PUFsecurity

PUFcc7 – TLS 1.3 Compliant Crypto Coprocessor

Datasheet

March 2024

Description

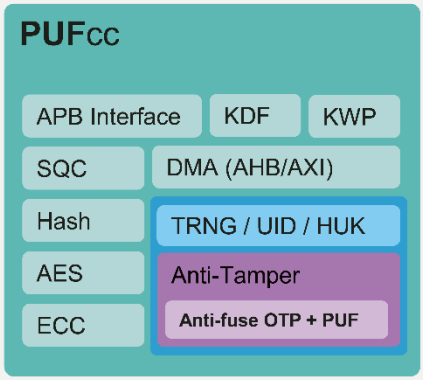
PUFcc7 is the latest revision of PUFsecurity's high-security Crypto Coprocessor. Compared to traditional security SoC designs in which each crypto component must be integrated separately, PUFcc7 is a much easier solution. As a result, PUFcc7 quickly improves the security level for any system as well as off-loading the security functions away from the processor core and operating system.

The security boundary for PUFcc is robust, based on physical separation of hardware, with less vulnerability than a software-only barrier. The on-board PUF is a well-protected source of static entropy, suitable to base an SoC's key management procedures, including key generation and derivation. In addition, PUFcc7's standard crypto engines offer the flexibility to perform a wide variety of secure operations, such as key exchange, secure boot, TLS 1.3 handshaking and messaging, authentication (MAC), or key wrapping (again taking advantage of the natural randomness inherent to the PUF) for the secure export of wrapped keys to external memory.

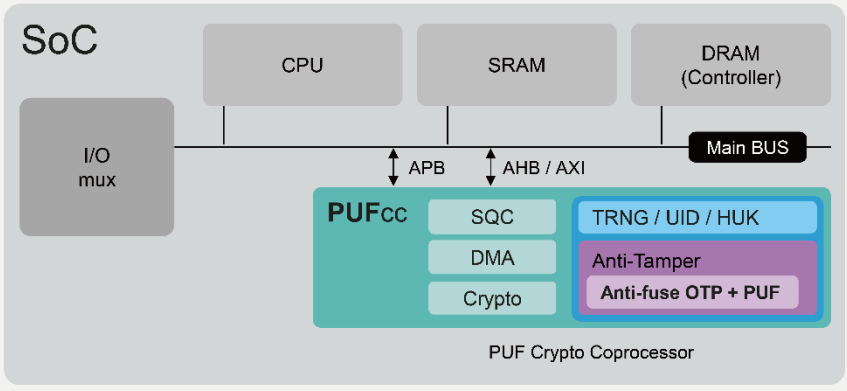
Features

- NIST CAVP certified and OSCCA standard compliant crypto engine suite
- Includes private/public key ciphers, message authentication code, hashes, and key derivation
- Key wrapping function for the secure export of keys
- Public-key coprocessor for digital signatures and key agreements over elliptic/Edward curves
- Four 256-bit PUF fingerprints with self-health checking, suitable for direct use as unique identification (UID) or as a root key (seed)
- Mass production OTP (8Kb standard) with hardware encryption and user-configurable partitions
- Comprehensive anti-tamper designs implemented through physical and RTL methods
- Silicon-proven and NIST-compliant deterministic random bit generator
- APB control interface with secure/non-secure access privilege
- AXI/AHB interface with 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 Libraries
- Hard Macro Release Note
- Testing Methodology
- Testbench

Details

Process Availability
- Scalable down to 3nm, with continuous development
- Available worldwide, at most 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, RMA debug, Read/Write, Read-Only, and Non-accessible modes)
- AXI/AHB interface for direct memory access for various SoC designs

PUF-based Storage
- Standard 8Kb OTP w/flexible partitioning
- Dummy insertion read based on RNG entropy to prevent side channel analysis
- Scrambler based on PUF value securely stores keys, unique to each PUFcc7
- Stored values cannot be changed/deleted
- Autoload function for automatic data readout after system power on

NIST SP800-90C Compliant 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
- Provides ideal minimum entropy (1)
- Unpredictable randomness and uniqueness with near-perfect 50% Hamming Weight and Distance
- On-demand keys for on-chip secret and off-chip ID or key generation/seeding
- Optimal reliability with lifetime zero Bit-Error-Rate (BER)
- Robust functionality over wide operating range (Temp: -40~175°C)

Interface Extensions for More Functionality
- Authenticated pairing with auxiliary PUFsecurity modules
- Memory Built-In Self Repair/Test Data Register/Secure Debug access through external Test Access Port

Key Derivation Function (KDF)
- Key/Password/Hash-based
- KDF_HASH
- RFC4306/2246/4346

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

Public Key Cryptography (PKC)
- NIST approved Elliptic/Edwards Curves
- ECDSA/ECDH/RSA
- EDdSA/X25519/X448
- SM2

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

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

Secure Hash Functions
- MD5/SHA1
- SHA2
- SHA3/SHAKE128/256
- SM3

Software
- Software stack including firmware, API, and Mbed-TLS driver

Comprehensive Anti-Tamper Designs
(Against Invasive Attack)
- Intrinsic physical security
- Data scrambling and shuffling
- Immune to 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 for address/data/mode IOs
- 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