PUFsecurity

PUFcc – Crypto Coprocessor

Datasheet

October 2023

Description

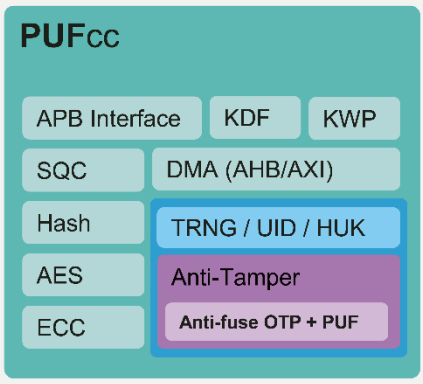
PUFcc is a novel high-security Crypto Coprocessor. Compared to traditional security SoC design (embedded HSM with secure core or discrete crypto components), PUFcc can provide a much easier to adopt hardware RoT with less vulnerability. As a result, PUFcc quickly improves the security level for any system without additional loading on the processor core or operating system.

The security boundary for PUFcc is quite robust, based on physical separation of hardware, with less vulnerability than a software-only barrier. The on-board PUF is a naturally well-protected source of static entropy, suitable for SoC architects to build a system's key hierarchy using established key generation and management procedures. In addition, PUFcc's crypto engines can perform a wide variety of secure operations, such as key exchange, secure boot or TLS (public key validation and signing), authentication (MAC), or key wrapping (again based on the natural randomness inherent to the PUF) and store said wrapped keys to external memory.

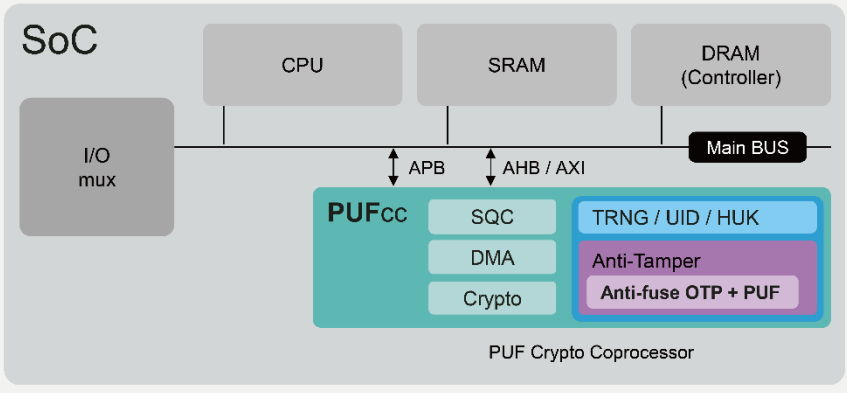
Features

- Comprehensively support all CPU architectures
- Crypto engine collective, consisting of private key cipher, message authentication code, hash, and key derivation functions that are NIST CAVP certified and OSCCA standards compliant
- Key wrapping function aiding the export of keys for external use
- Public-key coprocessor, supporting all elliptic curve cryptography functions
- 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
- APB control interface with secure/non-secure access privilege
- AXI/AHB interface for direct memory access

Crypto Coprocessor



Suggested Integration



Deliverables

- Datasheet
- Release Notes
- Integration Guidelines
- Timing .lib file
- LEF
- GDS Phantom File
- Simulation Environment and PUF-based hard-macro behavior model
- RTL: with Synthesis Script
- Application note (memory-mapped register/FW/API)
- Reference FW/API Libraries
- Hard Macro Release Note
- Testing Methodology
- Testbench

Details

Process Availability

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

Security Features

- PSA Certified Level 2 Ready
- Riscure certified
- Resistant to physical attacks, including decapsulation, microscope imaging, probing, reverse engineering, etc.

Controller/Interface

- Standard APB Control Interface
- AXI/AHB interface for direct memory access for various SoC designs
- Secure OTP Wrapper (Factory test, user, RMA debug, Read/Write, Read-Only, and Non-accessible modes)
- Autoload interface for system calibration upon powering on to support product LFM, secure boot, secure debug, etc.
- IEEE1687 JTAG testing interface
- XiP (PUFxip) package available
- External flash encryption (PUFenc) package available
- Memory Built-In Self Repair/Test Data Register/Secure Debug access through external Test Access Port

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

PUF-based TRNG

- Pre-harden and calibration free
- Ultra-fast initial time/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 optional accessory

PUF-based Unique ID

- With 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)

Key Derivation Function (KDF)

- KBKDF (CTR/FB)
- PBKDF
- KDF_HASH
- RFC4306/2246/4346

Key Wrapping (KWP)
- NIST SP800-38F key wrapping engine

Public Key Cryptography (PKC)
- NIST standard Elliptic Curves
- ECDSA/ECDH/RSA
- SM2

Message Authentication Code Engine (MAC)
- CMAC/HMAC/CBCMAC/GHASH
- POLY1305

Private Key Cryptography
- NIST SP800-SP38A/B/C/D/E supported
- AES128/192/256
- ChaCha20
- SM4
- ECB/CFB/OFB/CBC/CTR/CCM/GCM/XTS modes supported

Secure Hash Functions
- MD5/SHA1
- SHA224/256/384/512
- SHA512_224/_256
- SM3

Software
- Software stack that includes firmware, API, and Mbed-TLS drive

Comprehensive Anti-Tamper Designs

(Against Invasive Attack)
- Intrinsically physical security
- Data scrambling and shuffling
- Against voltage contrast attack

(Against Semi-Invasive Attack)
- Metal shielding
- Security-oriented IP layout
- Simulation circuit protection
- Interface protection
- Output data FI detection

(Against Non-Invasive Attack)
- Pin protection on address/mode pin and data
- Access control and Zeroization
- Unified power design
- Power floating detection
- Built-in secure repair
- Post-masking for UID and Key Storage to prevent malicious access

PUFsecurity Corporation

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

info@pufsecurity.com