



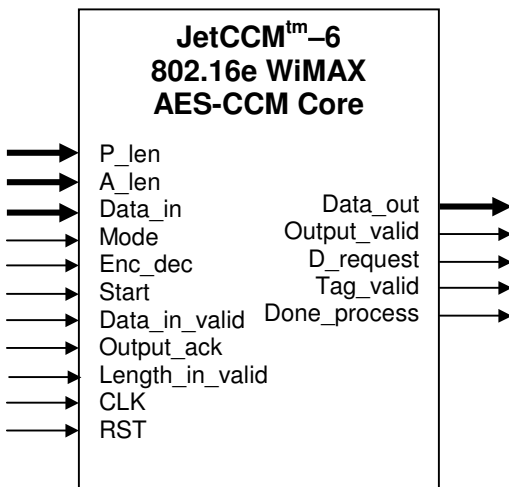
Overview

The WiMAX security standard IEEE 802.16e utilizes the NIST standard AES in CCM mode. The CCM mode combines the counter mode of encryption with the CBC-MAC mode of authentication and uses 128-bit key AES. WiMAX security also specifies the use of additional data encryption / authentication methods, including AES in CTR mode and AES CMAC.

The **JetCCM™-6** core is optimized for 802.16e applications by supporting the various AES modes. The core includes our fully verified JetAES™ 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

WiMAX IEEE802.16e



Features

- Small size
- 802.16e data rates supported
- Simple interface
- Fully synchronous design
- Flow-through design
- Support AES-CCM mode
- Support AES-CTR mode
- Support AES CMAC
- Combine both encryption-authentication and decryption-verification
- Support 128-bit key size based on 802.16e requirements
- 16-bit wide data path single core design
- 8-bit and 32-bit wide designs are also available for well-matched solutions
- On-the-fly hardware key expansion
- Key expansion can also be done 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 (RFC 3610). CCM mode combines the counter mode of encryption with the CBC-MAC mode of authentication.

WiMAX is a broadband wireless metropolitan area networks standard. The WiMAX security sublayer specified in IEEE 802.16e-2005 standard, defines security aspect of wireless metropolitan area networks and addresses the weaknesses in the original WiMAX security scheme.

WiMAX security sublayer in 802.16e specifies several data encryption methods, including AES in CCM mode with the 128-bit key size. For Multicast Broadcast Service (MBS) payload, data encryption method utilizes AES in CTR mode. WiMAX management message integrity protection uses AES CMAC as specified in NIST 800-38B.

JetCCMTM-6 core is an AES-CCM core optimized for 802.16e WiMAX applications and includes the fully verified JetAESTM cryptographic module. The core supports AES in CCM mode, AES in CTR mode and AES CMAC, all with 128-bit key. It performs encryption, authentication, decryption, and verification functionalities. The core implements a 16-bit wide data interface and 16-bit wide data path. 8-bit and 32-bit wide designs are also available for well-matched solutions. Both encryption and authentication are processed by a single AES module to minimize gate count. The 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 JetCCMTM-6 core with hardware on-the-fly key expansion for the 128-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	16	Length of plain text in bytes
A_len	Input	16	Length of AAD in bytes

Data_in	Input	16	Data input (AES Key followed by Nonce, AAD and Plaintext)
Mode	Input	2	AES mode selection
Enc_dec	Input	1	0 = Encryption; 1= Decryption
Start	Input	1	Start processing
Data_in_valid	Input	1	Data input valid signal
Length_in_valid	Input	1	Length_in valid signal
Output_ack	Input	1	Output acknowledge
Data_out	Output	16	Data output
Output_valid	Output	1	Output data valid
D_request	Output	1	Data input request
Tag_valid	Output	1	Tag output valid
Done_process	Output	1	Done processing data of the specified length

Implementation Results

Example ASIC implementation statistics for the JetCCMtm-6 core are shown below

Technology	Gate Count
TSMC 0.18 μ m	15668

Example implementation statistics on FPGAs for the JetCCMtm-6 core are shown below

Xilinx Family	Device	Slices	BRAM	CLK	I/O	Fmax (MHz)
Spartan-3E tm	XC3S250E-4	779	3	1	54	87
Spartan-3 tm	XC3S200-5	775	3	1	54	93
Virtex-II Pro tm	XC2VP2-7	752	3	1	54	197
Virtex-4 tm	XC4VLX25-11	793	3	1	54	204
Virtex-5 tm	XC5VLX30	238	3	1	54	316

Support

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

Verification

The JetCCMTM-6 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