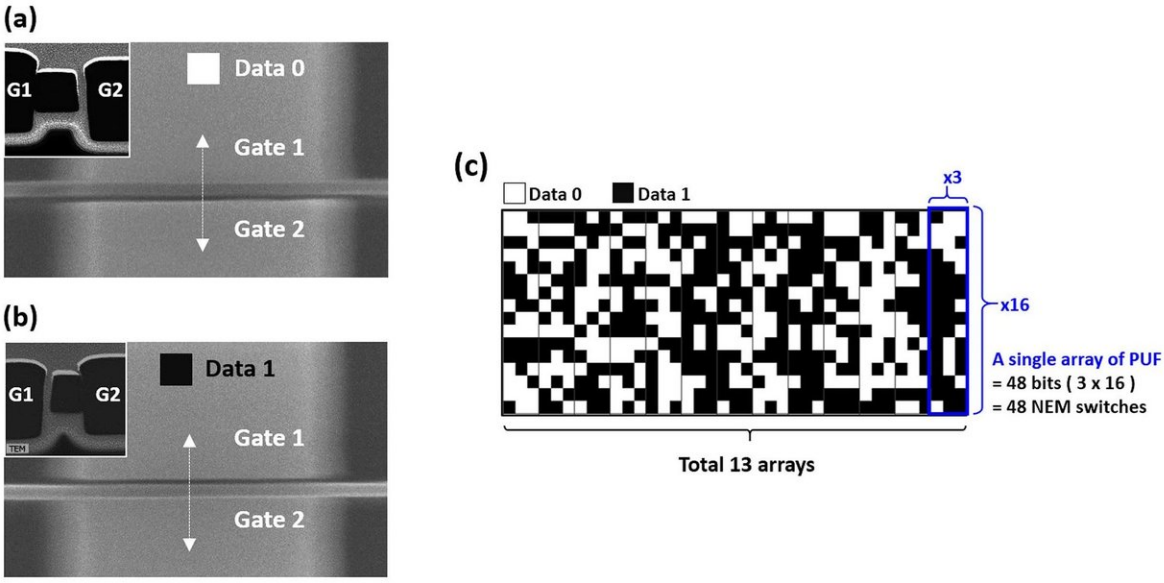
Nanoscale cryptography method gains robustness from stiction

January 4 2018, by Lisa Zyga



(a) The "0" state and (b) the "1" state correspond to the silicon nanowire touching either gate 1 or gate 2, respectively. (c) 13 PUF arrays consisting of 48 bits each. The randomness of the data originates from the random variations that occur during fabrication and cause the nanowire to randomly bend toward one of the two gates due to stiction. Credit: Hwang et al. ©2017 American Chemical Society

Most of the cryptographic methods that keep important data secure use

complex encryption software, and as a result, consume large amounts of power. As more and more electronic devices are being connected to the internet, there is a growing need for alternative low-power security methods, and this is often done by basing the security on hardware rather than software.

One of the most promising approaches to hardware-based, low-power security is to derive cryptographic keys from the randomness that inherently and uncontrollably emerges during the fabrication process of nanoscale devices. These methods, called "physical unclonable functions" (PUFs), convert the random variations in the physical devices into the binary states of "0" and "1" to create unique, random cryptographic keys. These keys can then be used to encrypt data into cipher text, as well as decrypt it back into plain text, in a process that remains secure as long as the key remains private.

However, one of the biggest challenges facing PUF technology is its vulnerability to harsh environments. Since the physical randomness that forms the basis of the key usually arises from variations in electrical characteristics, and electrical characteristics are affected by external factors such as high temperatures and radiation, these devices often do not preserve their states when exposed to such conditions.

In a new paper published in *ACS Nano*, researchers led by Yang-Kyu Choi at the Korea Advanced Institute of Science and Technology (KAIST), with coauthors from Samsung Electronics and SK Hynix Inc., have developed a new type of PUF device that remains stable under harsh conditions by taking advantage of a surprising factor: stiction.

Normally, stiction is a major failure phenomenon for micro- electro mechanical system and nano-electro mechanical system (MEMS/NEMS) devices, as it causes components to stick together due to forces that become prominent below the micrometer scale. In their work, however,

the researchers used stiction to their advantage by naturally inducing a strong capillary force during the drying step of the fabrication process. This force causes the silicon nanowire in the device to randomly bend in one of two directions, so that it touches either the gate on one side (corresponding to the "0" state) or the gate on the other side (the "1" state). A second force, the van der Waals force, causes the nanowire to remain adhered to the gate, maintaining its state.

The researchers demonstrated that this adhesion force is strong enough to withstand harsh environmental factors such as high temperatures, high-dose radiation, and microwaves. In a 288-bit array, not a single bit failed when exposed to these conditions.

Tests also showed that, due to the symmetric structure of the device, the nanowire has an equal probability of adhering to either of the two gates, indicating a high degree of randomness. When dozens of these devices are arranged in an array, they produce an unpredictable pattern of "0's" and "1's" that form the basis of a unique cryptographic key.

With its good randomness and reliability, the new security method could be used for aerospace and military applications.

"The NEM switch-based PUF provides two advantages: high compatibility with commercial silicon CMOS fabrication and robust stability," Choi told *Tech Xplore*. "The interesting things are that we used stiction, one of the chronic problems associated with NEMS, in order to improve robustness. Moreover, it can be self-destructing with a stealth mode when it is stolen and faces cyber-attack."

In the future, the researchers plan to further improve the security by doubling the encryption key size.

"We are planning to find a revamped method to enhance security by

increasing an encryption key size," Choi said. "In our paper, the silicon nanowire in the device had only a binary state ('0', '1'). In contrast, by subdividing the state of a single silicon nanowire more precisely, we can make a quarternary state ('00', '01', '10', '11'). This will make the effect of doubling the encryption key size without increasing an array size."

More information: Kyu-Man Hwang et al. "Nano-electromechanical Switch Based on a Physical Unclonable Function for Highly Robust and Stable Performance in Harsh Environments." *ACS Nano*. DOI: 10.1021/acsnano.7b06658