Reconfigurable Physically Unclonable Function (PUF) Based Security
Tech ID: 28868 / UC Case 2018-088-0

BRIEF DESCRIPTION
A platform for highly secure and reconfigurable hardware-intrinsic security primitives, physically unclonable function (PUF), based on the emergent analog RRAM crossbar technology.

BACKGROUND
The ever-expanding world of the internet and information technology has led to an increase of interconnected networks and sharing of valuable information online. As the amount of information disseminated online grows so does the need for a protected and safe way to store this information. 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 designed an architecture (RX-PUF) for highly secure and reconfigurable hardware-intrinsic security primitives, physically unclonable function (PUF), based on the emergent analog RRAM crossbar technology and analog Flash memory blocks. RX-PUF takes advantage of unique RRAM properties, such as I-V nonlinearity, and its device-to-device variations and tenability. These primitives have near ideal diffuseness, uniformity, and uniqueness. Its simple and low-cost design, small footprint, CMOS integration compatibility, and instance reconfigurability make this technology superior to other PUF hardware and highly suitable for security applications. This architecture, based on matured integrated floating gate technology offers low-cost CMOS-compatible solutions. With flash-based memory arrays already in production and their anticipated application in computational engines, the reliable, embeddable security apparatus will be of great value. A prototype of these RX-PUFs feature enhanced functional performance with a measured bit error rate of 0.7% at RT 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 without the need of “key” storage in auxiliary memory, making it seemingly impenetrable from attack.

ADVANTAGES
▶ Programmable
▶ Enhanced resilience against attack
▶ Can be easily integrated into existing devices
▶ Excellent physical characteristics (1600 F/²/ bit density and up to 41 fJ/bit energy efficiency)
▶ Extremely high resilience of RX-PUF against machine learning attacks

APPLICATIONS
▶ Semiconductors
▶ IC identification
▶ Secure channel communication
▶ Data encryption
▶ Anti-counterfeiting
▶ Military equipment

PATENT STATUS

CONTACT
Mary Raven
raven@tia.ucsb.edu
tel: View Phone Number.

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
ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- Versatile Stochastic Dot-Product Circuit
- Time-Domain Mixed-Signal Vector-By-Matrix Multiplier
- Ultra-Compact Energy-Efficient Neurocomputing Platform