Reconfigurable Physically Unclonable Function (PUF) Based Security

Tech ID: 28868 / UC Case 2018-088-0

BACKGROUND

The ubiquity of internet communication needs no introduction, and it follows that the security of the world's 4.5 billion internet users is critical. Conventional cryptographic and "secret key" approaches are vulnerable to physical and side-channeling attacks, making them unreliable security measures. Therefore, a need exists for a more dependable and impenetrable form of security

DESCRIPTION

Researchers at the University of California, Santa Barbara have developed an architecture for hardware-intrinsic security primitives that use random process-induced variations in subthreshold slope, leakage and tuning accuracy of Flash memories to build a reliable Physically Unclonable Function (PUF). This architecture allows for PUF circuits with fast and low power operation and low chip-area. The simple and low-cost design, small footprint, CMOS integration compatibility, and reconfigurability make this technology superior to existing PUF hardware and pitch-perfect for security applications.

A prototype of these RX-PUFs features enhanced functional performance with a measured bit error rate of 0.7% at room temperature and less than or equal to 5.3% at 100° C, without error correction methods. These hardware solutions have wide-ranging applications including IC identification, secure channel communication, and data encryption. In any case, none would require "key" storage in auxiliary memory, making it virtually impenetrable from attack.

ADVANTAGES

- Fast & low power operation (10 ns / 20 uW per bit)
- CMOS compatible
- Random & unpredictable primitives
- Low chip-area overhead (scalable to 28nm+)
- Programmable
- Enhanced resilience against attack (including machine learning attacks)
- Reconfigurable
- Excellent physical characteristics (1600 F^2/bit density and up to 41 fJ/bit energy efficiency)

APPLICATIONS

CONTACT

Pasquale S. Ferrari
ferrari@tia.ucsb.edu
tel: .

INVENTORS

- Ahmadabadi, Hussein Nili
- Fahimi, Zahra
- Mahmoodi, Mohammad Reza
- Strukov, Dmitri B.

OTHER INFORMATION

KEYWORDS

Physically unclonable function, PUF, security, cryptographic, security primitives, RRAM, CMOS, semiconductors, IC identification, data encryption, indtelecom, indansens, indmicroelec, indsoftw

CATEGORIZED AS

- **Computer**
  - Security
- **Security and Defense**
  - Cyber security
- **Semiconductors**
  - Other

RELATED CASES

2018-088-0

- Semiconductors
- IC identification
- Secure channel communication
- Anti-counterfeiting
- Military equipment
- “Key-less” Data encryption
- Data storage

RELATED MATERIALS

- Programmable Hardware-Intrinsic Security Primitives Enabled by Analogue State and Nonlinear Conductance Variations in Integrated Memristors - 02/01/2018
- Highly-Secure Physically Unclonable Cryptographic Primitives Using Nonlinear Conductance and Analog State Tuning in Memristive Crossbar Arrays - 11/01/2016

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	10,812,084	10/20/2020	2018-088

University of California, Santa Barbara
Office of Technology & Industry Alliances
342 Lagoon Road, ,Santa Barbara,CA 93106-2055 |
www.tia.ucsb.edu
Tel: 805-893-2073 | Fax: 805.893.5236 | padilla@tia.ucsb.edu