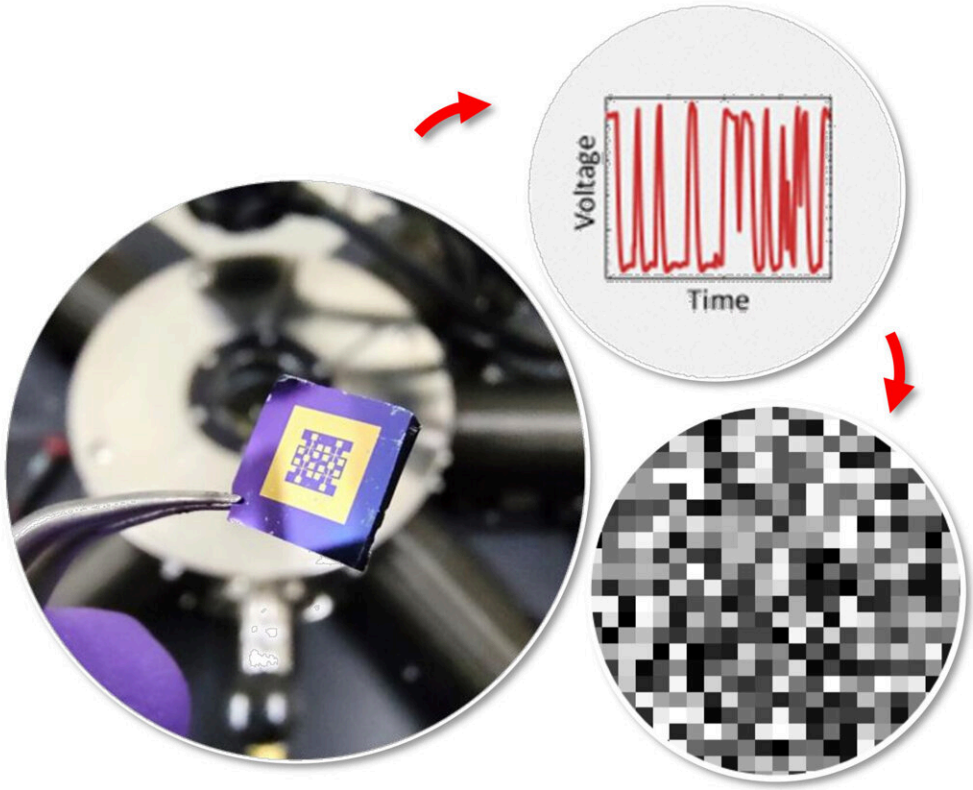
How randomly moving electrons can improve cyber security

May 27 2022



The image of the fabricated electronic chip that generates the random number. The chip is loaded into the measurement setup, where the randomness of the electron trapping/de-trapping is converted into binary outputs. Credit: Nithin Abraham

In October 2017, tech giant Yahoo! disclosed a data breach that had leaked sensitive information of over 3 billion user accounts, exposing them to identity theft. The company had to force all affected users to change passwords and re-encrypt their credentials. In recent years, there have been several instances of such security breaches that have left users vulnerable.

"Almost everything we do on the internet is encrypted for security. The strength of this encryption depends on the quality of random number generation," says Nithin Abraham, a Ph.D. student at the Department of Electrical Communication Engineering (ECE), Indian Institute of Science (IISc). Abraham is a part of a team led by Kausik Majumdar, Associate Professor at ECE, which has developed a record-breaking true random number generator (TRNG), which can improve data encryption and provide improved security for sensitive digital data such as credit card details, passwords and other personal information. The study describing this device has been published in the journal *ACS Nano*.

Encrypted information can be decoded only by authorized users who have access to a cryptographic "key." But the key needs to be unpredictable and, therefore, randomly generated to resist hacking. Cryptographic keys are typically generated in computers using pseudorandom number generators (PRNGs), which rely on mathematical formulae or pre-programmed tables to produce numbers that appear random but are not. In contrast, a TRNG extracts random numbers from inherently random physical processes, making it more secure.

In IISc's breakthrough TRNG device, random numbers are generated using the random motion of electrons. It consists of an artificial electron trap constructed by stacking atomically-thin layers of materials like black phosphorus and graphene. The current measured from the device increases when an electron is trapped, and decreases when it is released. Since electrons move in and out of the trap in a random manner, the

measured current also changes randomly. The timing of this change determines the generated random number. "You cannot predict exactly at what time the electron is going to enter the trap. So, there is an inherent randomness that is embedded in this process," explains Majumdar.

The performance of the device on the standard tests for cryptographic applications designed by the U.S. National Institute of Standards and Technology (NIST) has exceeded Majumdar's own expectations. "When the idea first struck me, I knew it would be a good random number generator, but I didn't expect it to have a record-high min-entropy," he says.

Min-entropy is a parameter used to measure the performance of TRNGs. Its value ranges from 0 (completely predictable) to 1 (completely random). The device from Majumdar's lab showed a record-high min-entropy of 0.98, a significant improvement over previously reported values, which were around 0.89. "Ours is by far the highest reported min-entropy among TRNGs," says Abraham.

The team's electronic TRNG is also more compact than its clunkier counterparts that are based on optical phenomena, says Abraham. "Since our device is purely electronic, millions of such devices can be created on a single chip," adds Majumdar. He and his group plan to improve the device by making it faster and developing a new fabrication process that would enable the mass production of these chips.

More information: Nithin Abraham et al, A High-Quality Entropy Source Using van der Waals Heterojunction for True Random Number Generation, *ACS Nano* (2022). DOI: 10.1021/acsnano.1c11084

Provided by Indian Institute of Science