**Neosyn · IP Core**

DATASHEET · REV A (PRELIMINARY)

# AES

AES-128/192/256 encryption & decryption core

• PRODUCTION READY

Product code: NSN-SEC-AES · Implemented in C⏚ · Source-included · Verilog / VHDL output

The Neosyn AES core implements the Advanced Encryption Standard (FIPS 197) for all three key sizes — 128, 192 and 256 bits — with a pipelined datapath tuned for FPGA resources.

It performs both encryption and decryption on 128-bit blocks. Written in readable C⏚ and shipped with source, the implementation is fully auditable — important for security review — rather than an opaque encrypted netlist.

The block core is intended to be composed with an external mode of operation (CBC, CTR, GCM, …) chosen by the integrator.

### KEY FEATURES

- AES-128 / 192 / 256
- Encryption & decryption
- Pipelined datapath
- FPGA-optimized
- FIPS-197 verified
- Readable C⏚
- Vendor-independent RTL
- Source-included

## Architecture

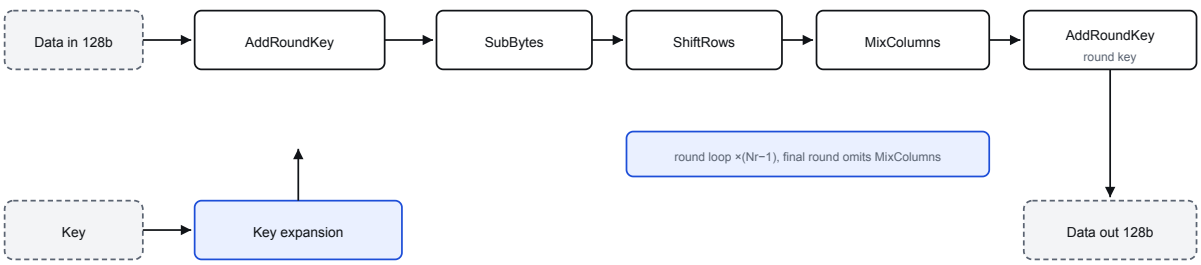


Figure 1. AES round datapath. Each round applies SubBytes, ShiftRows, MixColumns and AddRoundKey; the key-expansion block supplies per-round keys. The final round omits MixColumns.

# 1 Overview

The core implements the AES block cipher per FIPS 197. A key-expansion block derives the round keys from the 128/192/256-bit cipher key; the round datapath applies the standard transformations — SubBytes, ShiftRows, MixColumns and AddRoundKey — over the standard number of rounds for the selected key size.

The pipelined organisation is tuned to balance throughput against FPGA resource usage. Decryption applies the inverse transformations.

# 2 Features

- **Key sizes.** AES-128, AES-192 and AES-256.
- **Operations.** Encryption and decryption of 128-bit blocks.
- **Architecture.** Pipelined round datapath with hardware key expansion, optimised for FPGA resources.
- **Auditable.** Readable C⏚ source — reviewable for security assurance.
- **Composable.** Block core; chain externally for CBC/CTR/GCM modes.
- **Portability.** Vendor-independent RTL generated from C⏚.

# 3 Functional description

Refer to Figure 1.

## 3.1 Key expansion

The cipher key (128/192/256-bit) is expanded into the per-round key schedule used by every AddRoundKey step.

## 3.2 Round datapath

Each round applies SubBytes (S-box substitution), ShiftRows, MixColumns and AddRoundKey. An initial AddRoundKey precedes the rounds, and the final round omits MixColumns, per the standard.

## 3.3 Decryption

Decryption applies the inverse transformations (InvSubBytes, InvShiftRows, InvMixColumns) with the round keys applied in reverse order.

> **Security note.** The core implements the AES primitive only. Mode of operation, IV/nonce management and key handling are the integrator’s responsibility.

## 4 Interfaces & signals

The core exposes data and key inputs and a data output, with handshake.

| GROUP | DIRECTION | DESCRIPTION |
|---|---|---|
| Data in | in | 128-bit block, streaming with handshake |
| Key | in | 128 / 192 / 256-bit cipher key |
| Mode | in | Encrypt / decrypt select, key-size select |
| Data out | out | 128-bit result block, with handshake |
| Clock / reset | in | Core clock domain and synchronous reset |

Detailed signal-level pinout (per-bit widths, polarities, timing) is available on request and ships with the core.

## 5 Standards compliance

| ITEM | DETAIL |
|---|---|
| Cipher | AES — FIPS 197 |
| Key sizes | 128 / 192 / 256-bit |
| Block size | 128-bit |
| Operations | Encryption and decryption |
| Modes | Block core (chain externally for CBC/CTR/GCM) |

## 6 Performance

| PARAMETER | VALUE | NOTES |
|---|---|---|
| Block size | 128-bit | |
| Throughput | Available on request | pipelined; per configuration |
| Latency | Available on request | per key size |
| Max clock ($f_{MAX}$) | Available on request | per target device |

## 7 Resource utilization

Representative utilization per target FPGA family is provided on request from current synthesis reports.

| TARGET FAMILY | LUTS / CELLS | REGISTERS | BLOCK RAM | $F_{MAX}$ |
|---|---|---|---|---|
| Lattice ECP3 | on request | on request | on request | on request |
| AMD/Xilinx 7-series | on request | on request | on request | on request |
| Intel Cyclone | on request | on request | on request | on request |

Figures are supplied per project from characterised synthesis runs to avoid quoting unverified numbers.

## 8 Verification & validation

- Validated against the FIPS-197 known-answer test vectors.
- Encrypt/decrypt round-trip verified across all three key sizes.

## 9 Deliverables

- C⏚ source for the core (readable, modifiable)
- Generated synthesizable Verilog (VHDL on request)
- Self-checking testbench
- Integration guide and this datasheet
- Email integration support per the licensed tier

## 10 Ordering & licensing

| ITEM | DETAIL |
|---|---|
| Product code | NSN-SEC-AES |
| License | Single-project or perpetual; full C⏚ source included |
| Pricing | Quoted per use (project, volume, support tier) — contact Neosyn |
| Support | Email integration support; custom development available |
| Contact | neosyn.io/contact · info@neosyn.io |

## 11 Revision history

| REV | DATE | CHANGE |
|---|---|---|
| A | 2026 | Preliminary datasheet (Neosyn / C⏚ release). |