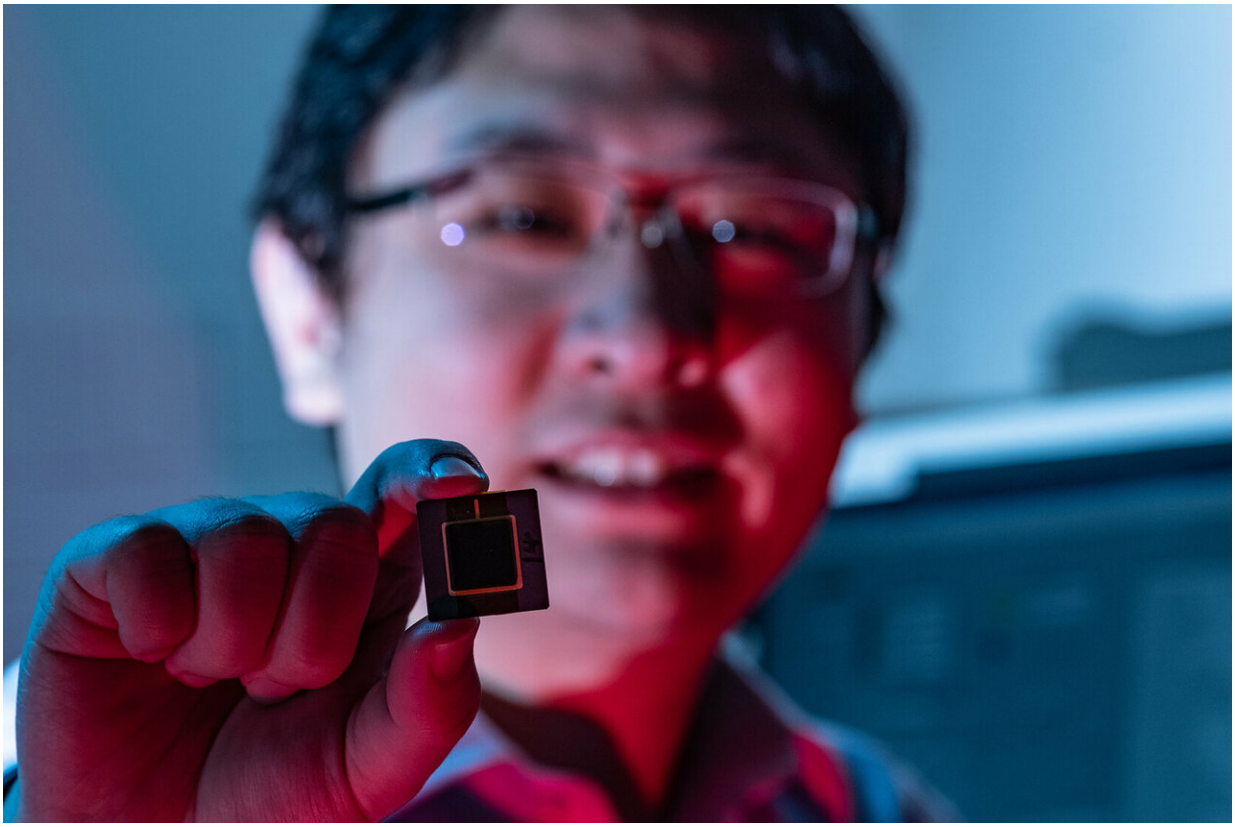
Physically unclonable function: Researchers unveil Internet of Things security feature

February 20 2019



Rice University integrated circuit designer Kaiyuan Yang with a prototype of a new device that is 10 times more reliable than current methods of producing unclonable digital fingerprints for Internet of Things (IoT) devices. Credit: Jeff Fitlow/Rice University

Rice University integrated circuit (IC) designers are at Silicon Valley's

premier chip-design conference to unveil technology that is 10 times more reliable than current methods of producing unclonable digital fingerprints for Internet of Things (IoT) devices.

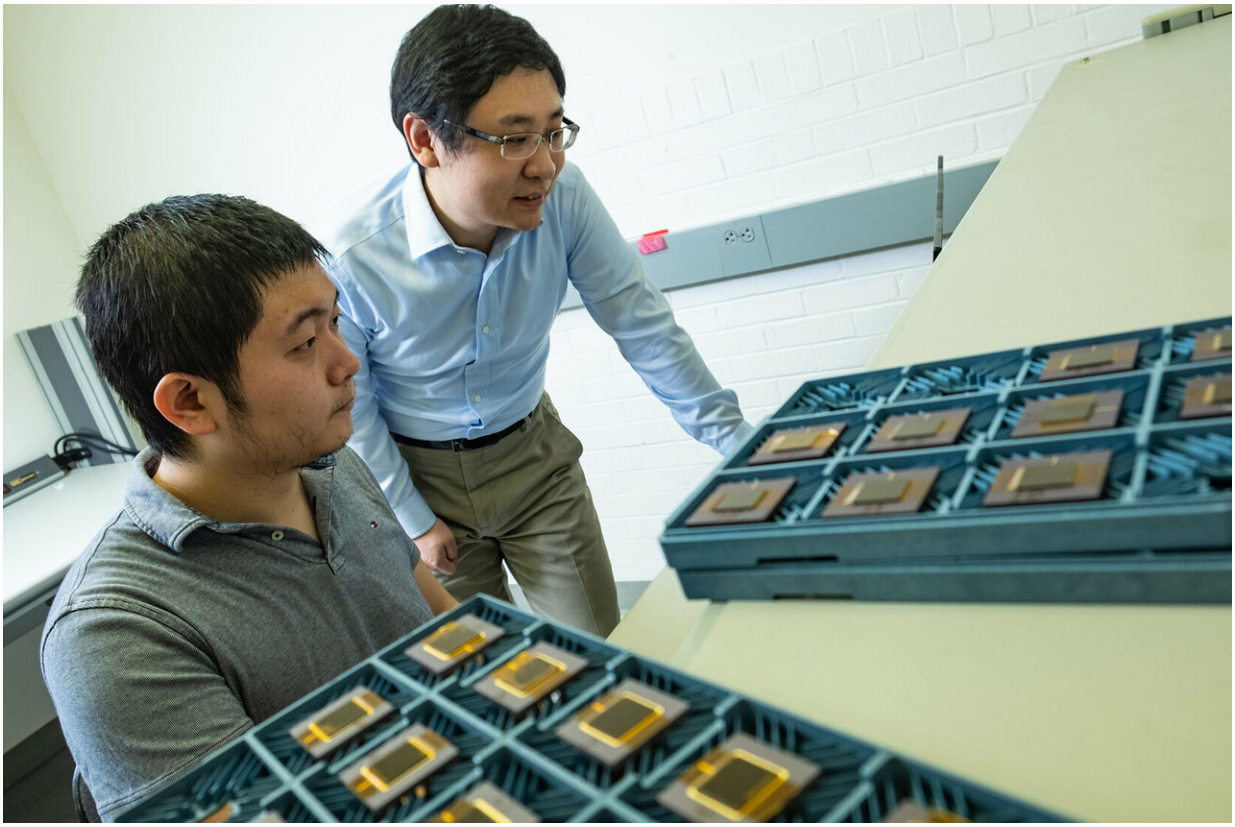
Rice's Kaiyuan Yang and Dai Li will present their physically unclonable function (PUF) technology today at the 2019 International Solid-State Circuits Conference (ISSCC), a prestigious scientific conference known informally as the "Chip Olympics." PUF uses a microchip's physical imperfections to produce unique security keys that can be used to authenticate devices linked to the Internet of Things.

Considering that some experts expect Earth to pass the threshold of 1 trillion internet-connected sensors within five years, there is growing pressure to improve the security of IoT devices.

Yang and Li's PUF provides a leap in reliability by generating two unique fingerprints for each PUF. This "zero-overhead" method uses the same PUF components to make both keys and does not require extra area and latency because of an innovative design feature that also allows their PUF to be about 15 times more energy efficient than previously published versions.

"Basically each PUF unit can work in two modes," said Yang, assistant professor of electrical and computer engineering. "In the first mode, it creates one fingerprint, and in the other mode it gives a second fingerprint. Each one is a unique identifier, and dual keys are much better for reliability. On the off chance the device fails in the first mode, it can use the second key. The probability that it will fail in both modes is extremely small."

As a means of authentication, PUF fingerprints have several of the same advantages as human fingerprints, he said.



Dai Li (left) and Kaiyuan Yang of Rice University's VLSI Lab will present their new security technology at the 2019 International Solid-State Circuits Conference (ISSCC), which is informally known as the 'Chip Olympics.' Credit: Jeff Fitlow/Rice University

"First, they are unique," Yang said. "You don't have to worry about two people having the same fingerprint. Second, they are bonded to the individual. You cannot change your fingerprint or copy it to someone else's finger. And finally, a fingerprint is unclonable. There's no way to create a new person who has the same fingerprint as someone else."

PUF-derived encryption keys are also unique, bonded and unclonable. To understand why, it helps to understand that each transistor on a

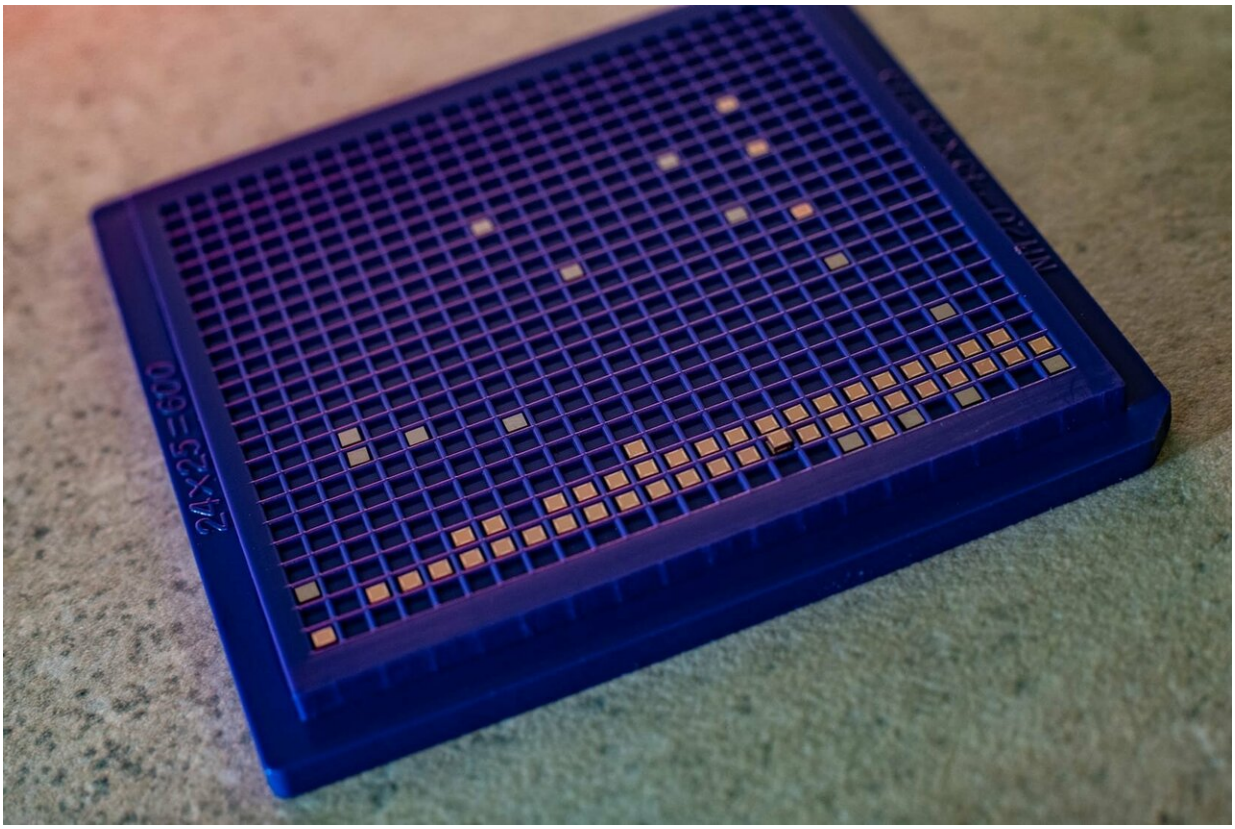
computer chip is incredibly small. More than a billion of them can be crammed onto a chip half the size of a credit card. But for all their precision, microchips are not perfect. The difference between transistors can amount to a few more atoms in one or a few less in another, but those miniscule differences are enough to produce the electronic fingerprints used to make PUF keys.

For a 128-bit key, a PUF device would send request signals to an array of PUF cells comprising several hundred transistors, allocating a one or zero to each bit based on the responses from the PUF cells. Unlike a numeric key that's stored in a traditional digital format, PUF keys are actively created each time they're requested, and different keys can be used by activating a different set of transistors.

Adopting PUF would allow chipmakers to inexpensively and securely generate secret keys for encryption as a standard feature on next-generation computer chips for IoT devices like "smart home" thermostats, security cameras and lightbulbs.

Encrypted lightbulbs? If that sounds like overkill, consider that unsecured IoT devices are what three young computer savants assembled by the hundreds of thousands to mount the October 2016 distributed denial-of-service attack that crippled the internet on the East Coast for most of a day.

"The general concept for IoT is to connect physical objects to the internet in order to integrate the physical and cyber worlds," Yang said. "In most consumer IoT today, the concept isn't fully realized because many of the devices are powered and almost all use existing IC feature sets that were developed for the mobile market."



Rice's new design for creating security keys with a physically unclonable function (PUF) proved more reliable, more energy efficient and smaller than previously published PUF technologies. Credit: Jeff Fitlow/Rice University

In contrast, the devices coming out of research labs like Yang's are designed for IoT from the ground up. Measuring just a few millimeters in size, the latest IoT prototypes can pack a processor, flash memory, wireless transmitter, antenna, one or more sensors, batteries and more into an area the size of a grain of rice.

PUF is not a new idea for IoT security, but Yang and Li's version of PUF is unique in terms of reliability, energy efficiency and the amount of area it would take to implement on a chip. For starters, Yang said the performance gains were measured in tests at military-grade temperatures

ranging from 125 degrees Celsius to minus 55 degrees Celsius and when supply voltage dropped by up to 50 percent.

"If even one transistor behaves abnormally under varying environmental conditions, the device will produce the wrong key, and it will look like an inauthentic device," Yang said. "For that reason, reliability, or stability, is the most important measure for PUF."

Energy efficiency also is important for IoT, where devices can be expected to run for a decade on a single battery charge. In Yang and Li's PUF, keys are created using a static voltage rather than by actively powering up the transistor. It's counterintuitive that the static approach would be more energy efficient because it's the equivalent of leaving the lights on 24/7 rather than flicking the switch to get a quick glance of the room.

"Normally, people have sleep mode activated, and when they want to create a key, they activate the transistor, switch it once and then put it to sleep again," Yang said. "In our design, the PUF module is always on, but it takes very little power, even less than a conventional system in sleep mode."

On-chip area—the amount of space and expense manufacturers would have to allocate to put the PUF device on a production chip—is the third metric where they outperform previously reported work. Their design occupied 2.37 square micrometers to generate one bit on prototypes produced using 65-nanometer complementary metal-oxide-semiconductor (CMOS) technology.

Provided by Rice University

Citation: Physically unclonable function: Researchers unveil Internet of Things security feature