



Embedded security you can trust

High Perf AES-CCM Core

CLP-20 Product Brief

Features

- Single and dual core options to tailor to a specific throughput and latency
- Single core gate count of 27k ASIC gates
- Dual core gate count of 53k ASIC gates
- Key expansion options available
- Support for AES Counter Mode Encryption (CTR) operation with CCM extensions
- 128 bit keys only extensible to 192 and 256 bit keys if required
- Optional interfaces include FIFO and dual-port RAM
- Test bench provided

Applications

AES-CCM has been chosen as the standard authenticating cipher for all wireless applications. To address the need for designs that encompass throughput up to 800 Mbps and low, predictable latency for multimedia services, Elliptic has created the CLP-20 to address this market need.

The core is based upon Elliptic's high performance, silicon proven AES multi-mode core and has been tailored specifically to the needs of the wireless standards being addressed in new designs.

General Description

The Advanced Encryption Standard (AES), is based on the Rijndael algorithm, has been standardized by NIST to replace DES which is no longer considered secure.. The AES algorithm is a 128 bit block cipher and supports three different key sizes; 128, 192, and 256 bits. The IEEE 802.11i standards body has selected AES with 128 bit key size in Counter Mode with CBC-MAC extensions and this algorithm is now used in all wireless applications as a universal standard. The CLP-20 implementation supports this requirement at speeds reaching beyond 1 Gbps.

Throughput

The CLP-20 can be synthesized in either a single core or dual implementation. Dual core designs obviously result in higher gates counts but by operating one core for the encryption and decryption operation and the other core in authentication mode, the latency and throughput can be substantially improved. The table below illustrates the trade-offs in gate count versus performance in reference to common applications of the core:

AES-CCM Configuration	Target Specification	AES-CCM Throughput@ Specified Clk Freq (bits/sec)	Clk Frequency (MHz)	Latency (clock cycles)
		Encrypt/Decrypt with H/W Key Expansion for 128 bits of AAD and 16256 bits of message data		
AES-CCM Single Core	802.11a,b,g	200 M	36	22
	802.11n	500 M	89	
	802.15.3	800 M	143	
AES-CCM Dual Core	802.11a,b,g	200 M	19	12
	802.11n	500 M	46	
	802.15.3	800 M	73	





Embedded security you can trust

High Perf AES-CCM Core

CLP-20 Product Brief

General Description cont'

Key Expansion Options

Elliptic offers a variety of key expander options for the CLP-20 as outlined below:

1. For customers that want to use the core with a fixed key that seldom changes, the key expansion can be done in an embedded processor and the expanded key stored in registers for use by the CLP-20.

2. Elliptic also offers a low speed key expander which occupies only 1000 ASIC gates. This option also requires registers to store the expanded key.

3. Finally for high performance applications where keys are rotated or multiple key contexts must be provided to the core, a high speed key expander is available.

The table below illustrates the choices that a designer has in key expansion options.

The choice of key expander options can be discussed with Elliptic applications engineering to determine which choice is appropriate for the application that the SoC is targeted at.

Key Expander Implementation	ASIC Gate Count (NAND2 Equivalent Gates)
Software	0 ¹
Compact Key Generator	1000 ²
Fast Key Generator 128-bit Key Size	9000

¹ Memory for key storage required.
² Key and cipher computations share a common S-box. This gate count value does not include S-box and dedicated memory gate count.

The CLP-20 is part of a complete family of AES cores that range from small gate counts and moderate throughput to very wide data path cores capable of Gbps operation. Please see the Elliptic web site for more information.

Other Products of the Family of AES Cores

- CLP-11: Tiny AES Core
- CLP-15: Ultra-High Throughput AES-GCM Core - 40 Gbps
- CLP-16: Ultra-High Throughput AES-GCM Core - 10 Gbps
- CLP-24: High Throughput AES-GCM Core - 5 Gbps
- CLP-28: 802.16/WiMAX AES Core
- CLP-33: XTS-AES Core
- CLP-34: AES Key Wrap Core
- CLP-45: Configurable Lookaside AES Core
- CLP-47: Configurable XTS-AES Core

Availability

The CLP-20 is available in soft IP form HDL Source. The deliverables available are:

HDL Source Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script & constraints
- Sample simulation script
- Documentation