PUFsecurity

Secure OTP- Tamperpoof storage

Datasheet

March 2024

Description

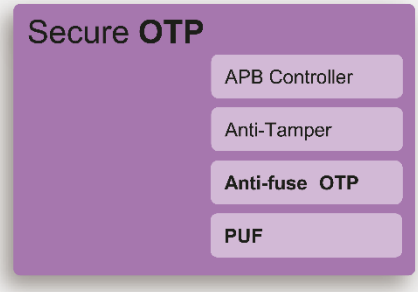
Secure OTP is a combined Physical Macro and Digital RTL providing safeguarded data protection. It is the ultimate solution for embedded Non-Volatile Memory in CMOS logic or logic-derived technologies. The RTL part provides glue logic of the OTP/PUF controller, tamperproof features, and standard AMBA interfacing. Secure OTPs tailored design maximizes efficiency and allows simplified integration across multiple emerging IC markets and ASIC applications. It is available in various densities and configurations with several CMOS technologies, delivering an embedded non-volatile memory with outstanding reliability and performance.

Secure OTP includes a 1024-bit Physical Unclonable Function (PUF) used for physical address scrambling and IO shuffling to enhance stored data security. It is a pure hardware PUF with a virtually ideal entropy that doesn't require any helper data for error correction, allowing access within a few microseconds.

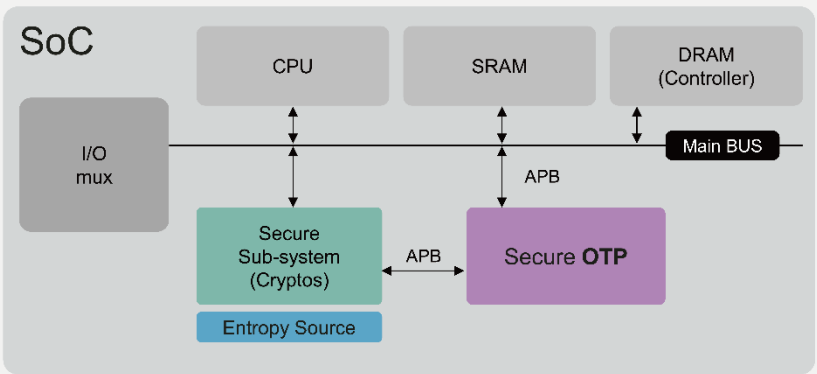
Features

- 100% compatible with any crypto coprocessor to provide secure storage
- Up to 128kb mass production OTP with built-in instant hardware encryption
- Comprehensive anti-tamper designs implemented through physical and RTL designs
- APB control interface with secure/non-secure access privilege
- Four 256-bit hardware PUF fingerprints for scrambling drop-in-use Secure OTP Storage
- Comprehensive permission, zeroization, and lock mechanism to enhance product lifecycle management and protection
- Software stack of Firmware and API

Tamperproof Storage



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 3nm, with 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
- Scrambler based on PUF value ensures secure data storage, unique to each chip
- Unique scramble value per chip, making the stored information in each chip different from each other
- Stored values cannot be changed/deleted

Controller/Interface

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

PUFsecurity Corporation

8F, No. 5, Tai-Yuan 1st St., Jhubei City,
Hsinchu County, 302082, Taiwan

info@pufsecurity.com