Physically Unclonable Function (PUF) Solution for ARC EM Processors

Highlights

- Secure and reliable PUF-based crypto key generation
- Physical fingerprint and entropy extraction from embedded SRAM
- Pure firmware implementation leveraging Synopsys SecureShield technology
- Optional high-performance implementation with Synopsys ARC CryptoPack acceleration
- Chip identification based on Fuzzy Identifier

Target Applications

- IoT
- Wearables
- Mobile
- Microcontrollers
- Sensors

Technology

- TSMC, UMC, Intel, Samsung
- 180nm, 150nm, 130nm, 90nm, 65nm, 45nm, 40nm, 28nm, 16nm, 14nm

PUF for Integrated Circuits

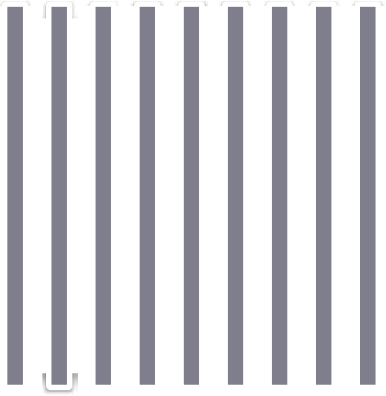
Tiny variations in a semiconductor manufacturing process make each transistor and each piece of silicon unique. These variations are random and uncontrollable, so it is impossible to make an exact clone of an integrated circuit (IC), hence we refer to this as a Physically Unclonable Function or PUF. These variations can be amplified and measured with standard embedded Static Random-Access Memory (SRAM) cells and the startup behavior of on chip SRAM results in a unique pattern that is analogous to a fingerprint for the IC.

Authentication with the PUF key

Cryptographic authentication of a chip is done with a secret key that is extracted from the SRAM PUF. This extraction is done with Intrinsic-ID's Quiddikey IP. Quiddikey guarantees the entropy of the key as well as a correct and secure key reconstruction under all circumstances. In contrast with the conventional approach, the PUF key is extracted from the chip and not externally programmed. It is linked to the chip's physical characteristics and inherently protected against cloning and tampering.

Detailed Operation of Quiddikey

During the key reconstruction phase, Quiddikey receives the Activation Code (AC) and reads the SRAM startup pattern. The AC includes helper data to enable Quiddikey to recreate the PUF key. It then receives a Key Code (KC), which is effectively an encrypted or wrapped user key. Quiddikey reconstructs the user key and provides this key to the host system.



Synopsys, Inc. • **690 East Middlefield Road** •

02/05/16.TT_CS6880_ARC2016_Intrinsic_PO.