PUFsecurity

PUFef – Embedded Flash Protection

Datasheet

June 2022

Description

PUFef is an embedded flash with PUFsecurity's Hardware Root of Trust IP, PUFrt. It is an ideal replacement for systems with existing embedded Non-Volatile Memory solutions that require security upgrades to their eFlash. PUFef offers comprehensive embedded flash protection that can be seamlessly integrated.

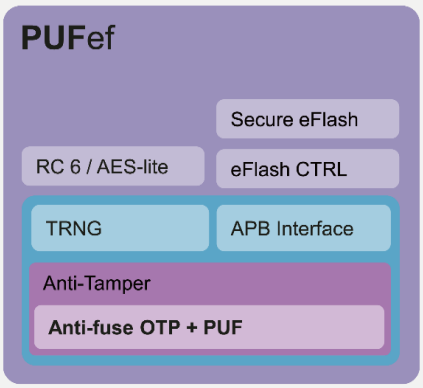
With real-time encryption/decryption based on the unique randomness built into each on-board PUF, PUFef supports execution in place (XIP) while offering secure data-at-rest protection for sensitive code and data. In addition, an optional error correction code (ECC) can also be implemented with the embedded Flash, further guaranteeing data stability over the system's lifetime.

PUFef includes a secure embedded flash unit (EFU) and PUFrt as the Hardware Root of Trust. The secure Embedded Flash is comprised of two regions; a clear region and a scrambled region. In the clear region, the clear data (not scrambled) is stored; the scrambled region provides data-scrambling and address-scrambling. The address scrambling means the data is stored in the slot indexed by the scrambled address.

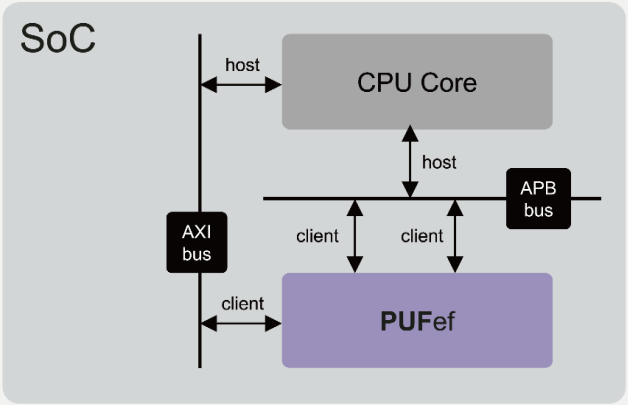
For data scrambling, the 32-bit data is scrambled before it is stored, and the stored data is descrambled before it is transferred to the bus. The scramble keys of the data scrambling and the address scrambling relate to the address of the slot and a 256-bit PUF (Physical-Unclonable-Function) secrets provided by PUFrt. It means the scramble keys of each device are unique.

A standard APB slave control module allows for easy drop-in integration of PUFef for systems that already support ARM's peripheral bus protocol. By unifying both PUFrt and Flash under the APB, system integrators can work with a familiar interface to execute the various RoT and embedded Flash functions of PUFef

Embedded Flash Protection



Suggested Integration



Features

PUFef

- Root of Trust (PUFrt) and eFlash unit (EFU)
- 2 APB control interfaces with secure/non-secure access privilege (accessing PUFrt and erasing EFU).
- The AXI interfaces for reading/programming EFU
- Hard Macro (PUF+OTP+eFlash) in GDS and Soft IP in RTL
- General code Storage XIP capability and data-at-rest protection
- Default EFU density: Clear region: 2^{10} x 32 bits, Scrambled region: 2^{17} x 32 bits

PUFrt

- Four 256-bit hardware PUF fingerprint that could be used as a unique private key, UID, or root key
- 8k-bits mass production OTP with built-in instant hardware encryption (customization available)
- Comprehensive anti-tamper designs in physical and RTL
- High-quality true random number generator
- Built-in PUF health check
- Boot code storage and OTA updates

Deliverables

- Datasheet
- Release Notes
- Integration Guidelines
- Timing .lib File
- LEF
- GDS Phantom File
- Verilog HDL File (Behavior Model)
- Verilog HDL File (FPGA)
- Application Note
- Reference Scripts
- Hard Macro Release Note
- Test Methodology
- Testbench

Details

Process Availability

- Available across worldwide foundries, with condinual development in new process nodes

Security Features

- Riscure certified anti-tamper design
- Resistant to physical attacks, including decapsulation, microscope imaging, probing, reverse engineering, etc.
- Data encryption and address scrambling for eFlash data protection

Controller/Interface

- Standard APB Interface
- Standard AXI Interface
- Secure OTP Wrapper (Factory test, user, Read/Write, Read-Only, and Non-accessible modes)

Emedded Flash Unit

- Clear region: 2^{10} x 32 bits for configuration; customization available
- Scramble region: 2^{17} x 32 bits for secure storage; customization available
- APB interface for clear region access and erase verification
- AXI interface for secure access to the scramble region
- Controller for eFlash testmode entry and testmode protection

PUF-based Key Storage

- Built-in 8kbits OTP; customization available
- Dummy insertion read based on entropy from TRNG
- Scrambler based on the PUF value ensures the key is stored securely and cannot be read out directly
- Unique scramble value per chip, making the stored information in each chip different from each other
- The value stored cannot be changed and deleted

PUF-based TRNG

- Ultra-fast initialization / stabilization (<100us)
- High-speed throughput (> 160 Mbits/sec)
- Ultra-low power consumption (< 0.38 pJ/bit)
- Compliant with NIST SP800-22 and NIST SP800-90B with IID/restart test
- NIST SP800-90A DRBG for >1Gbps random number generation available as optional accessory

PUF-based Unique ID

- To provide Ideal minimum entropy (1)
- Unpredictable randomness and uniqueness for UID with 50% Hamming weight and Hamming distance
- On-demand keys for on-chip secret and off-chip ID generation
- Optimal reliability with lifetime zero Bit-Error-Rate (BER)
- Robustness of working under different circumstances (Temp: -40~175°C)

PUFsecurity Corporation

8F, No. 5, Tai-Yuan 1st St., Jhubei City,
Hsinchu County, 302082, Taiwan
Tel: +886-3-560-1168

Please visit our website for further information or to download and try our IPs

https://www.pufsecurity.com/ip-go