High-Speed Encryption IP Core

Product Summary

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.

With our AES-HS Core, you can make security happen in your product.

How to get started

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

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
- Standards-conformant to NIST FIPS-197
- Customizable support with 128-bit or 256-bit keys, and encryption and decryption in the same module
- 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

Order Now

Want to learn more about AES-HS? Additional detail is provided on the reverse side. Or give us a call.

XILINX
ALLIANCE PROGRAM
PREMIER MEMBER

ZYNQ

technology engineering so you can focus

write sales@dornerworks.com
call 616-245-8369
click www.dornerworks.com

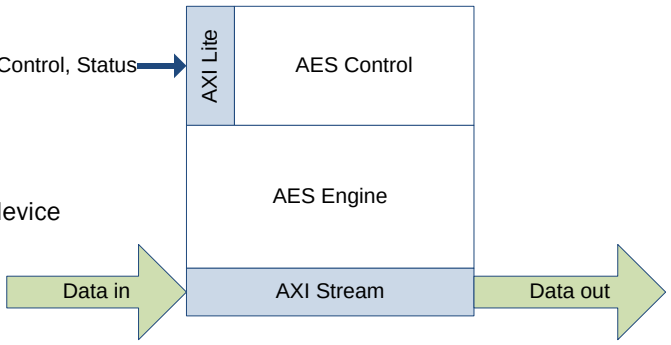
3445 Lake Eastbrook Blvd SE
Grand Rapids, MI 49546
USA

AES-HS: High-speed encryption core

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.

Features

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



Design Tools

- Vivado Design Suite 2016.1 or later

Device Support

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

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

write sales@dornerworks.com
call 616-245-8369
click www.dornerworks.com

3445 Lake Eastbrook Blvd SE
Grand Rapids, MI 49546
USA