Researchers demonstrate two security methods that efficiently protect analog-to-digital converters from powerful attacks

June 14 2022, by Adam Zewe

MIT researchers demonstrated that analog-to-digital converters in smart devices are vulnerable to power and electromagnetic side-channel attacks that hackers use to “eavesdrop” on devices and steal secret information. They developed two security strategies that effectively and efficiently block both types of attacks. Credit: MIT News

Researchers are pushing to outpace hackers and develop stronger protections that keep data safe from malicious agents who would steal information by eavesdropping on smart devices.

Much of the work done to prevent these "side-channel attacks" has focused on the vulnerability of digital processors. For instance, hackers can measure the electric current drawn by a smartwatch's processor and use it to reconstruct secret data being processed, such as a password.

Recently, MIT researchers published a paper in the *IEEE Journal of Solid-State Circuits*, which demonstrated that analog-to-digital converters in smart devices, which encode real-world signals from sensors into digital values that can be processed computationally, are susceptible to power side-channel attacks. A hacker could measure the power supply current of the analog-to-digital converter and use machine learning to accurately reconstruct output data.

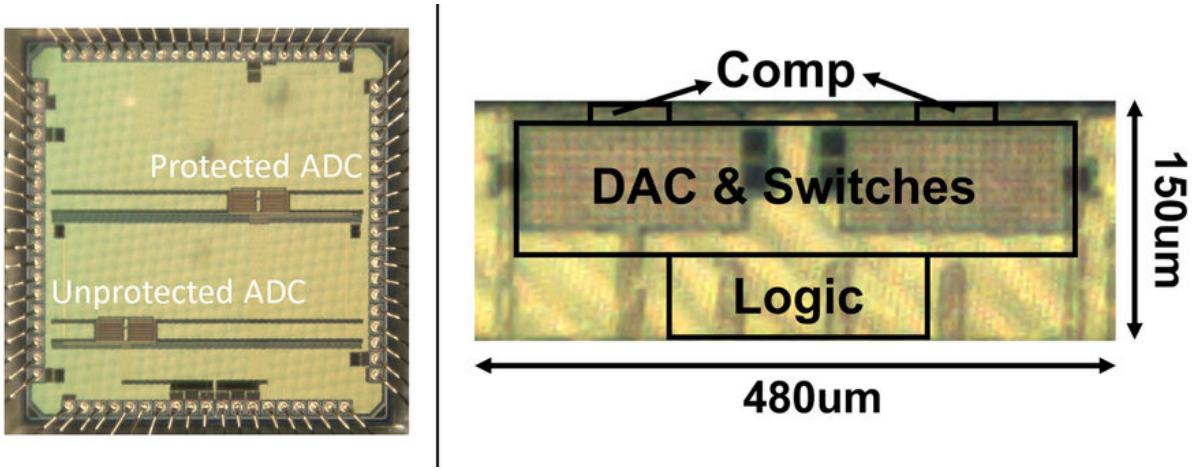
Now, in two new papers, researchers show that analog-to-digital converters are also susceptible to a stealthier form of side-channel attack, and describe techniques that effectively block both attacks. Their techniques are more efficient and less expensive than other security methods.

Minimizing power consumption and cost are critical factors for portable smart devices, says Hae-Seung Lee, the Advanced Television and Signal Processing Professor of Electrical Engineering, director of the Microsystems Technology Laboratories, and senior author of the most recent research paper.

"Side-channel attacks are always a cat and mouse game. If we hadn't done the work, the hackers most likely would have come up with these methods and used them to attack analog-to-digital converters, so we are preempting the action of the hackers," he adds.

Joining Lee on the paper is first-author and graduate student Ruicong Chen; graduate student Hanrui Wang; and Anantha Chandrakasan, dean of the MIT School of Engineering and the Vannevar Bush Professor of Electrical Engineering and Computer Science. The research will be presented at the IEEE Symposium on VLSI Circuits. A related paper, written by first-author and graduate student Maitreyi Ashok; Edlyn Levine, formerly with MITRE and now chief science officer at America's Frontier Fund; and senior author Chandrakasan, was recently presented at the IEEE Custom Integrated Circuits Conference.

The authors of the *IEEE Journal of Solid-State Circuits* paper are lead-author Taehoon Jeong, who was a graduate student at MIT and is now with Apple, Inc, Chandrakasan, and Lee, a senior author.



MIT researchers developed two security schemes that protect analog-to-digital converters (ADC) from power and electromagnetic side-channel attacks using randomization. On the left is a micrograph of an ADC that randomly splits the analog-to-digital conversion process into groups of unit increments and switches them at different times. On the right is a micrograph of an ADC that splits the chip into two halves, enabling it to select two random starting points for the conversion process while speeding up the conversion. Credit: Taehoon Jeong et al

A noninvasive attack

To conduct a power side-channel attack, a malicious agent typically solders a resistor onto the device's circuit board to measure its power usage. But an electromagnetic side-channel attack is noninvasive; the agent uses an electromagnetic probe that can monitor electric current without touching the device.

The researchers showed that an electromagnetic side-channel attack was just as effective as a power side-channel attack on an analog-to-digital converter, even when the probe was held 1 centimeter away from the chip. A hacker could use this attack to steal private data from an implantable medical device.

To thwart these attacks, the researchers added randomization to the ADC conversion process.

An ADC takes an unknown input voltage, perhaps from a biometric sensor, and converts it to a digital value. To do this, a common type of ADC sets a threshold in the center of its voltage range and uses a circuit called a comparator to compare the input voltage to the threshold. If the comparator decides the input is larger, the ADC sets a new threshold in the top half of the range and runs the comparator again.

This process continues until the unknown range becomes so small it can assign a digital value to the input.

The ADC typically sets thresholds using capacitors, which draw different amounts of electric current when they switch. An attacker can monitor the power supplies and use them to train a machine-learning model that reconstructs output data with surprising accuracy.

Randomizing the process

To prevent this, Ashok and her collaborators used a random number generator to decide when each capacitor switches. This randomization makes it much harder for an attacker to correlate power supplies with output data. Their technique also keeps the comparator running constantly, which prevents an attacker from determining when each stage of the conversion began and ended.

"The idea is to split up what would normally be a binary search process into smaller chunks where it becomes difficult to know what stage in the binary search process you are on. By introducing some randomness into the conversion, the leakage is independent from what the individual operations are," Ashok explains.

Chen and his collaborators developed an ADC that randomizes the starting point of the conversion process. This method uses two comparators and an algorithm to randomly set two thresholds instead of one, so there are millions of possible ways an ADC could arrive at a digital output. This makes it nearly impossible for an attacker to correlate a power supply waveform to a digital output.

Using two thresholds and splitting the chip into two halves not only allows random starting points, but it also removes any speed penalty, which enables it to run almost as fast as a standard ADC.

Both methods are resilient against power and electromagnetic side-channel attacks without hurting the performance of the ADC. Ashok's method only required 14 percent more chip area, while Chen's did not require any additional area. Both use much less power than other secure ADCs.

Each technique is tailored for a specific use. The scheme Ashok

developed is simple, which makes it well-suited for low-power applications like smart devices. Chen's technique, which is more complex, is designed for high-speed applications like video processing.

"For the past half-century of ADC research, people have focused on improving the power, performance, or area of the circuit. We've shown that it is also extremely important to consider the security side of ADCs. We have new dimensions for designers to consider," Chen says.

Now that they have shown the effectiveness of these methods, the researchers plan to use them to develop detection-driven chips. In these chips, protection would only turn on when the chip detects a side-channel attack, which could boost energy efficiency while maintaining security.

"To create secure low-power edge-devices, it is necessary to optimize every single component of the system. The notion of secure analog and mixed-signal circuits is a relatively new and important research direction. Our research shows it is possible to essentially with high accuracy infer the data at the output of analog-to-digital converters by leveraging advances in machine learning and fine-grained measurement techniques," Chandrakasan says. "Through optimized circuit methods such optimizing switching schemes, it is possible to create power and EM side-channel secure circuits, enabling fully secure systems. This is going to be critical in applications such as health care, where data privacy is critical."

More information: Taehoon Jeong et al, S2ADC: A 12-bit, 1.25MS/s Secure SAR ADC with Power Side-Channel Attack Resistance, *2020 IEEE Custom Integrated Circuits Conference (CICC)* (2020). DOI: 10.1109/CICC48029.2020.9075919