AES-HS: High-Speed Encryption IP Core

Reduce your cyber risk with reliable, fast encryption

The near instantaneous high-bandwidth communication of the modern world carries with it the risk of exposure of critical data. Keeping confidential data secure from the wrong people is important to protect your customers and your business. How can you protect your data without compromising performance?

You'll need to implement encryption on your product—and you can get that high performance with *hardware accelerated* encryption. The AES-HS Core is an encryption/decryption solution for FPGAs that easily scales to your needs. DornerWorks has been working on FPGA-based hardware acceleration for years, and Xilinx recommends us for design services as a Premier Member of their Alliance Program.

Features

- FIPS 140 and NIST SP800-38A compliant
- Implements AES CTR block mode to NIST FIPS 197
- Supports 128-bit and 256-bit keys
- Supports > 80 Gbps throughput on Xilinx UltraScale+ devices with a single core
- Configurable to optimize for highest performance or reduced device utilization (see below)
- AXI-4 Lite interface for configuration and control
- AXI-4 Streaming interface for input and output

Benefits

- Worry-free integration into your design, so you can protect your data without being an encryption expert
- Scalable to high-performance or high-efficiency configurations
- Unmatched performance, tested up to 80 Gbps with a single instance so you can get high performance without a dual-core solution

Target applications

- High-speed data networks
- IT infrastructure
- Video streaming
- Hardware-accelerated encryption and decryption

More on FPGA Encryption IP Cores:
http://dornerworks.com/fpga-ip

Contact us to learn more
www.DornerWorks.com
sales@dornerworks.com
616-245-8369

XILINX ALLIANCE PROGRAM PREMIER MEMBER

ZYNQ

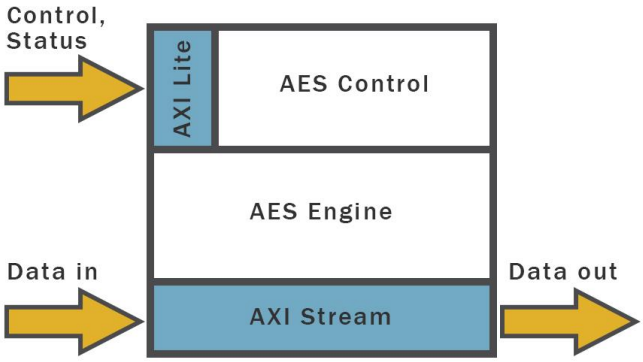
You shouldn't have to be an expert in everything

Working with DornerWorks can help you resolve any of these stress creators in your team. If you've checked any of the boxes on this Freedom to Focus Checklist, call us today, and allow us to work with you to develop your product, take it to the next level, and provide the freedom you're looking for to focus on your best thing.

DornerWorks, Ltd. 3445 Lake Eastbrook Blvd SE, Grand Rapids, MI 49546 USA

A High-Performance IP Core Solution

The AES-HS IP Core developed by DornerWorks is a high-performance encryption and decryption IP core, implementing the AES algorithm as described in the NIST Federal Information Processing Standard (FIPS) Publication 197. It operates using the CTR block mode of operation. This implementation has been measured to provide greater than 80 Gbps of throughput—with a single instance of the core—on recent Xilinx UltraScale+ FPGA devices, and it is designed to be easily integrated into existing systems by making use of the standard AXI-4 interfaces for control and I/O.



Design Deliverables

- Fully synthesizable RTL source code
- Complete VHDL testbench with test vectors
- Example design with required demo software
- User documentation

Design Tools

- Vivado Design Suite 2016.1 or later

Device Support

- Zynq-7000, Virtex-7, Kintex UltraScale+, Zynq UltraScale+, Artix-7

How to get started

1. Order the AES-HS Core now
2. Develop your solution
3. Launch your accelerated encryption product

Device Utilization

Want to know if the AES-HS IP will fit with your device or application? Here are a few configuration examples.

Device	Config	Key Length	Performance	Clock	Slices	LUTs	FFs	BRAMS
Artix-7 (-1)	Small	128	8 Gbps	270 MHz	1600	4700	4200	2
Artix-7 (-3)	Fast	128	42 Gbps	333 MHz	3400	12000	7800	2
Virtex-7 (-1)	Tiny	128	5 Gbps	400 MHz	1100	2700	3100	2
Virtex-7 (-1)	Small	128	12 Gbps	400 MHz	1500	4700	4200	2
Virtex-7 (-3)	Fast	128	64 Gbps	500 MHz	3400	12000	8000	2
Virtex-7 (-3)	Fast	256	64 Gbps	500 MHz	4900	16000	14000	2
Virtex-7 (-3)	Fast	128/256	64 Gbps	500 MHz	5800	20000	15000	2

Device	Config	Key Length	Performance	Clock	CLBs	LUTs	FFs	BRAMs
Kintex UltraScale+ (-1)	Small	128	17 Gbps	555 MHz	840	4700	4200	2
Kintex UltraScale+ (-3)	Fast	128	85 Gbps	666 MHz	2100	12000	8000	2

*Zynq® and UltraScale+™ are trademarks of Xilinx.