Singapore researchers built the fastest laser-based random number generator

By **Kerem Gülen** - 02/03/2021

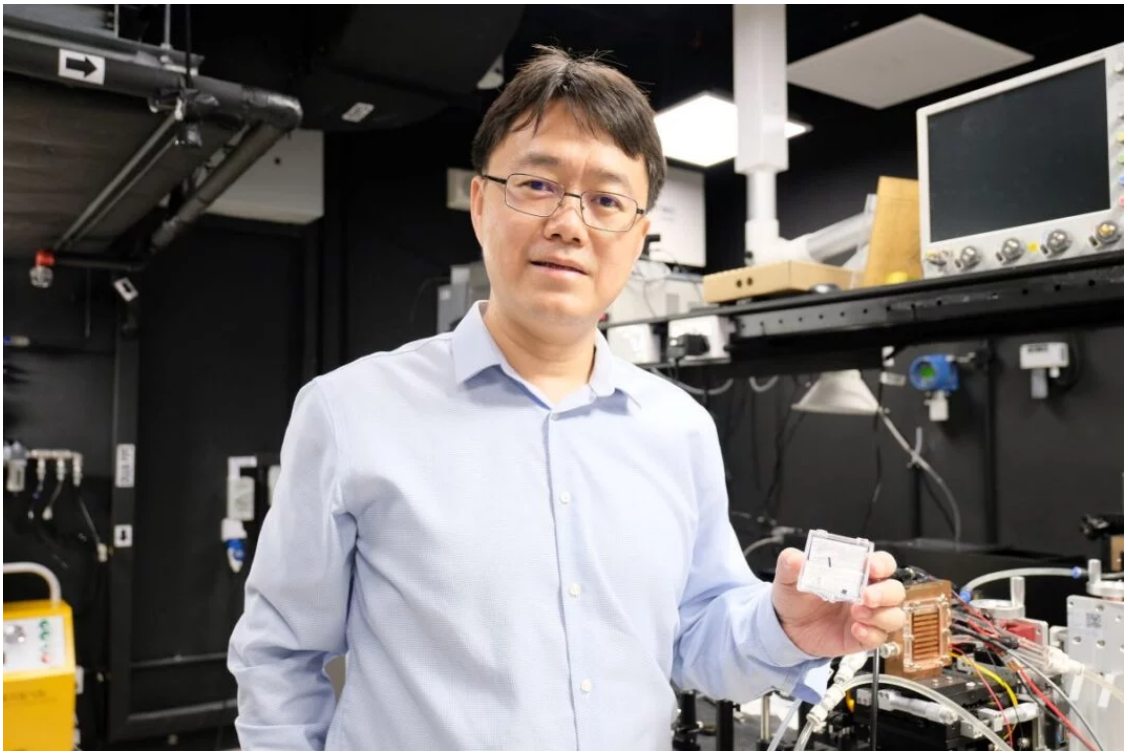
A group of scientists from NTU Singapore, Yale, and Trinity College Dublin have managed to generate up to 250TBs of random numbers per second using a laser-based system, more than 100 times what is generated by current computer-based methods.

Random number generation (RNG) is a key element in the world of cybersecurity. In cryptographic systems, these random numbers make it possible to generate tokens with a high level of entropy and therefore they are more difficult to crack.

Meet the fastest laser-based random number generator

“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,” explains Wang Qijie, a professor at NTU School of Electronics and the Institute of Photonics.

The system uses a laser together with a special hourglass-shaped cavity. The random numbers generated are based on reflections from this cavity. The researchers found that, as with snowflakes, no two number sequences generated were the same, due to the unpredictable nature of the light reflecting off the cavity.



Wang Qijie, a professor at NTU School of Electronics

The laser in the system is one millimeter long, smaller than most lasers. This is telling us that it is an energy-efficient system that operates on a single ampere, so no expensive power source is required.

When the laser is illuminated on a surface, its light contains a constantly changing pattern that brightens randomly due to overlapping. Through a computer, it is possible to translate this brightness to create a random series of ones and zeros.

According to research published at the end of February, researchers have been able to obtain up to 254 trillion digits per second or, rather, 254 points per billionth of a second.

In just 12 seconds, the system could generate a set of random numbers equivalent to the size of the information in the world's largest library, which is in the U.S. Congress.

To work in the real world, this laser random number generator would need to be equipped with light detectors that can send the data in real-time, in order to handle the massive transfer of information obtained.

This work could open a new era in cryptography. Random numbers are used for all sorts of purposes, such as generating data encryption keys and one-time passwords. With its 53-qubit quantum computer, Google showed the power of its project using a random number generator. Now, scientists have found another way to obtain them on a large scale.