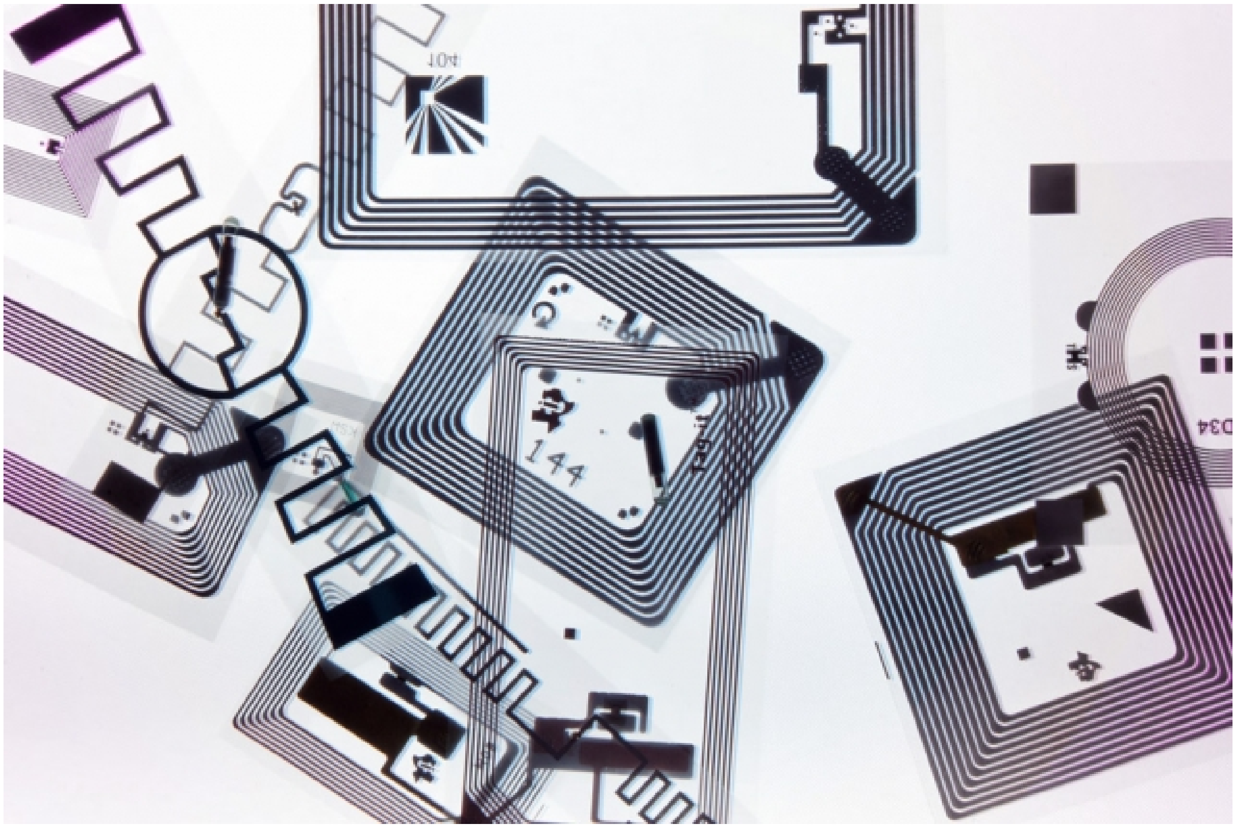
PHYS.ORG

"Fingerprinting" chips to fight counterfeiting

May 1 2015, by Rob Matheson



MIT spinout Verayo has created technology that tracks random variations in silicon chips to assign them unique "fingerprints." Integrated into radio frequency identification tags (shown here), the chips can be scanned by a mobile device or reader to determine if the tag is authentic. Credit: Verayo

It's often said that no two human fingerprints are exactly alike. For that reason, police often use them as evidence to link suspects to crime scenes.

The same goes for silicon chips: Manufacturing processes cause microscopic variations in chips that are unpredictable, permanent, and effectively impossible to clone.

MIT spinout Verayo is now using these unclonable variations to "fingerprint" silicon chips used in consumer-product tags—which can then be scanned via mobile device and authenticated—to aid in the fight against worldwide counterfeiting.

According to a 2013 United Nations report, about 2 to 5 percent of internationally traded goods—including electronics, food, and pharmaceuticals—are counterfeited, costing governments and private companies hundreds of billions of dollars annually.

"This is low-cost authentication using 'silicon biometrics,'" says Srini Devadas, the Edwin Sibley Webster Professor in MIT's Department of Electrical Engineering and Computer Science, and Verayo's co-founder and chief scientist.

Verayo's technology—now in use worldwide—is based on Devadas' seminal research into these variations within silicon chips, called "physical unclonable functions" (PUFs), which cause minute speed differences in a chip's response to electrical signals.

The Verayo technology assigns manufactured chips sets of 128-bit numbers—based on these speed differences—that are stored in a database in the cloud. Integrated into radio frequency identification (RFID) tags, the chips can be scanned by a mobile device or reader that will query the database to determine if the tag is authentic. A different 128-bit number is used for each authentication.

Verayo is currently targeting the consumer-product market, partnering last year with its largest client, Canon Inc., to incorporate Verayo's chips into RFID tags of cameras being sold across China. Other Verayo clients include gift- and loyalty-card providers. The technology can also be used to identify fake licenses and passports.

Now conducting pilot studies with wineries, the company is also seeking to penetrate the consumables market, which could significantly boost sales, Devadas says. "You can build this chip for a nickel, but you have to sell a lot of these chips to make money," he says.

But with more than 40 million chips sold worldwide since 2013, Devadas adds, "This is productization and academic success. As far as I'm concerned, this is great."

A Verayo chip is integrated into a label on a Canon camera box. When scanned with a mobile device, a check mark signifies that the chip is authentic. Credit: Srini Devadas

Racing signals

PUFs are created during silicon-chip manufacturing, when wires vary in thickness, and the chemical vapor deposition process—used to produce semiconductor wafers—creates microscopic bumps. Depending on these variations, electrons flow with more or less resistance through different paths of the chip, varying processing speeds.

The PUF technology works by "racing" signals across the chips. Two identical electric signals—derived from an input "challenge"—are sent through the chip, at the same time, and assigned two different paths. The signals race toward a latch that measures what signal the chip processed slower or faster—called a "response." The output is a 1 if one path is faster, and 0 if the other is faster. Repeating the process with different input signals for each race will give a 128-bit number—and it can be repeated hundreds of times.

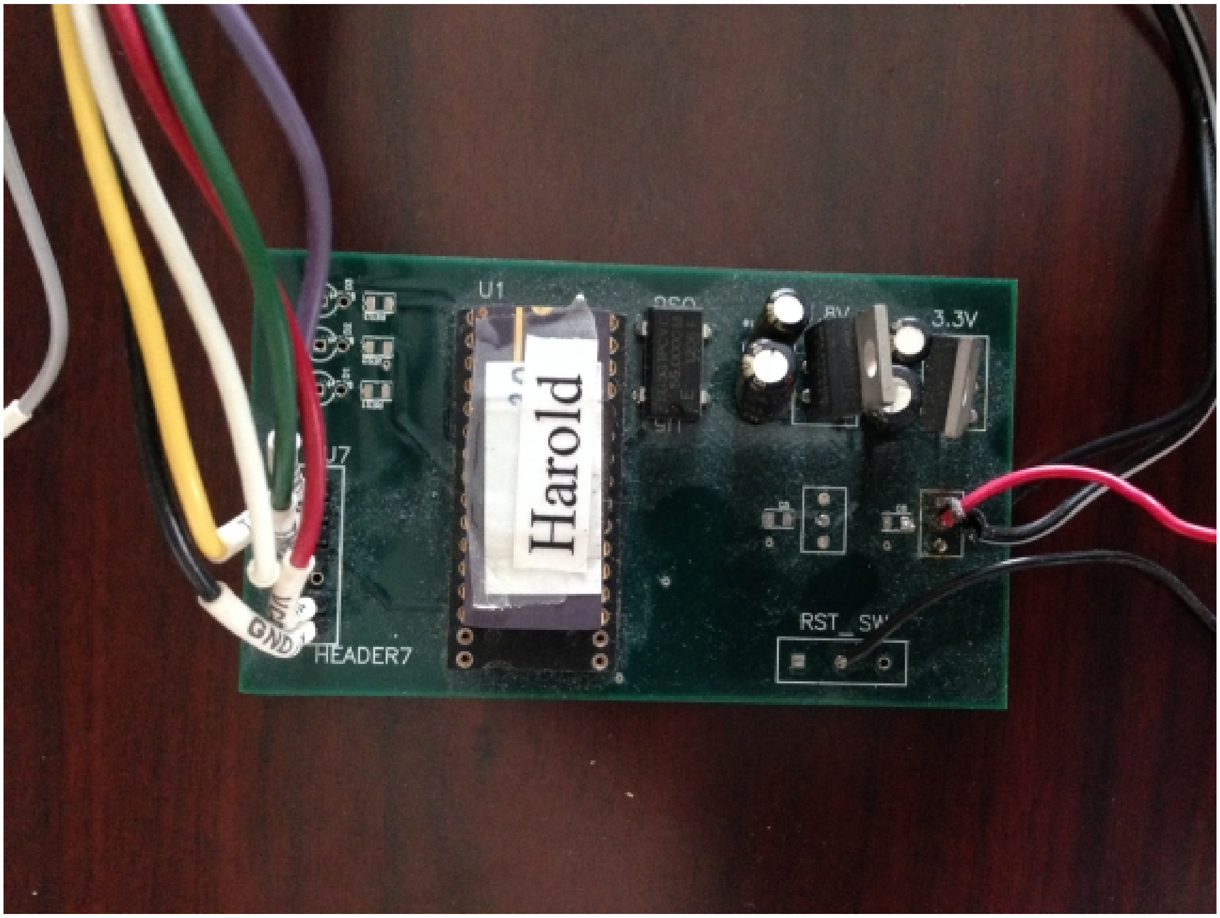
"Then, suddenly, you have a miniscule probability you're going to get the same 128-bit resolution for any given race," Devadas says.

When the tag is scanned, the reader will first identify the tag. Then, it will present the chip with a random challenge of the many that are stored in the database. If the response has 96 or more matching bits, it's considered authentic. Tags are attached to Canon camera packages, which consumers can scan using smartphones with near-field communication.

In 2002, Devadas and other MIT researchers delivered a seminal paper introducing silicon PUF technology at the Computer and Communications Security Conference, which coined the name and described the first integrated PUF circuit. This March, that paper earned an A. Richard Newton Technical Impact Award from the Institute of Electrical and Electronics Engineers and the Association for Computing Machinery—"which is a test of time for the concept and technology," Devadas says.

By 2004, Devadas and his students had developed a few dozen bulky, PUF-enabled circuits, labeling each with a human name, such as "Harold," "Cameron," and "Dennis." They stored the speed characteristics of each in a database on their computer; when a given circuit was scanned using a custom reader, its name would pop up on the screen.

This project earned Devadas a grant from the MIT Deshpande Center for Technological Innovation, and several government grants, which helped Verayo launch in its current Silicon Valley headquarters.



One of Devadas's early PUF-enabled circuits, labeled with the name “Harold." When this circuit was scanned with a custom reader, its name would pop up on a computer screen. Credit: Srini Devadas

Keeping volatile secrets

Although Verayo is focused on the consumer space, the technology has other uses, such as generating "volatile secret keys," Devadas says, which would only be revealed when activated by voltage.

Because PUF chips do not store such secrets, Devadas says, they need voltage to reveal their unique numeric identification—which could be stored as cryptographic keys. "When the chip powers up, there will be this 128-bit number that gets generated, but it doesn't exist when the chip is powered down," Devadas says. "If I don't have a way of pulling [the key] out, I won't know what it is."

This technology has advantages, Devadas says, over traditional nonvolatile data-storage devices, such as flash or erasable programmable read-only memory chips, which retain hackable data even when switched off. These nonvolatile chips are still difficult to break into, he adds, but not as difficult as PUF-enabled chips, which need to be inspected internally when the chip is powered on and the right challenges are applied.

"All of cryptography is based on something remaining secret," Devadas says. "PUFs are a way of generating those secrets in a more physically secure manner."

Attracting funding from the Department of Defense, this concept could help, for instance, ensure that drones don't connect with hacked servers, or that wearables don't share data with unauthorized servers.

Devadas says the PUF-technology market has seen significant growth in recent years, with other companies now developing in the space. But the competition doesn't discourage the PUF pioneer—in fact, Devadas is excited about the increased interest.

"It does feel like the world is coming around," he says. "And we're still here—that's the beauty of it."

More information: www.verayo.com/

*This story is republished courtesy of MIT News (*web.mit.edu/newsoffice/*), a popular site that covers news about MIT research, innovation and teaching.*

Provided by Massachusetts Institute of Technology

Citation: "Fingerprinting" chips to fight counterfeiting (2015, May 1) retrieved 26 April 2024 from https://phys.org/news/2015-05-fingerprinting-chips-counterfeiting.html