PUFsecurity

PUFcc – Crypto Coprocessor

Datasheet

April 2022

Description

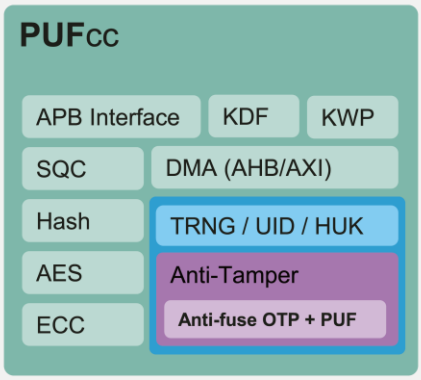
PUFcc is a novel high-security Crypto Coprocessor. Compared to traditional security SoC design (embedded HSM with secure core or discrete crypto components), PUFcc can provide a much easier to adopt hardware RoT with less vulnerability. As a result, PUFcc quickly improves the security level for any system 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.

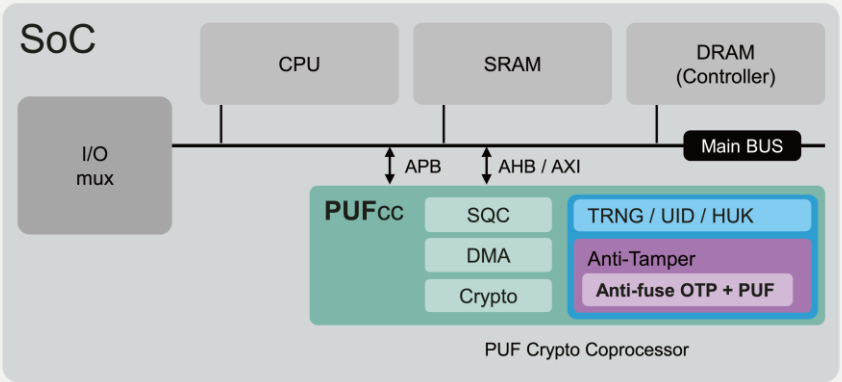
Features

- Crypto engine collective, consisting of private key cipher, message authentication code, hash, and key derivation functions that are NIST CAVP certified and OSCCA standards complied
- Key wrapping function aiding the export of keys for external use
- Public-key coprocessor, supporting all elliptic curve cryptography functions
- Four 256-bits hardware PUF fingerprints with self-health check, that could be used as a unique identification (UID) or a root key(seed)
- 8k-bits mass production OTP with built-in instant hardware encryption as standard off shelf
- Customization in OTP size is available
- Comprehensive anti-tamper designs in physical and RTL
- High-quality 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
- Phantom GDS
- Simulation Environment and PUF-based hard-macro behavior model
- RTL: with Synthesis Script
- Application note (memory-mapped register/FW/API)
- FW/API Reference code
- Hard Macro Release Note
- Testing Methodology
- Test Bench

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 Access Control Factory test, user, Read/Write, Read-Only, and Non-accessible modes)
- AXI/AHB interface for direct memory access for various SoC designs

PUF-based Storage
- Built-in 8k-bits 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 initial time/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)

Key Derivation Function (KDF)
- KBKDF (CTR/FB)
- PBKDF

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
- Cipher: AES128/192/256
- ChaCha20
- SM4
- ECB/CBC/CTR/CCM/GCM/XTS modes supported

Secure Hash Functions

- SHA224/256/384/512
- SHA512_224/256
- SM3

Software

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

Comprehensive Anti-Tamper Designs

(For Invasive Attack)

- Intrinsically physical security
- Data scrambling and shuffling
- Against voltage contrast attack

(For Semi-Invasive Attack)

- Metal shielding
- Security-oriented IP layout
- Simulation circuit protection
- Interface protection
- Output data detection

(For 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 against malicious access

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