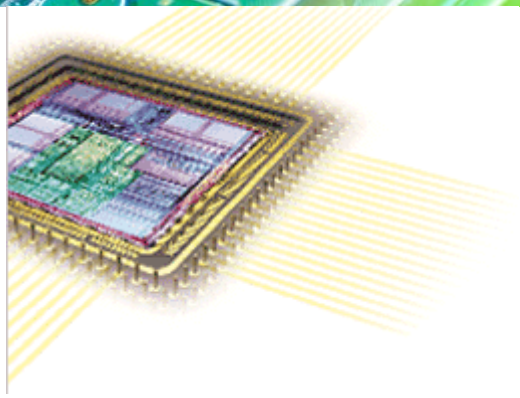
ntAES128

AES Codec with 128-bit datapath



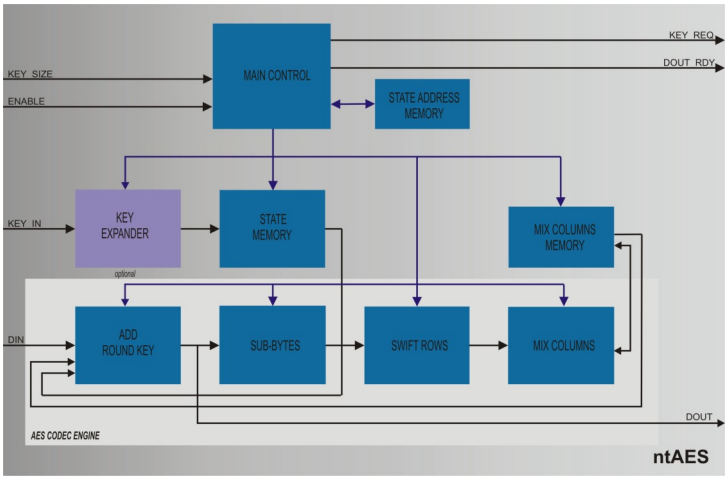
ntAES128 core implements the NIST FIPS-197 Advanced Encryption Standard and can be programmed to either encrypt or decrypt 128-bit blocks of data using a 128-bit, 192-bit or 256-bit key. The ntAES128 has been carefully designed for high throughput applications with optimal logic resources utilization. The encryptor core accepts a 128-bit plaintext input word, and generates a corresponding 128-bit ciphertext output word using a supplied 128, 192, or 256-bit AES key. The decryptor core provides the reverse function, generating plaintext from supplied ciphertext, using the same AES key as was used for encryption. The hardware roundkey expansion logic has been designed as a discrete building block. This allows either to build a complete stand-alone AES solution, or to save logic resources by leaving the key generation process to the user. Alternatively, the roundkey expansion logic can be shared between multiple encryption/decryption cores for optimal silicon area resources utilization. The implementation is very low on latency, high speed with a simple interface for easy integration in SoC applications.

Applications

The ntAES128 core can be used in a variety of applications, including:

- Electronic financial transactions.
  eCommerce, Banking, Securities exchange, Point-of-Sale
- Secure communications.
  Storage Area Networks (SAN), Virtual Private Networks (VPN)
  Video Conferencing, Voice services
- Secure environments.
  Satellite communications, Surveillance systems, Network appliances
- Personal mobile communications.
  Video phones, PDA, Point-to-Point Wireless

Block Diagram



Features

- Compliant to Advanced Encryption Standard (AES) (FIPS PUB 197).
- Supports both encryption and decryption functions.
- Supports 128/192/256-bit Cipher keys.
- 128-bit data block.
- Supports ECB, CBC, CFB, OFB and CTR modes.
- Optional Key Expansion module.
- Supports I/O data flow control capability.
- Exhibits highly optimized performance-silicon area ratio.
- Ideal for high throughput rate applications.
- Fully synchronous design.
- Silicon proven in ASIC and FPGA technologies for a variety of applications.

Implementation results

The core has been targeted to both ASIC and FPGA technologies for various applications. Noesis Technologies can also deliver netlist versions of the core optimized to specific area resources and performance requirements.

Silicon Vendor	Device	Resources	Fmax (MHz)
Xilinx	Virtex 5	365 CLB Slices / 6 Block RAMs	193

Key size	Throughput rate [1]
128 bits	2.25 Gbps
192 bits	1.875 Gbps
256 bits	1.607 Gbps

1. Throughput rates are for Xilinx Virtex-5 technology.

Deliverables

Noesis has engaged an "open" licensing philosophy in order to allow maximum technology transfer to our client's engineering teams and to facilitate the integration of our IP cores into our client's product. Various licensing models are available. The ntAES128 core is available as a soft core (synthesizable HDL) or as a firm core (netlist for FPGA technologies). The following deliverables are included:

- Fully commented synthesizable VHDL or Verilog source code or FPGA netlist.
- VHDL or Verilog test benches and example configuration files.
- C++ model.
- Comprehensive technical documentation.
- Technical support.

Support

Technical support by phone or email is included. First year of maintenance is also included. Additional support and annual maintenance options are available.

Ordering information

To purchase or make any further inquiries about our ntAES128 core, or any other Noesis Technologies products or services, contact us at info@noesis-tech.com. Noesis Technologies products are purchased under a License Agreement, copies of which are available on request.

Noesis Technologies L.P.
Patras Science Park
Stadiou Rd, Platani Rion
GR-26504 - Patras
GREECE
Phone: +30 2610 911531
Email: info@noesis-tech.com

NOESIS TECHNOLOGIES

www.noesis-tech.com