Building Trust in System-in-Packages

SRAM PUFs can be used from the earliest moment of production to secure any chiplet, any time, any place

As device scaling becomes unfeasible and too expensive for most applications, the popularity of using multiple small chiplets, each with a dedicated function, within a system-in-package (SiP) grows. Future complex designs could easily include 100 chiplets sourced from a variety of vendors, making the already complex and increasingly untrustworthy SoC supply chain even more so. Spreading functionality over multiple chiplets from different vendors increases the attack surface of electronic systems in many ways. Chiplets from untrusted sources can be malicious, vulnerable to attacks, or unreliable. Third parties can overproduce chiplets or steal IP.

Traditional methods for tracking and securing chips are too costly, unreliable, and not flexible enough for complex SiP designs. Intrinsic ID offers very strong and flexible authentication solutions based on its patented SRAM physical unclonable function, or SRAM PUF, technology. These solutions can be used from the earliest moment in production to ensure that every chiplet is genuine and secure. IP can be bound to the hardware of the chiplet and communications between all parts of the system can be securely authenticated to protect from eavesdropping and alteration.

Features

- Uses standard SRAM as a PUF to create a hardware root of trust (RoT)
- Offers key provisioning, wrapping, and unwrapping to enable secure key storage across the supply chain and for the lifetime of the device
- Root keys are never stored, but re-created from the PUF each time they are needed
- Keys are bound to the chiplet and can only be recreated and accessed on the chiplet on which they have been created

Benefits

- No need for secure storage inside the chiplet to store a root key
- Technology scaling independent, fully digital IP – offering the best combination of security, flexibility and cost
- Highly reliable solution in the most advanced technology nodes
- Enables identification and tracking of chiplets that have no NVM available
- Offers stronger authentication and higher security than traditional key storage in NVM

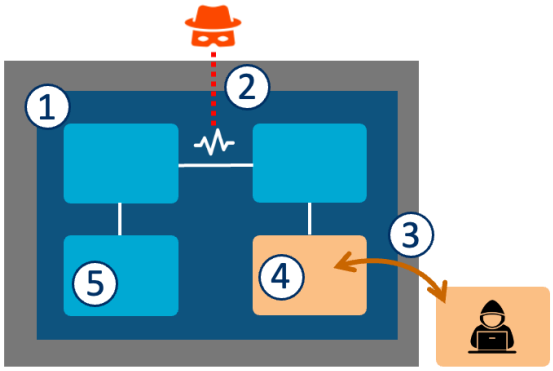
Applications

- Secure key storage
- Authentication
- Flexible key provisioning
- Anti-counterfeiting
- IP binding
- Supply chain protection

Certifications

- NIST CAVP
- Supports FIPS 140-3
- ISO/IEC 20897-compliant PUF
- SRAM PUF-enabled products have been certified by EMVCo, Visa, CC EAL6+, PSA, and ioXt
- DoD and EU governments qualified

Security Challenges for SiPs



1. Components are fabricated in multiple locations, requiring trusted third parties
2. Top-layer chip-to-chip interfaces are susceptible to man-in-the-middle attacks
3. Insertion of untrusted chiplets
4. Untrusted chiplets can be malicious, vulnerable to attacks, or unreliable
5. Third parties can overproduce or steal IP

Trust Validation Levels with SRAM PUF Solutions

Depending on the application, the threat model, and the security boundaries of the system, different levels of trust validation for SiPs may apply.

A first level of trust validation is obtained by using SRAM PUFs to identify chiplets and detect counterfeit chiplets. Only 0.2 kB of SRAM is needed to create a fuzzy chiplet identifier that can be stored in the Intrinsic ID Zign® Tag database. This solution works on any chiplet and enables tracking from the earliest moment in production. Zign Tag offers a robust and scalable solution, without the need to store an identity or key on the device, enabling the identification and tracking of chiplets that have no NVM available.

The Intrinsic ID flagship products QuiddiKey and Zign X00 offer **a higher level of trust validation**, e.g. for chiplet and data authentication or for IP binding. These solutions enable secure connections using PUF-based chiplet-unique symmetric keys that are only known within the SiP. No UID programming is needed and there is no need for OTP inside the chiplet to store keys.

The strongest level of authentication can be achieved by combining SRAM PUFs with asymmetric crypto connected to a traditional PKI system where every chiplet obtains a device certificate from the manufacturer guaranteeing its authenticity. A certificate is only as strong as the protection of the private key. PUF-based solutions offer the strongest form of key protection.

Security Solutions in Hardware or Software

Intrinsic ID PUF-based security solutions are available in hardware IP as well as software. They use the inherently random start-up values of SRAM as a PUF, which generates the entropy required for a strong hardware RoT. The root key is re-generated every time the chip is powered up and is only available (in volatile memory) when needed. This means the key is never present in persistent memory, not even when the chip is powered down, which raises the security significantly and eliminates the need for OTP or secure memory.

QuiddiKey® RoT IP can be used with any foundry and process node. It is available in off-the-shelf configurations with size ranging between 45k and 72k gates and can be applied easily to almost any chip. QuiddiKey has been deployed and proven in hundreds of millions of devices certified by EMVCo, Visa, CC EAL6+, PSA, ioXt, and governments across the globe.

The Intrinsic ID **Zign X00** embedded software solutions democratize RoT 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 7 kB and 30 kB.