Secure the Connected World

PUFsecurity

an eMemory Company

PUFsecurity leveraged NeoPUF's physical unclonable technology from our parent company, eMemory, and developed a series of security solutions that combine both digital and analog capabilities. We are continuously creating hardware security functions including:

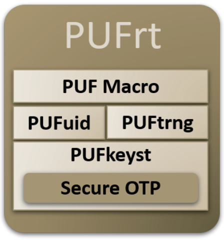
- Identity recognition (UID)
- True random number generator (tRNG)
- Key generation (key derivation function / key wrapping)
- Secure storage of sensitive information and keys

With these requirements in mind, we developed integrated security solutions including standard solution PUFrt, premium solution PUFiot, and high-end solution PUFse.

In the field of IoT security solutions, PUFsecurity provides cost-effective products and leverages over 43 process platform from eMemory's foundry partners. As a result, we offer a competitive advantage and are confident in promoting our PUF-based security products as the best choice for embedded hardware security solutions.

pufsecurity.com | info@pufsecurity.com | +886 3-560-1010 |
8F, No. 5, Tai-Yuan 1st St., Jhubei City, Hsinchu County, 30288, Taiwan

Uncompromised Security Solutions

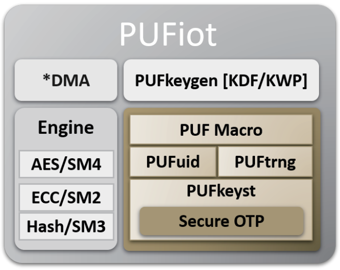


Standard Solution: PUFrt (Hardware Root of Trust)

- Foundation of trust and security for chip systems (UID+tRNG+Secure OTP)
- Offers 1024-bit identification code with PUF and tRNG (NIST SP 800-90B/800-22)
- PUFtrng with high-quality entropy, short initial time and low-power consumption
- PUF-based 4096-bit secure storage space

Feature Highlights

Fast & low-power tRNG *Reliable chip ID* *Advanced OTP read / write protection*

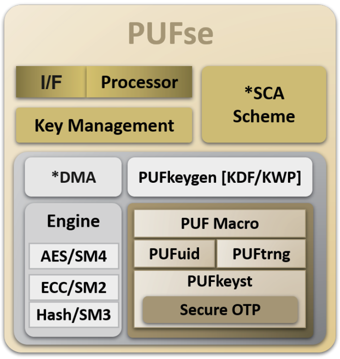


Premium Solution: PUFiot (IoT Security)

- Supports NIST-standard key management functions (key derivation and wrapping)
- Hash algorithm (DMA) and elliptic curve passwords for IoT security needs
- Available for general bus protocols such as AXI/AMBA
- Meets Chinese Standard Public Algorithms SM2, SM3, SM4 issued by OSCCA
- Supports secure boot and firmware protection

Feature Highlights

PUFrt integrated *OSCCA compliance* *KDF / KWP NIST compliance* *BUS & DMA support*

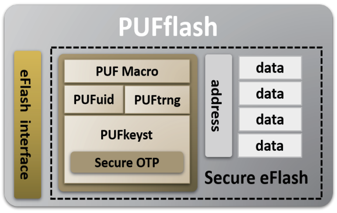


High-end solution: PUFse (secure element)

- Security computing + asset management + key storage + permission control
- A comprehensive solution of secure boot
- Supports firmware protection and online update (OTA)
- A complete solution for both digital and hybrids
- Achieves security and autonomy with efficient integration

Feature Highlights

PUFiot integrated *OTA support* *Secure boot* *Side channel attack resistant*



Secure Embedded Flash: PUFflash

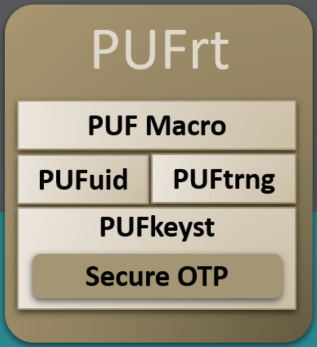
- Meets MCU microcontroller application scenarios and cost
- Enables secure data read / write through embedded PUFrt core
- Achieves address obfuscation and data masking for data writing in an easy way

Feature Highlights

Secure data storage *No performance side-effect* *No extra integration burden*

https://www.pufsecurity.com/solution

PUFrt —



PUFrt

PUF Macro

PUFuid

PUFtrng

PUFkeyst

Secure OTP

Standard Solution

When thinking about the fundamental and essential security requirements of SoC, there are three questions that always rack engineers' brains:

- How to effectively have a unique ID for production identity management?
- How to create an output of random numbers to ensure key generation randomness for sensitive data encryption/decryption?
- How to securely save Keys with physical tempering prevention?

Features

PUFrt is designed for solving these basic but imperative concerns. It's name comes from the abbreviation of PUF-based root of trust.

It is composed of PUFsecurity's PUF-based products including PUFuid, PUFtrng and PUFkeyst with features as follows:

- PUFuid : Easy and robust ID generation for production management
- PUFtrng : High quality static entropy with superb short initial time and low power consumption
- PUFkeyst : Secure key storage with built-in 4k-bits OTP and logic designs of - PUFtrng and PUF values

Application

PUFrt is a PUF-based hardware security root of trust and suitable for

- Low-weight IoT device
- Power-sensitive IoT device
- Basis of hardware-based root of trust

Security is abstract and difficult to most SoC designers but PUFrt is user-friendly and its uncompromising performance makes it worthy to equip in each SoC.

https://www.pufsecurity.com/pufrt