SYNOPSYS®
Silicon to Software™

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.

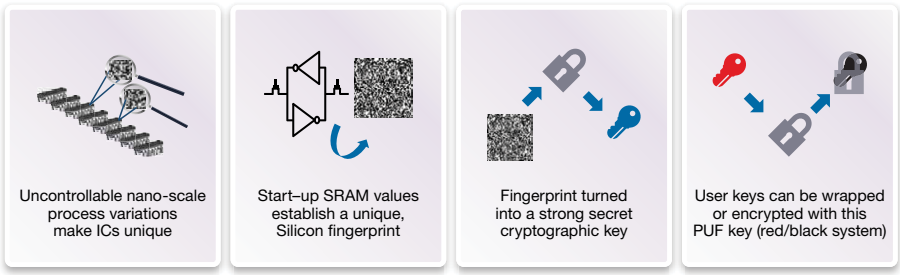

Figure 1. Flow of PUF technology used for secure key management

Physically Unclonable Function Solution for ARC EM Processors

The Physically Unclonable Function (PUF) solution from Intrinsic-ID is available for DesignWare® ARC® EM Processors and enables designers to extract a unique device fingerprint from standard embedded SRAM. This fingerprint can be used as a device identifier or as a cryptographic key. In the latter case, it effectively creates a secure key vault without the need to add non-volatile memory (NVM) or a dedicated security core. In combination with ARC EM Processor security options such as the Enhanced Security Package and CryptoPack, the PUF solution provides a high-performance, low-power security engine for protecting low-power IoT edge nodes such as wearables or smart home devices.

Identification with Fuzzy-ID

The startup pattern from an SRAM PUF can be used to uniquely identify a chip. Some of the bits in the pattern are unstable, so the matching has to be done using software known as the Fuzzy Identifier algorithm. This algorithm converts the unique but variable fuzzy identifier into a unique, collision-free fixed identifier comparable to a chip Identifier like the Electronic Chip ID (ECID).

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.

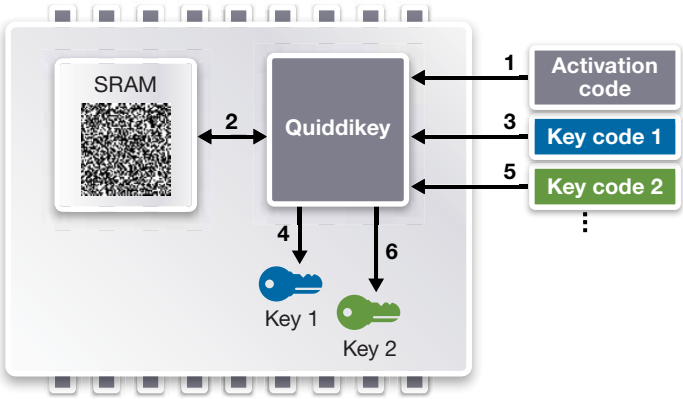

Figure 2. Generation of an activation code during enrollment

AC and KC are non-sensitive i.e., they contain no information about the keys or the PUF itself and can be stored off-chip or remotely. The AC and the PUF key are established during the enrollment phase. This phase typically takes place only once, usually during device manufacturing, device testing or at first use. The KC is established during a key programming phase where Quiddikey-Flex converts the plain text user key into a wrapped key code.

When combined with cryptographic algorithms in hardware or firmware, this can become a fully self-contained root of trust or secure element.

Data Authentication and Encryption

In most IoT applications, remote endpoints send data to a central hub. It is critical to protect both the integrity and the privacy of this data. To protect the integrity of the data and ensure that it cannot be tampered with, the data should be protected with a Message Authentication Code (MAC). Data can be encrypted with AES 256, for example, to ensure privacy and confidentiality.

The encryption and authentication algorithms can use the cryptographic keys generated by Quiddikey. This eliminates the need to store any of the keys in NVM where they could potentially be unsafe.

If no NVM is available to store the AC and KC, they can be stored remotely. With the Fuzzy Identifier as an index, they can be retrieved from the remote server. As AC and KC are non-sensitive, this is an inherently secure approach.

Performance

The PUF algorithms are only required after power-up. They can be further accelerated using Synopsys' ARC CryptoPack hardware extensions. The authentication and encryption of data can also be executed by the ARC EM core with CryptoPack to maximize performance and minimize power consumption.

Implementation

The PUF is based on standard SRAM cells (1 kbyte minimum). The Quiddikey PUF logic, as well as the authentication and encryption, are implemented in firmware leveraging Synopsys SecureShield™ technology and both can be enhanced with the CryptoPack option.

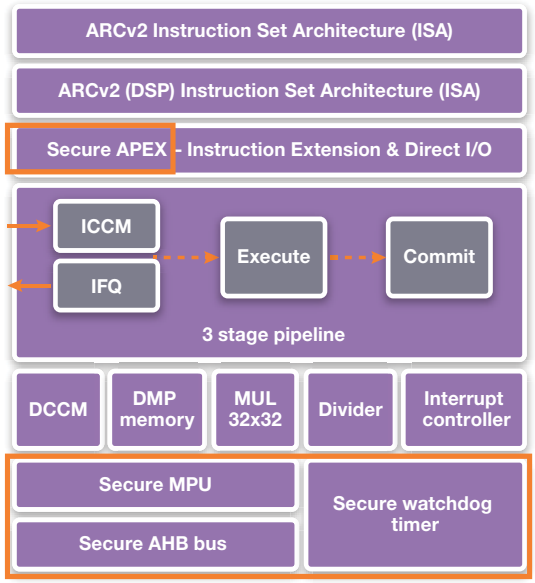

Figure 3. Enhanced Security Package on ARC EM Processor

Since the Quiddikey implementation is firmware, it requires protection. SecureShield provides a trusted execution environment for the firmware, with instruction and data encryption, and isolation from other software running on the ARC EM processor using the secure MPU.

The optional Fuzzy Identifier algorithm is software that runs on a server or Cloud system and converts a fuzzy or noisy PUF response into a fixed identifier. This way any chip can be identified without the need for storing or programming an identifier or serial number.

Testing, compliance, and quality

The PUF is based on Intrinsic-ID's SRAM PUF technology, Quiddikey, and has undergone rigorous testing:

- Wide range of technology nodes (180nm, 150nm, 130nm, 90nm, 65nm, 45nm, 40nm, 28nm, 16nm, 14nm)
- Reliability testing for temperature (-40°C to +125°C), aging (25 years), voltage supply (+/- 20%), EMC, humidity

About Intrinsic-ID

Intrinsic-ID is a world leader in the field of Cyber Physical Security Systems as a provider of "Physical Unclonable Functions" (PUF). Using patented PUF technology, secret keys and identifiers are reliably extracted from the physical properties of chips. Intrinsic-ID's wide range of security solutions serve the following markets: Embedded systems, IoT, Identification, automotive, communications, content distribution, pay TV, government and defense. www.intrinsic-id.com

About DesignWare IP

Synopsys is a leading provider of high-quality, silicon-proven IP solutions for SoC designs. The broad DesignWare IP portfolio includes logic libraries, embedded memories, embedded test, analog IP, wired interface IP, wireless interface IP, security IP, embedded processors, and subsystems. To accelerate prototyping, software development and integration of IP into SoCs, Synopsys' IP Accelerated initiative offers IP Prototyping Kits, IP Virtual Development Kits and IP subsystems. Synopsys' extensive investment in IP quality, comprehensive technical support and robust IP development methodology enables designers to reduce integration risk and accelerate time-to-market.

For more information on DesignWare IP, visit http://www.synopsys.com/designware. Follow us on Twitter at http://twitter.com/designware_ip.