UNIVERSITY OF MINNESOTA
Driven to Discover℠

Robust Device Authentication for Integrated Circuits

Technology ID
20160192

Category
Engineering & Physical Sciences/Instrumentation, Sensors & Controls
Software & IT/Algorithms
Software & IT/Cyber Security

View online

Physical Unclonable Function Authentication with Self Correction

A lightweight, secure and reliable method authenticates chip-unique signatures from integrated circuits to address electronics counterfeiting. The method, based on Physical Unclonable Function (PUF) authentication, uses a key (selected for authentication purposes) with a two-level finite-state machine (FSM) to correct erroneous bits in the authentication process that can be generated by age, temperature, voltage, and various environmental variations. The technology includes a FSM and a physical structure that provides a response to a challenge. However, before the physical structure is ever provided with the challenge, the response to the challenge is unpredictable. The FSM moves from an initial state to an intermediate state when it receives a response from the physical structure, and moves from the intermediate state to a final state when it receives a key. The final state indicates whether the physical structure is a counterfeit physical structure.

More Efficient Error Correcting Code

PUFs extract chip-unique signatures from integrated circuits (ICs) by exploiting uncontrollable randomness due to manufacturing process variations. These signatures can then be used for many hardware security applications such as authentication, anti-counterfeiting, IC metering, signature generation and obfuscation. However, most of these applications require error correcting methods to produce consistent PUF responses across different environmental conditions. Sometimes, due to environmental variations, PUF signatures are erroneous, and while an error correction coder can correct these errors, it requires a large increase in hardware. This technology generates the correct signature, without requiring any additional error correction circuitry, by associating a key with the signature during the design time. Experimental results show that this self-correcting two-level FSM approach costs significantly less than commonly used error correcting codes. In addition, the new method consumes 2 to 10 times less area and 20 to 100 times less power than previous technology.

BENEFITS AND FEATURES:

- Authenticates chip-unique signatures from integrated circuits
- Physical Unclonable Function (PUF) authentication
- Self-correcting two-level finite-state machine (FSM) approach associates a key with the signature
- Corrects erroneous bits in authentication process
- Physical structure provides a response to a challenge
- Lightweight, secure and reliable
- Significantly lower cost than commonly used error correcting codes
- Consumes 2 to 10 times less area
- Uses 20 to 100 times less power

APPLICATIONS:

- Integrated circuit chips
- Integrated devices
- Anti-counterfeiting measures

Phase of Development - Prototype development

Researchers

Keshab K. Parhi, PhD
Professor, Electrical and Computer Engineering
External Link (ece.umn.edu)
Chris H. Kim, PhD
Professor, Electrical and Computer Engineering
External Link (ece.umn.edu)
Yingjie Lao
Electrical and Computer Engineering

Publications

Reliable PUF-Based Local Authentication With Self-Correction
IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Volume: 36, Issue: 2, Feb. 2017

Available for Non-exclusive Licensing

The University relies on industry partners to scale up technologies to large enough production capacity for commercial purposes. The license is available for this technology and would be for the sale, manufacture or use of products claimed by the issued patents. Please contact us to share your business needs and technical interest in this technology and if you are interested in licensing the technology for further research and development.