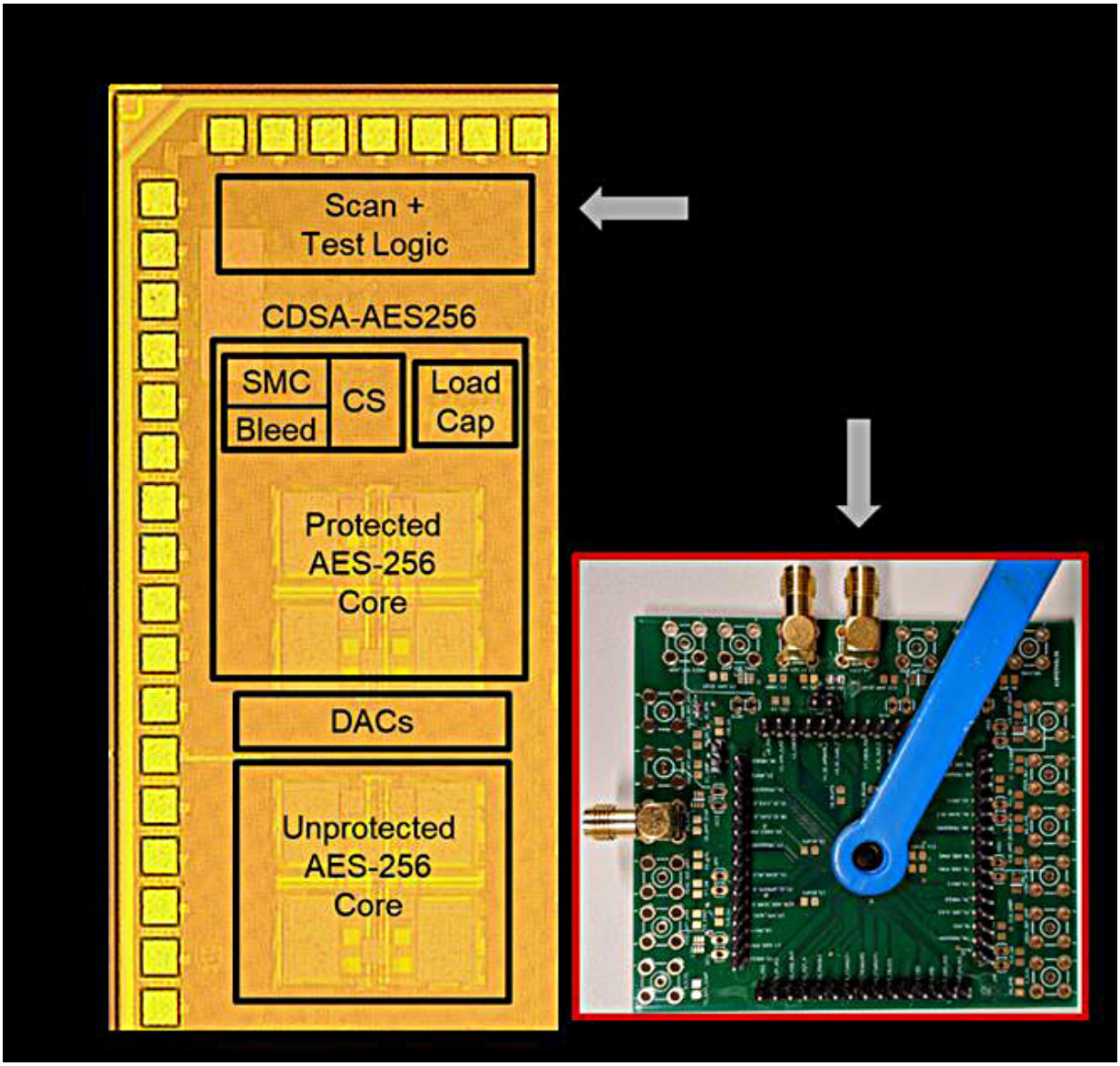
Mixed-signal hardware security thwarts powerful electromagnetic attacks

February 19 2020, by Chris Adam



Purdue University innovators created hardware technology to use mixed-signal

circuits to embed critical information to stop computer attacks. Credit: Shreyas Sen/Purdue University

Security of embedded devices is essential in today's internet-connected world. Security is typically guaranteed mathematically using a small secret key to encrypt the private messages.

When these computationally secure encryption algorithms are implemented on a physical hardware, they leak critical side-channel information in the form of power consumption or electromagnetic radiation. Now, Purdue University innovators have developed technology to kill the problem at the source itself—tackling physical-layer vulnerabilities with physical-layer solutions.

Recent attacks have shown that such side-channel attacks can happen in just a few minutes from a short distance away. Recently, these attacks were used in the counterfeiting of e-cigarette batteries by stealing the secret encryption keys from authentic batteries to gain market share.

"This leakage is inevitable as it is created due to the accelerating and decelerating electrons, which are at the core of today's digital circuits performing the encryption operations," said Debayan Das, a Ph.D. student in Purdue's College of Engineering. "Such attacks are becoming a significant threat to resource-constrained edge devices that use symmetric key encryption with a relatively static secret key like smart cards. Our technology has been shown to be 100 times more resilient to these attacks against Internet of Things devices than current solutions."

Das is a member of Purdue's SparcLab team, directed by Shreyas Sen, an assistant professor of electrical and computer engineering. The team developed technology to use mixed-signal circuits to embed the crypto

core within a signature attenuation hardware with lower-level metal routing, such that the critical signature is suppressed even before it reaches the higher-level metal layers and the supply pin. Das said this drastically reduces electromagnetic and power information leakage.

"Our technique basically makes an attack impractical in many situations," Das said. "Our protection mechanism is generic enough that it can be applied to any cryptographic engine to improve side-channel security."

A paper the team prepared in collaboration with Intel Corp. and the Georgia Institute of Technology will be presented this week at the International Solid-States Circuit Conference, the world's premier integrated circuit design conference.

Provided by Purdue University