SECURITY & TRUST

Garmo-PUF-Core

Security — multi-source silicon PUF root-key subsystem

IP-2081 · Evaluation package · Evaluation / IP scope

Function and architecture

- SRAM/RO/bistable PUF source abstraction
- at least two physically independent sources
- Enrollment helper data with BCH/LDPC-style fuzzy extractor boundary
- Aging/temperature compensation and confidence scoring

Integration summary

Garmo-PUF-Core integration role: Security — multi-source silicon PUF root-key subsystem. Documented composition: SRAM/RO/bistable PUF source abstraction; at least two physically independent sources; Enrollment helper data with BCH/LDPC-style fuzzy extractor boundary; Aging/temperature compensation and confidence scoring.

Technical record

Canonical identity	IP-2081
Responsibility	Security — multi-source silicon PUF root-key subsystem
Documented interface architecture	PUF hard-macro sample bus, CSR, key-ladder output, lifecycle/zeroize
Documented building blocks	SRAM/RO/bistable PUF source abstraction; at least two physically independent sources; Enrollment helper data with BCH/LDPC-style fuzzy extractor boundary; Aging/temperature compensation and confidence scoring
Delivery boundary	Evaluation / IP scope
Evidence scope	Evaluation package
Architecture targets · not measurements	256-bit derived root key; <1e-6 reconstruction failure target after ECC; zero stored root secret.

Delivery and release binding

- Interface version and parameter set
- Clock/reset domains and integration constraints
- Companion memory, PHY and software requirements

• Verification collateral and acceptance criteria

Confirm for the selected release: Node/library binding, Clock/reset limits, Physical and protocol dependencies, Artifact hashes, Acceptance criteria.

Evidence and qualification

Canonical technology and its architecture/integration role are recorded. The offered delivery is confirmed against the exact release before licensing.

Physical entropy, uniqueness and stability require measured silicon characterization.

Canonical status: P3 / REPRESENTATIVE ARCHITECTURE RTL — concrete integration specification and synthesizable RTL shell/representative datapath only; all frequency, throughput, power, area, jitter and standards-superiority figures remain architecture targets until the required evidence hierarchy closes. Analog/custom production claims require transistor-level/custom-layout, extracted PVT/Monte-Carlo and silicon characterization.

Source basis: Bible v7.42 IP-2081

Evaluation and licensing

Evaluation: Evaluate an individual IP configuration. Production: Named-design production license. Custom work: Node binding or derivative integration. Rights, pricing, support and acceptance criteria are agreed for the exact scope.

Contact: patrick@garmolabs.com | Product path: /ip/garmo-puf-core