

The Advanced Encryption Standard (AES) has been standardized by NIST through the FIPS-197 standard. It has become the cornerstone of cryptography and is now included in 802.11i, WiMAX, SSL, IPsec and many other applications. The CLP-48f core is a fully proven block available for immediate licensing.

Key Features:

- Supports encrypt operation in ECB mode
- Decrypt only and encrypt/decrypt optionally available
- CBC, CCM, GCM, XCBC and XTS versions optionally available
- Hardware key expander available
- Support for 128-, 192- and/or 256-bit keys
- 128-bit data interface
- Verified through the National Institute of Standards and Technology (NIST) Crypto Algorithm Program (CAVP)
- Fully compliant with NIST FIPS-197
- Ellipsys Security Architecture (ESA) software offers a complete suite of security solutions for embedded applications

Applications:

- IPsec and SSL designs in residential gateways, multi-service access products
- Storage – SAN/NAS applications
- Wireless applications such as 802.11i and 802.16
- Military communications systems
- Secure video surveillance
- Secure audio communications

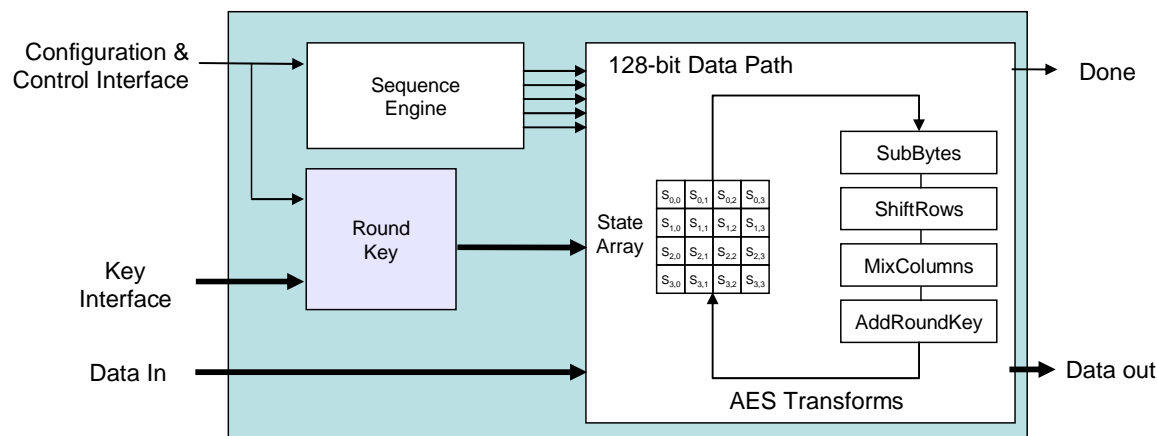


Figure 1 CLP-48f Block Diagram

General Description

The Advanced Encryption Standard (AES), a subset of the Rijndael algorithm, has been standardized by NIST through FIPS-197. The AES algorithm is a 128-bit block cipher that supports three different key sizes: 128-, 192-, and 256-bits.

The CLP-48f implementation fully supports the AES algorithm for any or all three key sizes. The base core supports Electronic Code Book (ECB) in encrypt only mode. It can be optionally augmented to support Cipher Block Chaining (CBC), Counter Mode (CTR), Counter Mode with CBC-MAC (CCM), Galois Counter Mode (GCM), XCBC mode for cipher based hash applications and storage security through XTS mode..

The base CLP-48f core offers the following performance in target Xilinx FPGAs:

Part Number	Family	Maximum Clock Frequency (MHz)	Encryption Throughput (Mbps)
5vlx50-3	Virtex 5	213	2471
xc4vlx160-12	Virtex 4	205	2354
xc3s5000-5	Spartan 3	148	1195

A reference synthesis result for a Xilinx Virtex-5 FPGA is shown in the table below. Resource requirements for other FPGAs and configurations are available upon request

Family	Example Devices	F _{max} ¹ (MHz)	LUTs	Occupied Slices	GCLK	BRAM	Design Tools
Virtex-5	XC5VLX50-3	213	785	287	1	4	ISE 10

Notes: 1. F_{max} is quoted assuming all core inputs are driven by flip-flops and all core outputs drive flip-flops in order to present realistic application data

The CLP-48f is a member of a broad range of security cores available from Elliptic Technologies. Please contact us for further information for cores that range from small footprint designs to ultra-high throughput capability all available in Xilinx FPGAs. The CLP-48f is available as soft IP in HDL format. The deliverables offered include:

HDL Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script
- Documentation

Ellipsys Security Architecture

The Ellipsys Security Architecture offers security software which can assist with system development. The architecture is pictured below and consists of five distinct products encompassing symmetric and asymmetric cryptography primitives, secure boot, Linux IPsec and a DTCP stack. The architecture offers a well defined, uniform API blending industry standard PKCS#11 with Ellipsys extensions in support of third party applications software. The Ellipsys Security Architecture can be adapted to support hardware offload including the core featured in this product brief. Ellipsys is written to be highly portable and is licensed in C source code.

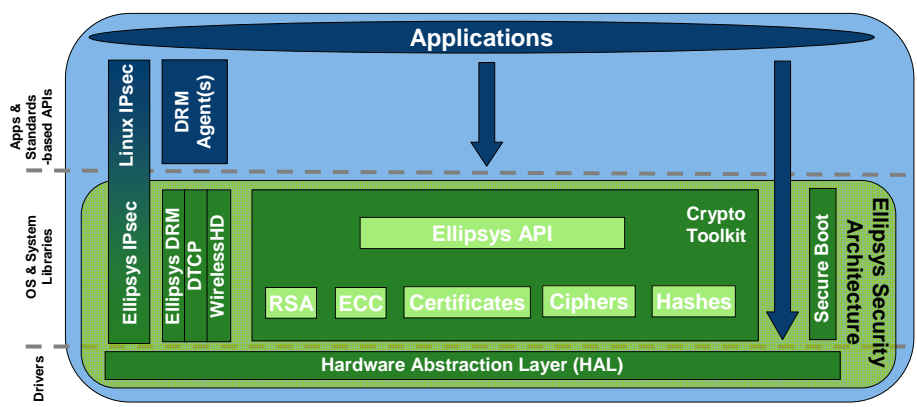


Figure 2 Ellipsys Security Architecture

For more information, please contact Elliptic Technologies at:

© Elliptic Technologies Inc.
62 Steacie Drive, Suite 201
Ottawa, ON, K2K 2A9

Phone: +1 613 254-5456
Fax: +1 613 254-7260
Email: info@elliptictech.com