Physically Unclonable Functions
Using Spintronic Domain Wall Memory

Researchers at the University of South Florida have developed methods and an apparatus to build Physically Unclonable Functions (PUFs) using Spintronic Domain Wall Memory (DWM).

The manufacturing of the present day Integrated Circuits (IC) are mostly outsourced to external companies and this business model is exposed to tampering and IC Cloning. Not only does IC Cloning breach the Intellectual Property (IP), but it also siphons off the economic benefits of the product. Traditionally, unique keys are generated by the ICs for important applications such as IP security, counter-plagiarism, etc.; however, adversaries can decode secret keys through Reverse Engineering (RE). The duplicated chip with the RE obtained key cannot be distinguished from a genuine chip. In order to address these issues an auxiliary circuit (i.e., PUF) is incorporated in authentic chips. PUFs are designed to exploit the physical properties of chips (e.g., process) to generate unique identification keys.

USF inventors have developed a novel low-power consumption technique to effectively generate unique identification keys using Spintronic Domain Wall Memory based PUFs. This technology leverages the nonlinear dynamics of domain wall memory in the physical magnetic system for its application in hardware security and authentication.

**ADVANTAGES:**
- Operates within a wide range of voltages
- Integrates excellent sources of entropy
- Low power consumption
- Attack resistant

**A Low Over-head, Memory Based Security Primitive**

Power vs Number of Heads for DW Memory-PUF. More than 10X Power Saving with DWM PUFs.

Tech ID # 14A064  US Patent # 9,859,018