

Message Authentication IP Core

The KiviHash-AES-GMAC IP core generates and verifies authentication tags using Galois Message Authentication Code (GMAC), as specified in NIST SP 800-38D. GMAC is derived from AES-GCM and provides data integrity and authenticity without encrypting the data. It is suited to systems that need to authenticate messages or data streams while keeping their contents in plaintext. The core supports AES keys of 128, 192 and 256 bits, a 96-bit IV, and tag lengths from 32 to 128 bits. It accepts either a pre-expanded key or performs key expansion internally by default. Its fully synchronous architecture is designed for integration into FPGA and ASIC systems.

Variants	Description
KiviHash-AES-GMAC-Fast	Optimized for high processing throughput, suitable for designs that require increased performance while maintaining efficient use of resources.