Secure OTP- Tamperpoof storage

Datasheet

June 2022

Description

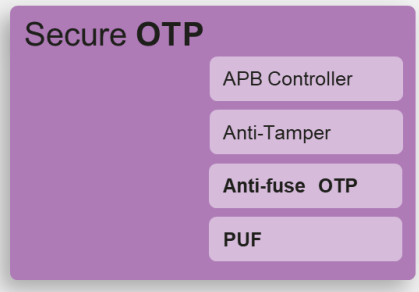
Secure OTP is a combined Physical Macro and Digital RTL providing safeguarded data protection. It is the ultimate solution for embedded Non-Volatile Memory in CMOS logic or logic-derived technologies. The RTL part provides glue logic of the OTP/PUF controller, tamperproof features, and standard AMBA 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.

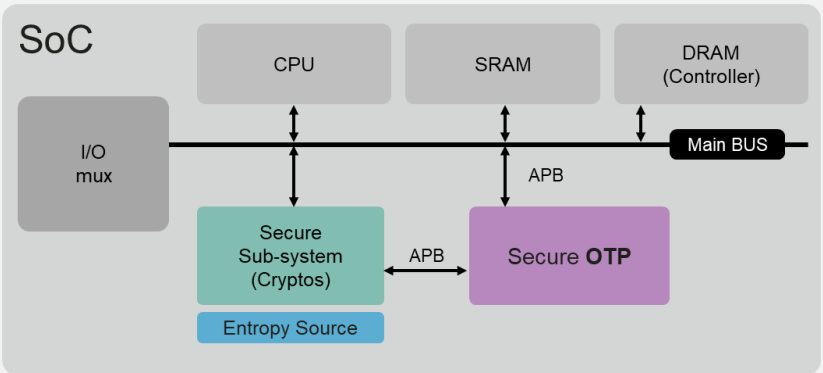
Secure OTP leads the field in terms of enhanced security OTP platform availability. Through PUFsecurity's parent company, eMemory, we draw from over 20 years of experience partnering with foundries and delivering high-quality IPs.

Today, the rising security risks to IoT devices are limiting the market's potential. The answer is creating a collaborative security ecosystem that draws from the safest Hardware, Software, and Operating System solutions. Secure OTP can become the bedrock of any chip security ecosystem and protect critical data such as the root key and the boot code.

Tamperproof Storage



Suggested Integration



Features

- Up to 128kb mass production OTP with built-in instant hardware encryption (customization available)
- Comprehensive anti-tamper designs in physical and RTL
- 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

Deliverables

- Datasheet
- Integration Note
- Application Note
- Test Methodology
- Verilog HDL File (Behavior Model)
- Verilog HDL File (FPGA)
- Hard Macro GDS
- Scripts and Testbench
- Reference FW/API

Details

Process Availability

- Scalable down to 5nm, with 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 Secure Storage

- Built-in OTP for up to 128kb
- Scrambler based on the PUF value ensures secure data storage
- Unique scramble value per chip, making the stored information in each chip different from each other
- The value stored cannot be changed or deleted

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