PUFsecurity

PUFrt - Hardware Root of Trust

Datasheet

April 2022

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.

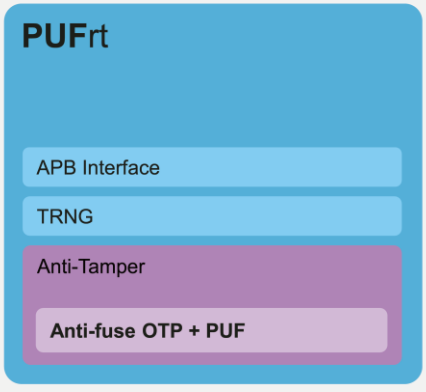
This Riscure certified IP offers the flexibility for users to add only the cryptographic engines that their designs need and comes with a well-designed anti-tamper shell against attacks. PUFrt can be integrated into a wide variety of systems, from a lightweight hardware security key to a full-functioning 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, an additional 8k-bit secure storage space with PUF is provided for the key or sensitive information injected by the customer, which makes the original security and NeoFuse OTP more resistant to physical attacks.

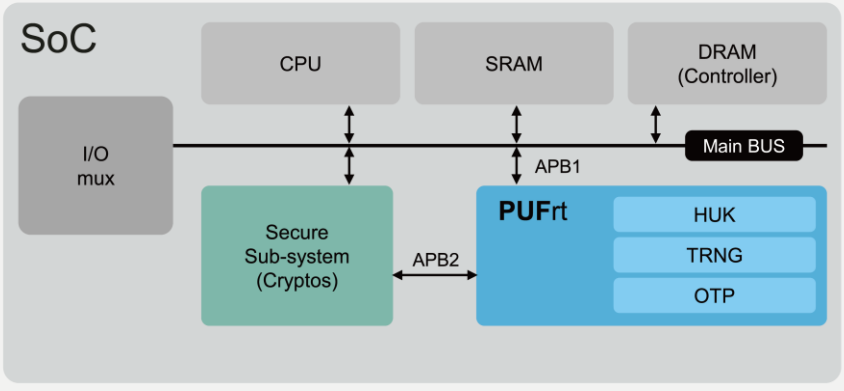
Features

- Four 256-bits 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
- APB control interface with secure/non-secure access privilege
- Built-in PUF health check

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
- Hard Macro Release Note
- Test Methodology
- Testbench

Details

Process Availability

- Scalable down to 6nm, and continuous development
- Available across worldwide foundries

Security Features

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

Controller/Interface

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

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