KiviCrypt-AES-GCM

IP Core Product Brief 20260429

KiviCrypt-AES-GCM Overview

The KiviCrypt-AES-GCM IP core implements the Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) specified in the NIST SP800-38D. AES-GCM is a widely used cryptographic algorithm for Authenticated Encryption with Associated Data (AEAD) purposes, providing both data confidentiality and authenticity. The IP core supports key sizes of 128, 192, and 256 bits, with a standard IV length of 96 bits. It can operate either with a pre-expanded key or with an internal key expansion mechanism, which is used by default. Its architecture is maintaining a fully synchronous design, making it suitable for both FPGA and ASIC implementations.

Variants	Description
KiviCrypt-AES-GCM-Fast	Optimized for minimal logic and power usage, making it suitable for designs with stringent FPGA resource or energy constraints.
KiviCrypt-AES-GCM-HighSpeed	Optimized for high processing throughput, suitable for designs that require increased performance while maintaining efficient use of resources.

Key Features

- NIST SP 800-38D compliant
- Key size: 128, 192, 256 bits
- IV length: 96 bits
- Works with pre-expanded key or internal key expansion (default)
- Optional with DMA engine
- Optional AMBA® AXI4-Lite
- Fully synchronous design
- Optional HAL and software driver (C-code, platform independent)
- For any FPGA and ASIC

Application and Use Cases

- Secure communication: IPsec, TLS, MACsec
- High-speed data paths: Protecting data streams
- Firmware updates: Ensuring confidentiality and integrity of updates
- Secure storage: Encrypting & authenticating data in flash/external memory
- Internal bus protection: Securing data transfers between FPGA & SoC

Test and Verification

- NIST test vectors for AES-GCM block cipher mode
- Extended verification through simulation
- FPGA integration and implementation tests
- Unity tests for driver and whole IP Core

Licensing & Services

- Product license
  - One-time license fee
  - Single or multi project license
- Free evaluation license
- Technical support by email
- Maintenance & updates

Deliverables

- Product license
  - System Verilog RTL source code or netlist format
- Free evaluation license
  - Netlist format, time bombed
- Testbenches
- Integration examples
- Software HAL & driver source code
- Software example

Documentation

FPGA Implementation Results

	KiviCrypt-AES-GCM-Fast			KiviCrypt-AES-GCM-HighSpeed		
AMD (Xilinx)	**LUTs**	**fmax (MHz)**	**max. Troughput (Gbps)**	**LUTs**	**fmax (MHz)**	**max. Troughput (Gbps)**
Spartan 7	11158	113.4	1.5	18598	110.7	14.2
Kintex 7	11159	172.0	2.2	18436	176.9	22.6
Zync US+ MPSoC	11161	289.7	3.7	18483	256.4	32.8
Versal AI Cores Series	9365	341.8	4.4	18427	327.7	42.0

Efinix	**XLR**	**fmax (MHz)**	**max. Troughput (Gbps)**	**XLR**	**fmax (MHz)**	**max. Troughput (Gbps)**
Titanium	15196	280.3	3.58	18373	256.6	32.8
Topaz	15196	188.6	2.40	18373	147.6	18.9
Trion	15196	68.5	0.88	18373	60.4	7.7