SECURITY & TRUST

Garmo-AES-256-GCM

Multi-context authenticated-encryption datapath architecture.

IP-2083 · Evaluation package · Evaluation / IP scope

Function and architecture

- AES-128/192/256, GCM/GMAC/CTR with 512-bit parallel datapath
- 8+ interleaved contexts, independent IV/AAD/length state
- Pipelined GHASH using multi-lane carry-less multiply tree

Integration summary

Garmo-AES-256-GCM integration role: Security — ultra-high-throughput multi-context AES-GCM engine. Documented composition: AES-128/192/256, GCM/GMAC/CTR with 512-bit parallel datapath; 8+ interleaved contexts, independent IV/AAD/length state; Pipelined GHASH using multi-lane carry-less multiply tree.

Technical record

Canonical identity	IP-2083
Responsibility	Security — ultra-high-throughput multi-context AES-GCM engine
Documented interface architecture	AXI-stream plaintext/ciphertext/AAD, key-ladder input, descriptor queue, IRQ
Documented building blocks	AES-128/192/256, GCM/GMAC/CTR with 512-bit parallel datapath; 8+ interleaved contexts, independent IV/AAD/length state; Pipelined GHASH using multi-lane carry-less multiply tree
Delivery boundary	Evaluation / IP scope
Evidence scope	Evaluation package
Architecture targets · not measurements	512 bits/cycle; 768 Gb/s @1.5 GHz per engine; dual-engine option 1.536 Tb/s.

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.

No node-port, silicon-performance, standards certification or analog qualification is inherited from a related product.

Canonical status: P0 / 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.

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-aes-256-gcm