



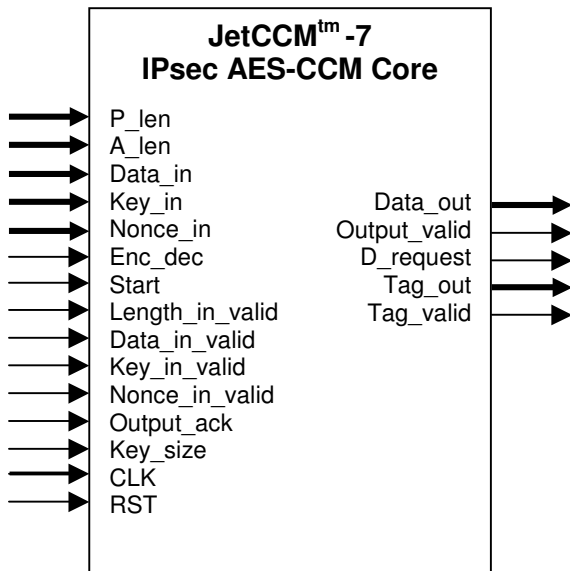
Overview

IETF RFC4309 standard defines IPsec security payload by utilizes the NIST standard AES in CCM mode for both encryption and message authentication. The CCM mode uses AES and combines the counter mode of encryption with the CBC-MAC mode of authentication.

The **JetCCMtm-7** core is optimized for RFC4309 IPSEC applications. The core includes our fully verified JetAEStm cryptographic core and supports encryption, decryption, authentication, and verification functionalities. Its design is fully synchronous for portability. The core is available for licensing in both source and netlist form.

Application

IPsec, Virtual Private Networks (VPN)



Features

- Fully compliant with IPsec AES-CCM mode
- High throughput > 2 Gbps
- Simple interface
- Fully synchronous design
- Flow-through design
- Combine both AES-CCM encryption-authentication and decryption-verification
- Support all three AES key sizes based on IPsec requirements
- On-the-fly hardware key expansion
- Key expansion can also be performed in software to reduced the gate count
- Core is available as a synthesizable Verilog source code, or as a netlist
- Self-checking test bench

General Description

Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by NIST to replace DES. DES is now considered to be insecure for many applications.

CCM mode (Counter with CBC-MAC) is a mode of operation for use with block cipher such as AES. CCM mode combines the counter mode of encryption with the CBC-MAC mode of authentication.

IPsec defines security infrastructure to provide data confidentiality, data integrity and data authentication for Internet Protocol (IP) communications. IPsec secures network operation by protecting traffic on an end-to-end basis. IETF RFC4309 standard specifies AES-CCM mode for IPsec encapsulating security payload (ESP). The security payload utilizes AES-CCM with 128, 192 or 256-bit key sizes.

JetCCM[™]-7 core is an AES-CCM core optimized for IETF RFC4309-based IPsec applications and includes the fully verified JetAES[™] cryptographic module. The core supports encryption, authentication, decryption, and verification functionalities. It implements a 128-bit wide data path and 128-bit wide data interfaces.

JetCCM[™]-7 core supports all three key sizes based on RFC4309 requirements. The core is implemented for flow-through operation. Its design is fully synchronous for portability.

The key expansion logic inside the core works as a standalone block which can generate the AES roundkeys on-the-fly. If the input key does not change frequently, then the roundkeys can be pre-expanded and stored in memory by the Key Expansion Logic. Alternatively, the roundkeys can also be generated and stored in memory by an embedded processor. Thus, these options can further reduce gate count.

Core I/O

The core I/O signals of the JetCCM[™]-7 core with hardware on-the-fly key expansion for the 256-bit key size are described in the table below.

Signal	I/O	Width	Description
CLK	Input	1	Master clock
RST	Input	1	Master reset; 1 = reset
P_len	Input	32	Length of plain text in bytes
A_len	Input	64	Length of AAD in bytes
Data_in	Input	128	Data input (AAD and plaintext)
Key_in	Input	256	Key input

Nonce_in	Input	88	Nonce input
Enc_dec	Input	1	0 = Encryption; 1= Decryption
Start	Input	1	Start processing
Length_in_valid	Input	1	Length in valid signal
Data_in_valid	Input	1	Data_in valid signal
Key_in_valid	Input	1	Key_in valid signal
Nonce_in_valid	Input	1	Nonce_in valid signal
Output_ack	Input	1	Output acknowledgement
Key_size	Input	1	Select 128-bit, 192-bit or 256-bit key
Data_out	Output	128	Data output
Output_valid	Output	1	Output data valid
D_request	Output	1	Data input request
Tag_out	Ouput	128	Tag out
Tag_valid	Ouput	1	Tag valid

Implementation Results

Example ASIC implementation statistics for the JetCCMtm-7 core are shown below

Technology	Gate Count
TSMC 0.18 μ m	75436

Example implementation statistics on FPGAs for the JetCCMtm-7 core are shown below

Xilinx Family	Device	Slices	BRAM	CLK	I/O	Fmax (MHz)
Spartan-3E tm	XC3S250E-4	1567	10	1	837	106
Spartan-3 tm	XC3S200-5	1616	10	1	837	95
Virtex-II Pro tm	XC2VP2-7	1592	10	1	837	173
Virtex-4 tm	XC4VLX25-11	1630	10	1	837	249
Virtex-5 tm	XC5VLX30	591	20	1	837	294

Support

Sixty days of phone and email technical support are included. Additional maintenance and support options are available.

Verification

The JetCCMTM-7 core has been thoroughly simulated and verified on Xilinx FPGA hardware using the NIST test vectors and additional software-generated test vectors.

Deliverables

The core is available in soft IP form, either as a Netlist or HDL Source. The deliverables include:

- For **Netlist Licenses** : Target specific net list
- For **HDL Licenses** : Fully synthesizable RTL Verilog source
- Self-checking test bench
- Simulation script, test vectors and expected results
- User documentation

Export Permits

Jetstream Media Technologies' security products are subject to the export control under the United States Bureau of Industry and Security (BIS) (www.bis.doc.gov). Customers must reference the U.S. rules governing exports and re-exports of encryption items specified in the Export Administration Regulations (EAR) (<http://www.access.gpo.gov/bis/index.html>), and consult with their legal advisors to determine if licenses are required. Please also refer to the export information page in our web site.

More Information

For more detailed information on this or any of our other products and services, please contact us and we will be pleased to discuss how we can assist with your individual requirements.

www.security-cores.com

or

www.jetsmt.com

Jetstream Media Technologies
800 W. 5th Ave.
Naperville, IL 60563 U.S.A.
Tel: 1 (630)-301-4778
Email: sales@jetsmt.com