchers exhibits the ability to generate random numbers more than 100 times quicker than existing technologies, thus opening the door to quicker, cost-effective, more secure data encryption in the present-day's digitally connected world.

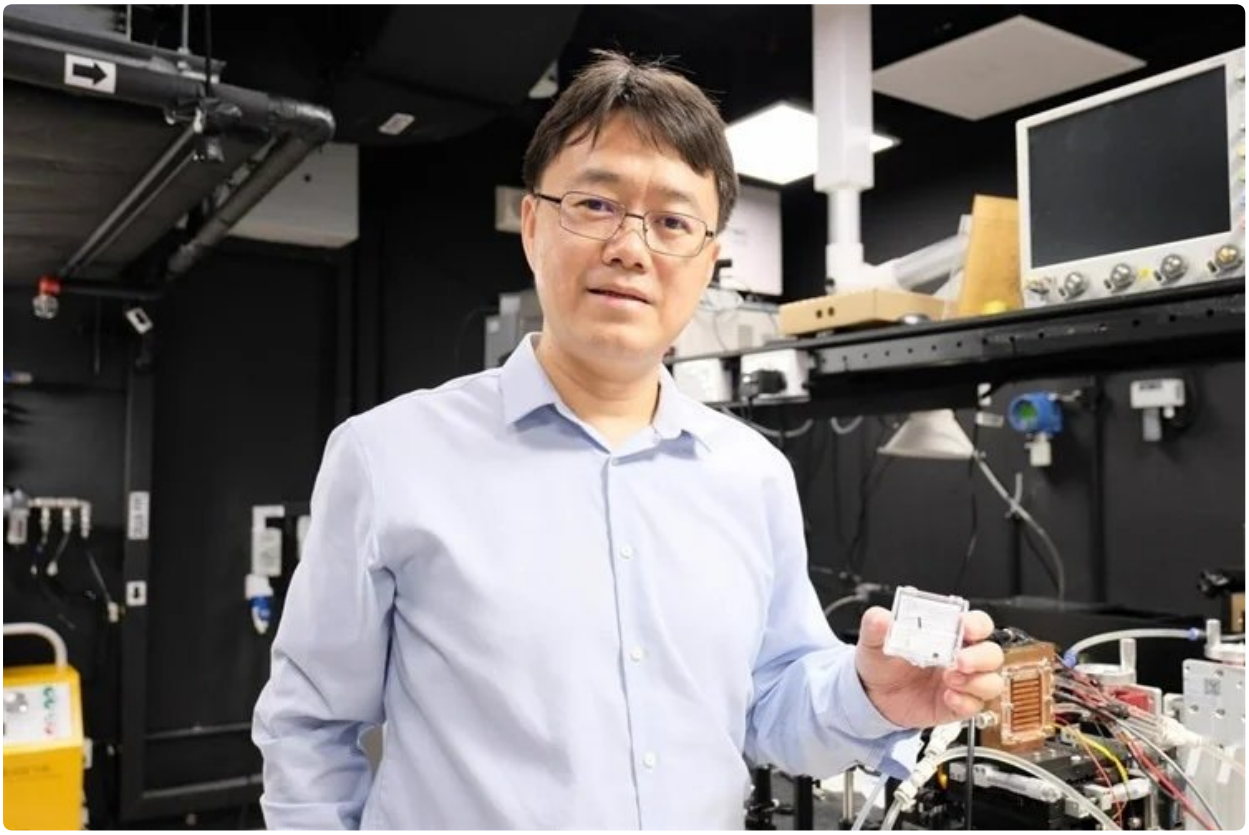

Image Credit: Nanyang Technological University, Singapore.

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

Random numbers serve a range of purposes, for example, producing data encryption keys and one-time passwords (OTPs) in day-to-day processes, such as e-commerce and

online banking to boost up their security.

The system employs a laser with an exclusive hourglass-shaped cavity for generating random patterns, formed by light rays that reflect and interact with each other inside the cavity. The system produces several series of random numbers simultaneously by reading the patterns.

The team observed that similar to snowflakes, no two number series generated with the system were the same.

This because of the unpredictable nature of reflection and interaction of the light rays with each other within the cavity.

The length of the laser employed in the system is nearly 1 mm, which is smaller than a majority of other lasers.

It is energy-efficient and can be operated using any household power socket, as it requires a current of just 1 A.

The study published in *Science*, one of the leading scientific journals in the world, on February 26th, 2021, describes how the researchers confirmed the effectiveness of their random number generator by performing two tests, of which one was published by the U.S. National Institute of Standards and Technology.

The researchers have demonstrated that the NTU-made random number generator—quicker and more secure compared to current comparable technologies—could enable the data of users to be protected in a world that steadily depends more on Internet transactions.

> *"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.*
>
> *Wang Qijie, Professor, School of Electrical and Electronic Engineering and School of Physical and Mathematical Science, Nanyang*

> *Technological University, Singapore*

Qijie is also affiliated with The Photonics Institute and headed the NTU team involved in the international study.

> *"Our system surpasses current random number generators, as the method can simultaneously generate many more random sequences of information at an even faster rate.*
>
> *Dr Zeng Yongquan, Research Fellow, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore*

Dr Yongquan co-designed the team's laser system, which can also generate nearly 250 terabytes of random bits per second—over 100 times faster compared to existing computer-based random number generators.

With its speed, the system would require just 12 seconds to generate a series of random numbers equivalent to the size of information available in the largest library in the world—the U.S. Library of Congress.

The team elaborated on the future of the system by taking efforts to make the technology ready for practical use, by integrating the laser into a small-sized chip that allows the random numbers generated to be directly fed into a computer.

Journal Reference:

Kim, K., *et al*. (2020) Massively parallel ultrafast random bit generation with a chip-scale laser. *Science*. doi.org/10.1126/science.abc2666.

Source: https://www.ntu.edu.sg/Pages/home.aspx