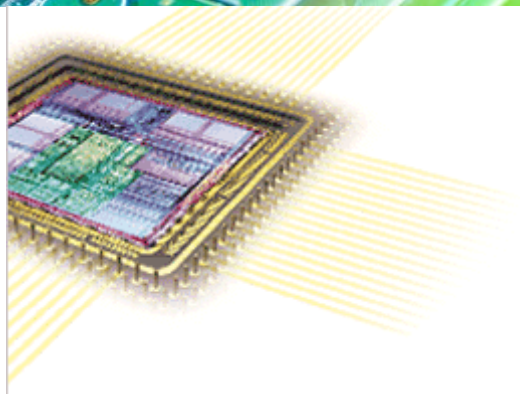
ntAES8

AES Codec with 8-bit datapath



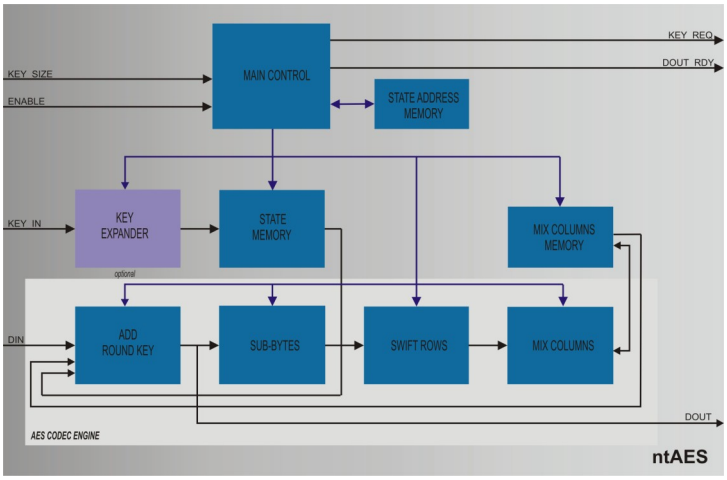
ntAES8 core implements the NIST FIPS-197 Advanced Encryption Standard and can be programmed to either encrypt or decrypt 128-bit blocks of data using a 128-bit, 192-bit or 256-bit key. The ntAES8 has been carefully designed to require minimum logic resources rendering it an ideal solution for low power applications. This has been achieved by using an 8-bit data path size which means that 16 clock cycles are required to load/unload the 128-bit plaintext/ciphertext block. The encryptor receives the 128-bit plaintext block in 8-bit input symbols and generates the corresponding 128-bit ciphertext block in 8-bit output symbols using a supplied 128, 192, or 256-bit AES key. The pre-computed key values are read from an internal round key RAM. A key expander module is provided as an optional module to allow automatic generation and loading of the round key RAM. The decryptor implements the reverse function, generating plaintext from supplied ciphertext, using the same AES key as was used for encryption. The implementation is very low on latency, high speed with a simple interface for easy integration in SoC applications.

Applications

The ntAES8 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.
- Processes an 128-bit block in 480/582/684 clock cycles for 128/192/256-bits cipher keys respectively.
- 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 low-power 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 [1]	Fmax (MHz)
Xilinx	Spartan 3	160 CLB Slices / 1 Block RAM	200
TSMC	0.18 um	1226 gates [1] / 7680 RAM bits	515

1. Equivalent NAND2 gate count.

Key size	Throughput rate [2]
128 bits	53.3 Mbps
192 bits	44 Mbps
256 bits	37.4 Mbps

2. Throughput rates are for Xilinx Spartan-3 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 ntAES8 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 ntAES8 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