PUF-Based RoT IP: Where Security and Safety Meet

The IP can be designed into the hardware at fabrication or implemented as "soft IP" post-silicon, enabling remote "brownfield" implementation of a hardware root of trust.

When adding automated driving functionalities to vehicles, functional safety only takes you so far. Each safety mechanism/system can be compromised by a security attack if not properly protected. Many attacks in the past years have led to new legislation, such as the UN regulation 155. The automotive industry now needs to ensure that their vehicle fleet is secure by design and each vehicle is safely maintained through its life cycle. Components in autonomous vehicles need to adhere to the industry standard ISO/SAE 21434 "Road vehicles – Cybersecurity Engineering."

On top of functional safety, automotive components require a proven, hardened level of security that provides resistance to invasive and non-invasive attacks, and securely and reliably protects those assets for their entire life. The Intrinsic ID security IP products have been protecting millions of ASIC/SoC/MCU and FPGA-based devices for more than a decade with no known breach or failure. Our leading-edge IP enables us to customize hardware security to deny adversaries access to any key material or data, even on autonomous assets. Intrinsic ID products are agnostic to foundry and process node and currently protect over 600 million devices.

Benefits

- Scalable across all foundries and process nodes:
  - Proven on i.e. GF, IFS, Samsung, UMC, TSMC
  - From 350 nm to 5 nm (3nm in design)
- No sensitive key material present on device
- High protection against tampering and invasive attacks
- Resistant to post-quantum attacks
- Empirically proven to be secure and reliable over 25 years product life

PUF-Based Hardware Root of Trust

The Intrinsic ID hardware security IP uses inherently random elements on the device as a physical unclonable function (PUF), which generates the entropy needed for a strong hardware root of trust. It enables designers to secure their products with internally generated, device-unique cryptographic keys.

The Intrinsic ID PUF technology is widely used to protect MCU, ASIC, SoC and FPGA devices. It is frequently updated with countermeasures to secure PUF key material and sensitive data from invasive and non-invasive attacks.

Markets

- Automotive
- Aerospace & Defense

Applications

- Authentication
- Secure key storage
- Trusted supply chain
- Flexible key provisioning
- Anti-counterfeiting
- Anti-reverse engineering
- Chiplet security

Certifications

- Meets ISO 26262 ASIL B fault metric
- ASIL D for systematic failures
- SESIP Level 3
- PSA Certified Level 3 RoT Component
- NIST CAVP
- ISO/IEC 20897-compliant PUF
- FIPS 140-3 support
- SRAM PUF-enabled products have been certified by EMVCo, Visa, CC EAL6+, PSA, and ioXt
- DoD and EU governments qualified

QuiddiKey – SRAM PUF RoT IP

Intrinsic ID QuiddiKey is the world-leading IP that uses standard SRAM as a PUF to create a hardware root of trust. It offers key provisioning, wrapping, and unwrapping to enable secure key storage across the supply chain and for the lifetime of the device. The PUF root key is never stored, but re-created from the PUF each time it is needed, offering the highest level of security. A key protected by QuiddiKey is integrity protected and can be decrypted solely on the same device where it was created.

QuiddiKey is the world's first IP to receive a SESIP and PSA Certified level 3 certification. Our latest product, QuiddiKey 400, has been developed following an ISO 26262 functional safety compliant flow, and meets the ISO 26262 Automotive Safety Integrity Level (ASIL) B fault metric.

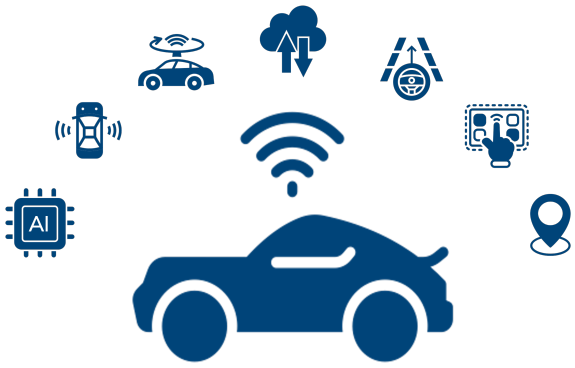
Apollo – Butterfly PUF IP

For FPGA architectures for which standard uninitialized SRAM is not available, e.g. Xilinx FPGA, a butterfly PUF enables designers to extract a PUF from standard FPGA fabric. This PUF is used to create a high-quality device-unique PUF key. The intrinsic PUF key can be used as a root key for key derivation and key wrapping. It enables designers to create and store an unlimited number of keys and data securely in unprotected NVM on/off chip.

Apollo operates on any Virtex-6 (ISE) or Series 7 or later (Vivado) device including Series 7, Zynq, UltraScale and UltraScale+ MP/SoC.

Zign – Embedded Software

The Intrinsic ID Zign X00 embedded software solutions democratize root of trust technology by uncoupling it from silicon fabrication, ensuring it can be accessed, understood, and implemented by application developers at scale. A trust anchor can even be retrofitted on deployed devices. The solution is available in off-the-shelf configurations with size ranging between 6 kB and 29 kB.



Use Cases

- **Trusted Supply Chain:** device is locked from moment of fabrication. Each owner can lock their IP using their device-unique keys throughout the device life cycle.
- **Flexible Key Provisioning:** enables generation of an almost unlimited number of keys for multiple uses and applications
- **Anti-Cloning:** binding of proprietary IP to unique device prevents cloning.
- **Secure Communication:** Communications between all parts of the system can be securely authenticated to protect from eavesdropping and alteration.

Security Standards

Cryptographic algorithms are NIST CAVP certified and support a FIPS 140-3 system.

PUF – ISO/IEC 20897

HMAC – FIPS 198-1

HMAC-DRBG – NIST SP 800-90Ar1

KDF – NIST SP 800-56C, NIST SP 800-108

AES – FIPS PUB 197, NIST SP 800-38A

SHA – FIPS PUB 180-4

NIST elliptic curves – NIST SP 800-186

ECC-CDH – NIST SP 800-56Ar3

DRBG/RNG – NIST SP 800-90A/B

INTRINSIC ID

www.Intrinsic-ID.com | info@Intrinsic-ID.com