A Reverse-Engineering Assessment of a Secure Authenticator with PUF Technology

By Scott Jones, Managing Director, Embedded Security, Maxim Integrated

March 2018

maxim integrated™

Abstract

From fault injection to side-channel analysis and invasive techniques, cybercriminals continue to become more sophisticated in their attack methods that are applied to security ICs. With pervasive connectivity and the resulting exposure, hardware-based security provides the most effective solution for protecting the assets of embedded systems. The newest embedded security ICs feature the most advanced level of protection against invasive attacks currently available: the physically unclonable function (PUF). This paper provides the findings of a reverse-engineering study conducted by a third-party security lab to evaluate the security robustness of Maxim's secure authenticator with ChipDNA™ PUF technology.

Introduction

ChipDNA PUF technology protects against probing and reverse-engineering

A PUF is derived from the complex and variable physical and electrical properties of IC devices. Given that they're dependent upon random physical factors introduced during manufacturing that are unpredictable and uncontrollable, PUF circuits are virtually impossible to duplicate or clone. PUF technology natively generates a digital fingerprint for its associated IC. This fingerprint can then be used as a unique key, or secret, to support algorithms for authentication, identification, anti-counterfeiting, hardware-software binding, and encryption/decryption.

Maxim's **DS28E38 DeepCover® secure authenticator** is the first in the product line to feature the company's ChipDNA PUF technology. This PUF circuit relies on the naturally occurring random analog characteristics of fundamental MOSFET device structures to produce cryptographic keys. Through a patented approach, a unique key generated by each PUF circuit is guaranteed to be repeatable over temperature, voltage, and aging. The unique binary value isn't stored anywhere on the chip in non-volatile memory. It is simply generated when needed, and instantaneously erased when no longer in use. As such, there's no key for a cybercriminal to steal. If someone does try to attack a PUF-based device, with for example micro-probing or reverse-engineering methods, the attack would be thwarted due to the electrical characteristics of the PUF circuit being disturbed, which results in a modified and invalid PUF output.

In addition to ChipDNA PUF technology demonstrating excellent reliability over process, voltage, temperature, and aging, an evaluation of the PUF output to NIST-based randomness test suites[1] is successful with pass results. To determine the security robustness of the DS28E38-based PUF implementation, an external U.S.-based security lab attempted to reverse-engineer the chip, focusing in particular on the PUF circuitry and its associated digital circuits. The lab is an industry-recognized expert provider of reverse-engineering analysis of security ICs and other complex circuits. From this analysis, the lab assessed the difficulty of reverse-engineering the DS28E38, along with the possibility of compromising or cloning the circuit.

Evaluation Overview

The security lab provides this overview of its study: The design of the PUF is an array of cells which consists of a transistor-structure cell that is uniquely selected by digital circuitry. Once the cell is selected, it appears that the output analog value is compared against a known pre-selected value within the same array. The minor differences are compared and then converted from an analog to a digital value and stored within the digital circuitry. The single bit of data outputted from the security circuit arrives in the sea of logic gates, and no direct link between this register and any of the memory array was established during the reverse-engineering. The establishment of a direct link would be critical in the event that the

generated data could be directly read from a memory array and, therefore, read out or made into a deterministic value using backside laser probing.

The strength of this security circuit is derived from the small non-deterministic analog value differences that are sensed, measured, and compared in determining the "1" or "0" bit values. Utilizing these minor and sensitive analog differences makes it near impossible to clone the precise "physiology" of the chip and reproduce the results of each randomly selected cell. The minor process variation across the wafer, which translates into the randomness of the key generation, makes this an ideal PUF-generating circuit.

Adding to the strength of the circuit are the metal-plate shields that cover the security circuit array that generates the random bit. This is implemented using multiple metal layers, which are interconnected and connected to supplies. This makes delayering and focused ion beam (FIB) access to alter the cells very difficult without creating small variations. This makes physical attacks impossible given the extreme sensitivity of these circuits to leakage currents, or capacitive loading. In the same light, backside laser or scanning electron microscope (SEM)/FIB attacks would be difficult to carry out due to the interaction of the laser or electron beam-induced current (EBIC) with the silicon resulting in excessive charge carriers. These charge carriers would most likely upset and alter the PUF circuitry results, which again are derived from precise analog sources used to measure a delta in cell structures.

These points were highlighted by the security lab as DS28E38 security strengths:

- Security shields over PUF circuit
- Unique key-generation circuit
- Circuit easily upset with physical delayering or FIB attacks
- Circuit easily upset with back-side laser attacks
- Digital circuit has complex routing between library cells, utilizing all metal layers as interconnects, making net list extraction prone to errors

Reverse-Engineering Study Conclusion

The security lab provides this conclusion following its evaluation: After reverse-engineering efforts on the PUF circuit and some of the associated digital circuits, the security technology implemented by Maxim was determined to be highly effective and resistant against physical reverse-engineering attacks.

In particular (on this point is) the analog circuit, which is a uniquely designed PUF technology that generates data bits based on minor process variations across a single die. The design and implementation of the circuit makes it very robust against both physical and electrical attacks, and in our experience, this is one of the most effective PUF designs against circuit cloning and passive and active attacks in attempts to make the resultant key deterministic.

"This is one of the most effective PUF designs against circuit cloning and passive and active attacks..."

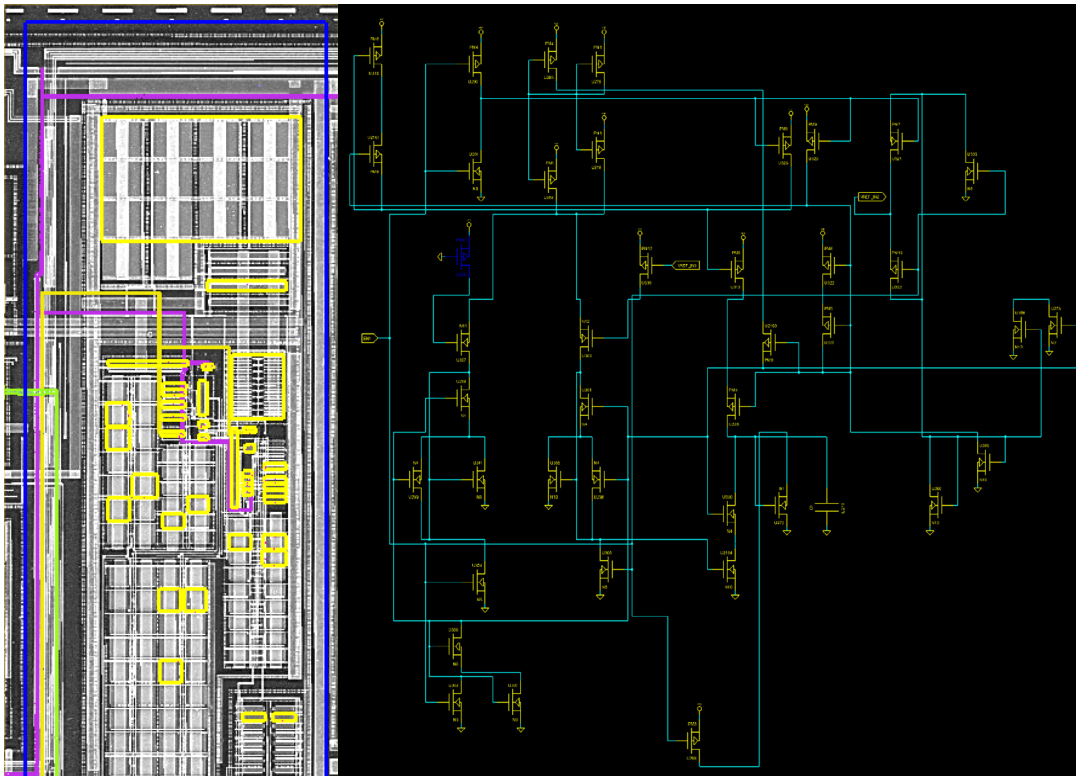

Figure 1. These images from the third-party reverse-engineering study of the DS28E38 show the layout and schematic of the circuit

Extraction of the digital circuits was done to a lesser extent where approximately 60% of the library cells were identified and laid down. It became very apparent that the digital circuit layout was done using all layers to implement a complex routing scheme in between the library cells. This was done most likely to make the circuit extraction difficult and prone to error. In fact, the lab ran into these very problems where multiple adjacent busses were observed to be shorted due to minor deprocessing problems, and the amount of GDS II correction required became an enormous problem which eventually limited the number of digital circuits that were extracted.

Growing Portfolio of ChipDNA PUF Security ICs

Maxim continues to expand its portfolio of DeepCover embedded security ICs with ChipDNA PUF technology. Another ChipDNA secure authenticator is the **DS28E50**, which also provides FIPS202-compliant secure hash algorithm (SHA-3) challenge and response authentication. On the secure microcontroller side, the **MAX32520** integrates ChipDNA PUF technology along with secure boot to protect IoT applications. The MAX32520 is based on an Arm® Cortex®-M4 processor and provides a FIPS/NIST-compliant True Random Number Generator along with environmental and tamper detection circuitry for enhanced system-level security.

Summary

As cybercriminals become more persistent and sophisticated, embedded security technologies provide robust protection against their attacks. PUF technology represents the most advanced level of cryptography currently available in the newest embedded security ICs. This paper covered the reverse-engineering evaluation conducted by a third party on Maxim's DS28E38 secure authenticator with ChipDNA PUF technology. As the study found, the IC has demonstrated its ability to reliably protect against invasive attacks.

Learn More

For more information about ChipDNA PUF circuitry, including access to the white paper, "How Unclonable, Turnkey Embedded Security Protects Designs from the Ground Up," visit: www.maximintegrated.com/chipdna

Sources

[1] https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software

Learn more

For more information, visit:
www.maximintegrated.com