PUFsecurity

PUFrt - Hardware Root of Trust

Datasheet

October 2023

Description

PUFrt is a Hardware Root of Trust (HRoT) offering the essential features necessary for establishing a trusted foundation from which all security operations, such as secure boot, can be based.

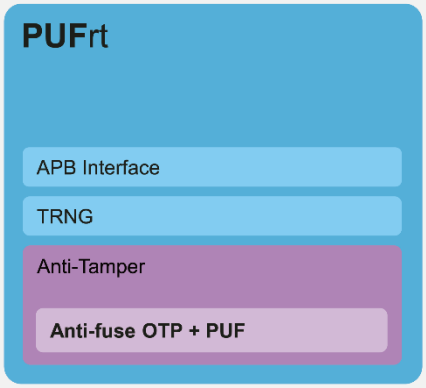
This Riscure certified IP offers the flexibility for users to add only the cryptographic engines that their designs need and comes with a well-designed anti-tamper shell against attacks. PUFrt can be integrated into a wide variety of systems, from a lightweight hardware security key to a full-functioning Security Coprocessor.

PUFrt provides a foundation of trust and security for the chip system. It contains a 1024-bit physical unclonable function (PUF), and a true random number generator (TRNG) that complies with the NIST SP800-90B/SP-800-22 standard specifications. These features aid in the encryption/decryption requirements of sensitive information and data, achieving a higher level of data security protection. Furthermore, a secure storage space is provided for customer use to keep private keys and sensitive information safe, based on eMemory's NeoFuse OTP with additional protections for even greater resistance to physical attacks.

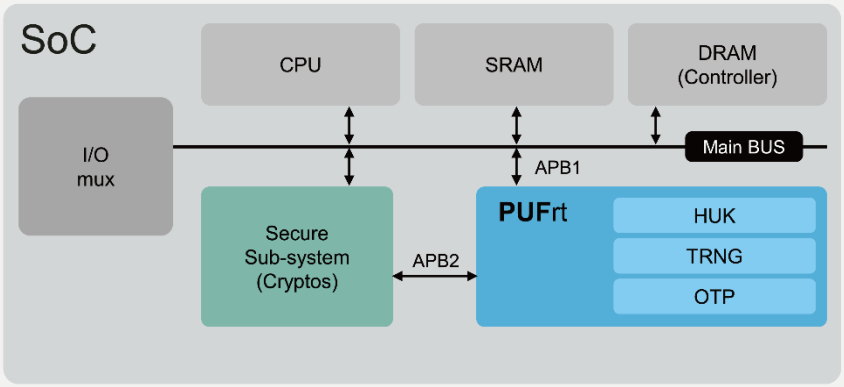
Features

- 100% compatible with any crypto coprocessor to be the root of trust
- Four 256-bit hardware PUF fingerprints with self-health check
- Up to 128kb mass production OTP with built-in instant hardware encryption
- Comprehensive anti-tamper designs implemented through physical and RTL designs
- High-speed, low-power and pre-harden true random number generator
- Supported APB/AHB/TCM interfacing with secure/non-secure access privilege

Root of Trust



Suggested Integration



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
- Reference API/FW Libraries
- Hard Macro Release Note
- Test Methodology
- Testbench

Details

Process Availability

- Scalable down to 5nm, and continuous development
- Available across worldwide foundries

Security Features

- Riscure certified
- Resistant to physical attacks, including decapsulation, microscope imaging, probing, reverse engineering, etc.

PUF-based Secure Storage

- Up to 128Kb OTP
- Various memory maps configurations to fulfill different usage scenarios
- Dummy insertion read based on entropy from TRNG
- Scrambler based on PUF value securely stores keys, unique to each PUFrt
- Stored values cannot be changed/deleted

Controller/Interface

- APB or AHB System Bus Interface
- APB or TCM Private Bus Interface
- Secure OTP Wrapper (Factory test, user, RMA debug, Read/Write, Read-Only, and Non-accessible modes)
- IEEE1687 JTAG testing interface
- Optional XiP package available
- Autoload interface for system calibration upon powering on to support product LFM, secure boot, secure debug, etc.
- Memory Built-In Self Repair/Test Data Register/Secure Debug access through external Test Access Port

PUF-based TRNG

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

PUF-based Unique ID

- With ideal minimum entropy of 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

info@pufsecurity.com