SECURE-IC
THE SECURITY SCIENCE COMPANY

PRODUCT SHEET

Securyzr™ > Securyzr™ Secure HW Solutions >Securyzr™ Security IP > Key Managment > SCZ_IP_PUF_200/300

# PHYSICAL UNCLONABLE FUNCTION (PUF)

PQC Post-Quantum Cryptography READY

**A Physically Unclonable Function (PUF) is a security mechanism that uses the inherent physical variations of a device to generate a unique, unclonable output. This output can be used as a cryptographic key or a device identifier. PUFs rely on the fact that the exact physical properties of a device, such as the physical and electrical characteristics on a chip, can never be replicated exactly. This makes PUFs a highly secure method for protecting sensitive information and ensuring device authenticity. PUFs are often used in a wide range of applications, including secure boot, secure storage, and secure key generation. This PQC ready PUF IP Core is compliant with ISO/IEC 20897where Secure-IC has been the lead party for PUF quality test standard, thus making it the easiest technology to use on the market and the most reliable (with no need to make a testchip before). In addition it can be used in any technology node and foundry.**

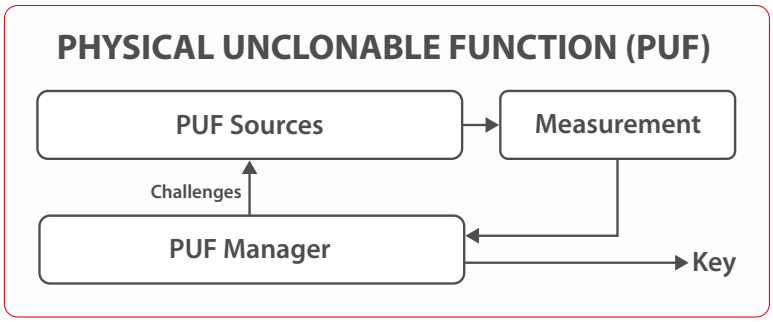
PUF IP Core is a secret key generation system based on Physically Unclonable Functions (PUF). The secret key is extracted by the PUF from the silicon by using its inherent properties: technological dispersions are amplified into digital signals (bits of information). The key generated by the PUF is not readable but extracted using a group of helper-data. This distinctive feature allows a real protection against the reverse-engineering techniques compared to traditional methods that store the key in non-volatile memory.

PUF IP core ensures the following properties:

- Steadiness
- Randomness
- Uniqueness
- Tamper resistance
- Mathematical Unclonability
- Physical unclonability

Security metrics:

- Entropy = 128.0 bit for a typical AES-128 key
- Reliability = fixed to the desired value, e.g., 1 FIT for ASIL D
- Entropy & reliability ensured in all specified corners (owing to adaptive control, a unique feature of our PUF)




Secure-IC have developed a **worldwide unique** PUF IP that does **not require** any **enrollment phase** nor a **rebuilding phase**. By leveraging our PUF generation method and expertise, we are offering a PUF IP capable of generating one or a few unique IDs or keys working straight out of the box.

ENROLLMENT PHASE **FREE** version available

## Features

- Secure storage without the use of any non volatile memory
- No external key provisioning required
- Does not require costly SRAM blocks
- Proven reliability regarding voltage, temperature and aging with error probability much lower than 10-9
- Security certification ready (including Common Criteria)
- Compliance with ISO/IEC 20897, adapted to CC AVA_VAN.5, FIPS 150-3 lvl 3, OSCCA level 2+
- Possibility to revoke keys (owing to compromission, refurbishing, expiry of a crypto-period)
- Protected against side-channel observation during key extraction using randomization (use of a PRNG)
- Formal security validation (stochastic model)
- Compatible with all process nodes (built from RTL + SDC sources)
- Low weight helper data (Possible to work without helper data at all)
- Health tests to attest of the IP proper functioning
- No calibration needed after design
- Easy integration
- AMBA (APB) interface

## Applications

- IoT
- Mobile
- Automotive (Qualified AEC-Q100 grade 0)
- Bank & Payment

## Ideal for

Physical Unclonable Functions (PUFs) are being used in various markets (examples) such as:

*Information security*
To secure digital devices by generating unique and unpredictable identifiers, which can be used for authentication, encryption, and access control.

*IoT*
To secure IoT devices, such as smart home systems, wearable devices, and industrial sensors, by providing unique and unclonable identities and preventing unauthorized access.

*Automotive*
Used in automotive systems to secure access to critical components, such as engine control units, and prevent tampering and reverse engineering.

*Healthcare*
To secure medical devices, such as pacemakers and insulin pumps, to prevent unauthorized access and protect sensitive patient information.

*Banking and finance*
Used in payment systems and financial services to secure transactions and prevent fraud.

*Government and military*
Used in government and military systems to secure sensitive information and protect against cyber attacks.

## Credential generation

The PUF IP ensures credential generation based on process variations properties which are unique from chip to chip, impossible to reproduce or emulate, hence alleviating the problem of external key management system and can be used for several use-cases, detailed hereafter:

- Generation of a unique identity for a semiconductor device
- Anti-tamper key protection against cloning or reverse engineering
- Chip sample authentication using a challenge response protocol
- Firmware authentication (integrity + genuine origin) using the generated key
- Firmware encryption (unique per device, which pairs a code with a device, thereby denying attack-one-break-all attacks) using the generated key

## Deliverables

- Technical specifications
- RTL of the AMBA wrapper
- RTL code of the entropy source
- Remote support for integration
- User guide
- Post-synthesis generic netlist
- SDC file
- Integration guidelines
- Test report documentation
- Self-checking RTL Testbench based on reference scenario for simulation. (Simulation scripts are adapted to Questasim, any change of Simulator shall be taken care of by the Licensee)

V1.2

SECURE-IC
THE SECURITY SCIENCE COMPANY

**HEADQUARTERS**
Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 72 - contact@secure-ic.com

**EMEA**
sales-EMEA@secure-ic.com

**AMERICAS**
sales-US@secure-ic.com

**APAC**
sales-APAC@secure-ic.com

**JAPAN**
sales-JAPAN@secure-ic.com

**CHINA**
sales-CHINA@secure-ic.com

CONTACT US
www.secure-ic.com