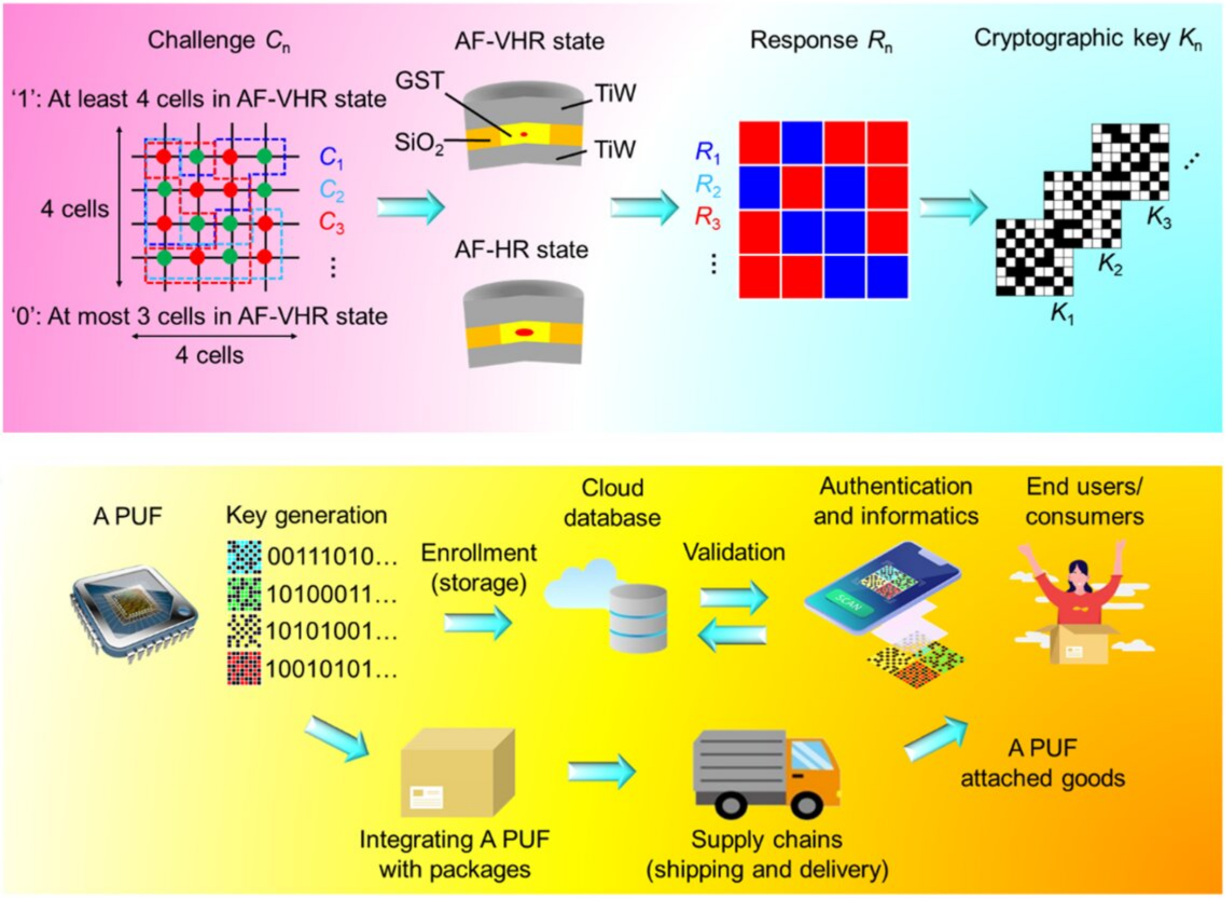
Researchers develop a phase-change key for new hardware security

November 18 2022



Graphic of the new types of PUF that can be designed using the phase-change material (PCM), based on the reversible switching between the amorphous glassy state and orderly crystal state of a chalcogenide layer, along with sensing different as-deposited amorphous states, showing a large contrast in electrical and optical properties (top panel). Schematic of the product authentication concept (bottom panel). Credit: Singapore University of Technology and Design

As more and more data are being shared and stored digitally, the number of data breaches taking place around the world is on the rise. Scientists are exploring new ways to secure and protect data from increasingly sophisticated cyber attacks.

A new type of reconfigurable, scalable, low power hardware security device with high resilience to AI attacks has been developed by researchers using phase-change materials. This research is led by Assistant Professor Desmond Loke from the Singapore University of Technology and Design (SUTD), and the study is published in *Advanced Science*.

Dr. Loke said, "We developed a novel hardware security device that can eventually be implemented to protect data across sectors and industries, as breaches in private data have been ever-increasing."

The device, known as the physical unclonable function (PUF), is a new type of phase-change PUF that is scalable, more energy-efficient and secure against AI attacks compared to traditional silicon PUFs. This is due to the electrical and physical properties of phase-change materials, along with the fabrication process.

The SUTD research team fabricated a group of phase-change devices, which switch reversibly between the glassy amorphous state and crystal orderly state. They then used the variation in the device's electrical conductance to construct the PUF due to the inherent randomness arising from the manufacturing process, which is not shown by conventional silicon-based devices.

The researchers modeled the characteristics of actual phase-change devices to generate a simulation of many more phase-change-based

PUFs. Dr. Loke and his team used machine learning, a method that allows AI to study a system and find new patterns, to test the PUF's security. To examine if the AI could use this training to make predictions about the encrypted key and reveal system insecurities, the researchers trained the AI with the phase-change PUF simulation data.

Dr. Loke added, "Normal humans are not able to develop a model from a vast amount of data, but neural networks could. We also found that it was not possible for the encryption process to be learned and that the AI could not develop a model to decrypt the phase-change PUF."

As potential hackers could not use the "stolen" key to reverse engineer a device for future use, the resistance to machine learning attacks makes the PUF more secure. The phase-change PUF can also create a new key immediately through the reconfiguration mode if the key is hacked.

The phase-change PUF could be used in a variety of applications with these features, together with the capacity to operate at high temperatures. Future research can pave a way for its use in household devices, printable and flexible electronics and other devices.

More information: Shao-Xiang Go et al, Ultrafast Near-Ideal Phase-Change Memristive Physical Unclonable Functions Driven by Amorphous State Variations, *Advanced Science* (2022). DOI: 10.1002/advs.202204453

Provided by Singapore University of Technology and Design

Citation: Researchers develop a phase-change key for new hardware security (2022, November 18) retrieved 16 April 2024 from https://techxplore.com/news/2022-11-phase-change-key-hardware.html