

Professor Wang Qijie, der leitende Wissenschaftler bei der Entwicklung des Lasersystems, abgebildet mit einem Prototyp. Bildnachweis: NTU Singapur

Ein internationales Wissenschaftlerteam hat ein System entwickelt, mit dem Zufallszahlen über hundertmal schneller als mit aktuellen Technologien generiert werden können. Dies ebnet den Weg für eine schnellere, billigere und sicherere Datenverschlüsselung in der heutigen digital vernetzten Welt.

Der Zufall **Generator** Das System wurde gemeinsam von Forschern der Nanyang Technological University, Singapur (NTU Singapur), der Yale University und des Trinity College Dublin entwickelt und an der NTU hergestellt.

Zufallszahlen werden für eine Vielzahl von Zwecken verwendet, z. B. zum Generieren von Datenverschlüsselungsschlüsseln und Einmalkennwörtern (OTPs) in alltäglichen Prozessen wie Online-Banking und E-Commerce, um ihre Sicherheit zu gewährleisten.

Das System verwendet einen Laser mit einem speziellen sanduhrförmigen Hohlraum, um zufällige Muster zu erzeugen, die durch Lichtstrahlen gebildet werden, die innerhalb des Hohlraums reflektieren und miteinander interagieren. Durch das Lesen der Muster erzeugt das System viele Serien von **zufällige Zahlen** gleichzeitig (siehe Bild 1).

Die Forscher fanden heraus, dass wie Schneeflocken keine zwei **Nummer** Die mit dem System erzeugten Sequenzen waren aufgrund der unvorhersehbaren Art und Weise, wie die Lichtstrahlen im Hohlraum reflektieren und miteinander interagieren, dieselben.

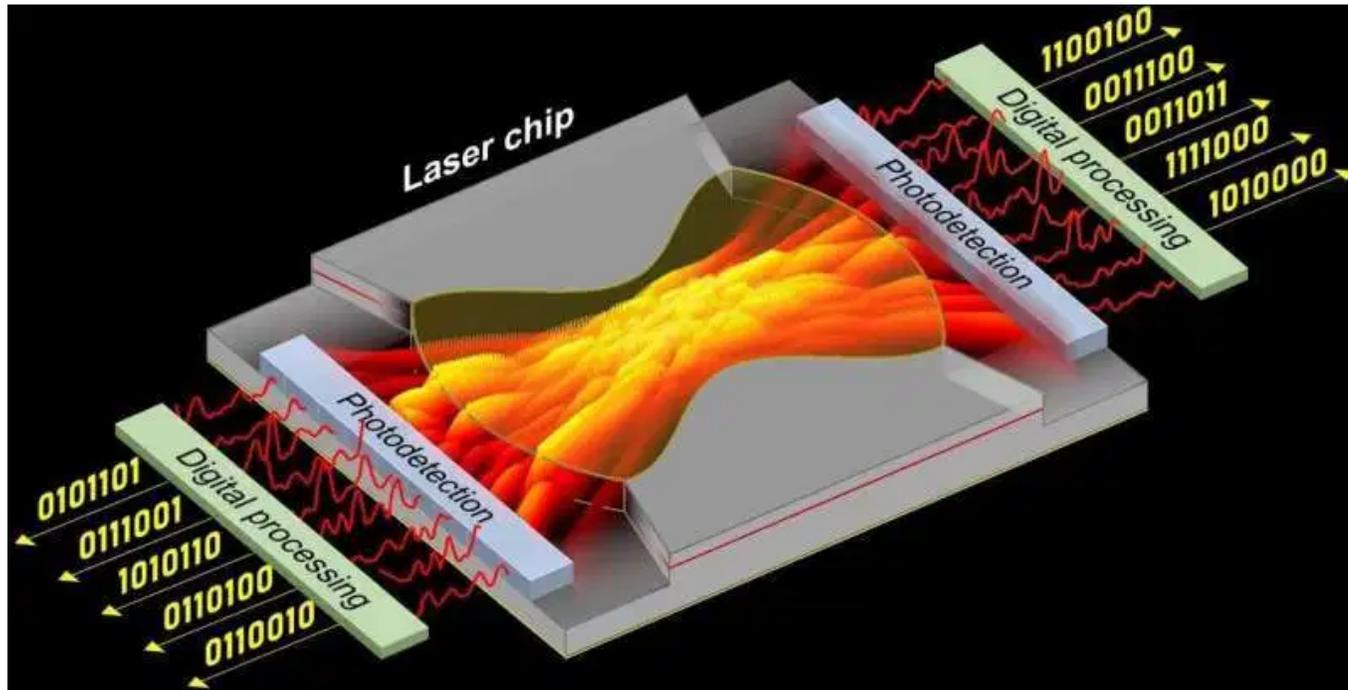
Der im System verwendete Laser ist etwa einen Millimeter lang und kleiner als die meisten anderen Laser. Es ist außerdem energieeffizient und kann mit jeder Haushaltssteckdose betrieben werden, da nur ein Strom von 1 Ampere (1A) benötigt wird.

Professor Wang Qijie, der leitende Wissenschaftler bei der Entwicklung des Lasersystems, abgebildet mit einer Nahaufnahme des Prototyps. Bildnachweis: NTU Singapur

In ihrer Studie in einer der weltweit führenden wissenschaftlichen Zeitschriften veröffentlicht *Wissenschaft Am 26. Februar 2021* überprüften die Forscher die Wirksamkeit ihres Zufallszahlengenerators anhand von zwei Tests, darunter einem, der vom US-amerikanischen National Institute of Standards and Technology veröffentlicht wurde.

Das Forschungsteam hat bewiesen, dass die NTU herstellt **Zufallszahlengenerator** Dies ist schneller und sicherer als bestehende vergleichbare Technologien und könnte dazu beitragen, die Daten der Benutzer in einer Welt zu schützen, in der immer mehr auf Internet-Transaktionen angewiesen ist (siehe Abbildung 2).

Professor Wang Qijie von der Fakultät für Elektrotechnik und Elektronik der NTU und der Fakultät für Physik und Mathematik sowie vom Photonics Institute, der das an der internationalen Forschung beteiligte NTU-Team leitete, sagte: "Aktuelle Zufallszahlengeneratoren, die von Computern betrieben werden, sind billig und Sie sind jedoch anfällig für Angriffe, da Hacker zukünftige Zahlenfolgen vorhersagen könnten, wenn sie den Algorithmus entdecken, der zum Generieren der Zahlen verwendet wird. Unser System ist sicherer, da es eine unvorhersehbare Methode zum Generieren von Zahlen verwendet, was es selbst für diejenigen mit dem unmöglich macht das gleiche Gerät zu replizieren. "



Das von NTU entworfene System zeichnet Lichtmuster auf, die durch die Reflexion eines Laserstrahls verursacht werden, und verwendet diese dann, um eine Reihe von Zufallszahlen zu erzeugen. Bildnachweis: NTU Singapur

Dr. Zeng Yongquan, ein wissenschaftlicher Mitarbeiter der Fakultät für Physikalische und Mathematische Wissenschaften der NTU, der das Lasersystem mitgestaltet hat, sagte: "Unser System übertrifft die aktuellen Zufallszahlengeneratoren, da die Methode gleichzeitig viel mehr zufällige Informationssequenzen an einem erzeugen kann noch schneller."

Das Lasersystem des Teams kann außerdem etwa 250 Terabyte Zufallsbits pro Sekunde erzeugen – mehr als hundertmal schneller als aktuelle computergestützte Zufallszahlengeneratoren.