AES Encryption IP

Pantherun, is a pioneering force in the realm of encryption technology and data protection solutions. At Pantherun, we are driven by a singular mission: to empower businesses and organizations to safeguard their most valuable asset – their data – against evolving cyber threats and security breaches.

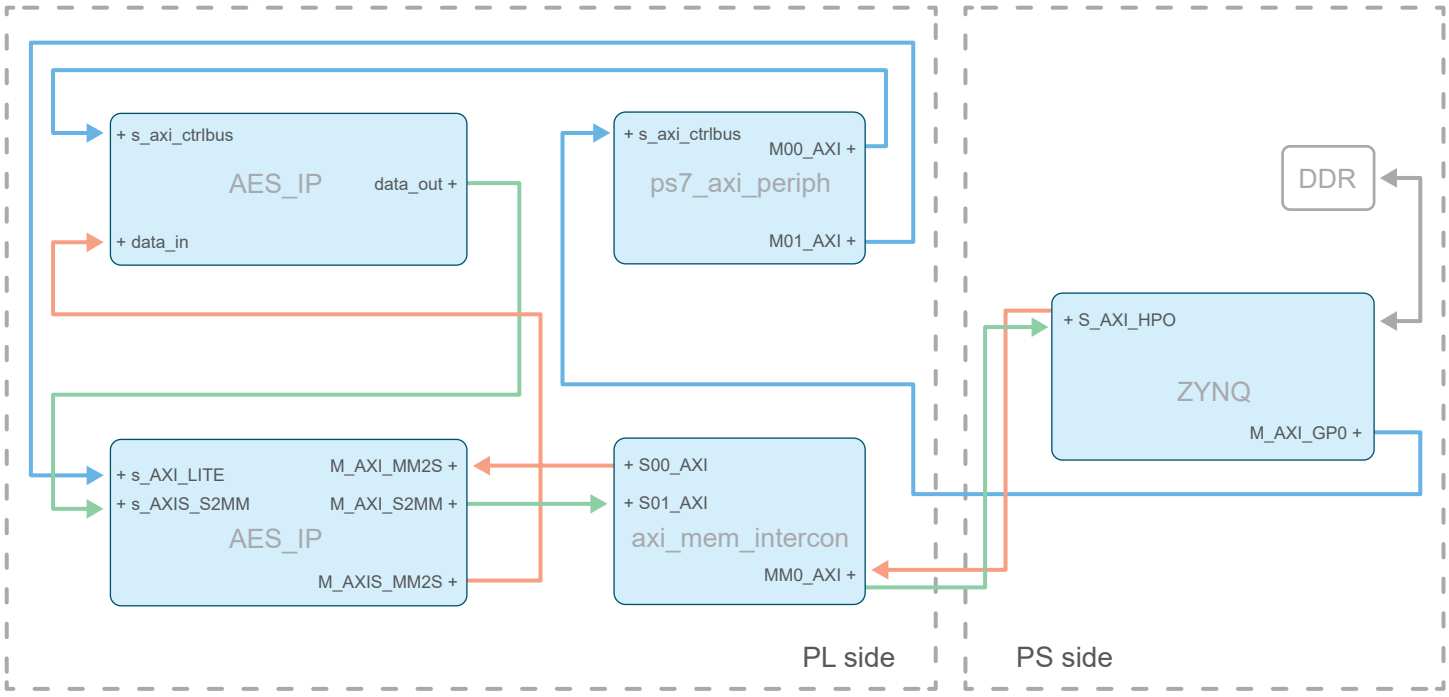
Our Commitment to Data Security

In an age where data breaches and cyberattacks pose significant risks to businesses of all sizes, data security has never been more critical. Pantherun is committed to providing state-of-the-art encryption technology and data protection solutions designed to mitigate these risks and ensure the confidentiality, integrity, and availability of sensitive information.

Expertise in Encryption Technology

With a team of highly skilled engineers and security experts, Pantherun brings decades of experience in encryption technology and cybersecurity to the table. From symmetric and asymmetric encryption algorithms to advanced cryptographic protocols, we possess the knowledge and expertise to develop robust, scalable, and future-proof encryption solutions tailored to our clients'specific needs.

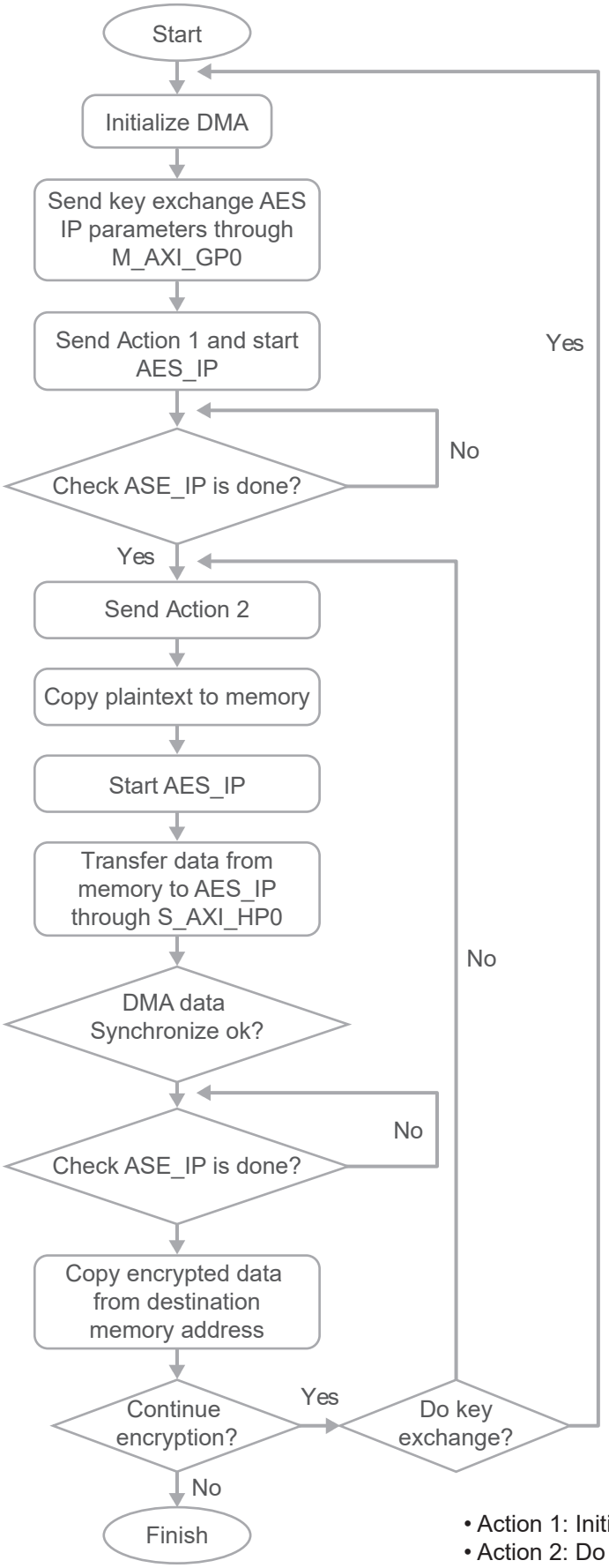
Our AES Encryption IP provides advanced encryption capabilities to secure data transmission and storage in various applications, including IoT devices, edge computing systems, cloud platforms, and communication networks. Built on the Advanced Encryption Standard (AES), our IP offers robust encryption algorithms to safeguard sensitive information against unauthorized access and data breaches.



- M_AXI_GP0: Low speed AXI Lite Bus (In blue)
- S_AXI_GP0: High speed AXI Stream bus (In red)

AES Encryption IP

Data Flow Diagram



Key Features

1. AES Encryption Standard: Implements the AES algorithm specified by the National Institute of Standards and Technology (NIST) for encryption and decryption.

2. Multiple Key Length Support: Supports key lengths of 128, 192, and 256 bits, providing flexibility to meet different security requirements.

3. High Performance: Optimized for high-speed encryption and decryption operations, enabling efficient processing of large volumes of data.

4. Low Power Consumption: Designed for low-power applications, minimizing energy consumption while maintaining high-performance encryption capabilities.

5. Small Footprint: Compact design enables integration into resource-constrained devices and systems without compromising performance or security.

6. Hardware Acceleration: Utilizes hardware-based encryption engines to accelerate cryptographic operations and offload processing from the main CPU.

7. Secure Key Management: Implements secure key storage and management mechanisms to protect encryption keys from unauthorized access or tampering.

8. Configurable Modes of Operation: Supports various modes of operation, including CTR (Counter Mode) and GCM (Galois/Counter Mode) to accommodate different encryption requirements.

9. For Silicon IP - Flexible Integration: Compatible with a wide range of processor architectures, FPGAs with ARM and RISC V core, including, but not limited to Intel-Altera, AMD-Xilinx and so on, and system-on-chip (SoC) designs, facilitating easy integration into existing hardware platforms.

10. Comprehensive Documentation: Includes detailed documentation, reference designs, and integration guidelines to simplify the integration process and accelerate time-to-market.

- Action 1: Initialise AES and Perform key exchange
- Action 2: Do AES CTR mode encryption/decryption only

EMAIL: info@pantherun.com
WEB: http://www.pantherun.com

AES Encryption IP

Applications

• Cameras & Image Handling
• Internet of Things (IoT) Devices
• Edge Computing Systems
• Cloud Infrastructure
• Network Security Appliances
• Storage Devices
• Communication Networks
• Automotive Networks

Benefits

• Data Security: Provides robust encryption to protect sensitive information from unauthorized access and data breaches.
• Performance: Delivers high-speed encryption and decryption capabilities to ensure efficient data processing.
• Power Efficiency: Minimizes energy consumption for battery-powered and low-power devices.
• Scalability: Supports multiple key lengths and configurable modes of operation to meet diverse security requirements.
• Integration: Easy integration into hardware platforms with comprehensive documentation and reference designs.

Technical Specifications(CTR)

• Encryption Algorithm: Advanced Encryption Standard (AES)-CTR mode
• Key Lengths: 128, 192, and 256 bits
• LUTs used: < 4K
• BRAM used: 18
• PL Clock: 125 MHz
• PS Clock: 600 MHz
• Throughput : 216Mbps
• Footprint: TBD
• Supported Standards: NIST FIPS 197

Technical Specifications(GCM)

• Encryption Algorithm: Advanced Encryption Standard (AES)-GCM mode
• Key Lengths: 128, 192, and 256 bits
• LUTs used: < 10K
• BRAM used: 23
• PL Clock: 125 MHz
• PS Clock: 600 MHz
• Throughput : 3Mbps
• Footprint: TBD
• Supported Standards: NIST SP 800-38D

Certifications

• Compliance with National Institute of Standards and Technology (NIST) standards for AES encryption.

Ordering Information

	Description	SKU
Chip with IP	10/100/1G AES for 1 port	CIP-AES-1
Only IP	10/100/1G AES for 1 port	NIP-AES-1
Soft IP	10/100/1G AES for 1 port	SIP-AES-1

Contact Information

For inquiries or to request a demonstration of our AES Encryption IP, please contact:
Company Name: Pantherun Technologies Private Limited
Address:311, 6th Main Road, HAL 2nd Stage,
Bangalore – 560038
Phone Number: +91 80 4164 4148
Email Address: info@pantherun.com
Website: https://www.pantherun.com/

Disclaimer

The information provided in this datasheet is subject to change without notice. Please contact us for the most up-to-date specifications and availability of our AES Encryption IP.