



AES Core G2, Xilinx Edition

March 5, 2006

Product Specification

Algotronix®

PO Box 23116
 Edinburgh, Scotland
 United Kingdom, EH8 8YB
 Phone: +44 131 556 9242
 Fax: +44 870 052 5069
 E-mail: cores@algotronix.com
 URL: www.algotronix.com

Features

- Highly flexible design configured using VHDL generic parameters
- Available under terms of the SignOnce IP License
- Cost effective, royalty free licence terms
- Full Implementation of FIPS 192
 - 128, 192 and 256 bit keys
 - Encrypt only, Decrypt only or Encrypt/Decrypt
- Full Implementation of SP800-38A Modes – ECB, CBC, OFB, CTR, CFB1, CFB8, CFB128
- Full Implementation of AESAVS testbench
 - Regression Mode for confirming design functionality
 - Qualification Mode for generating response files for certification lab.
- Supplied as VHDL source code to allow full security review

Table 1: Example Implementation Statistics – ECB, Encrypt Only, 128 bit key, Hardware Key Expansion, 'Push Button' flow with clock constraint

Family	Example Device	Fmax (MHz)	Slices ¹	I/O ²	GCLK	BRAM	MULT/DSP48	DCM	Throughput (MBit/sec)	Design Tools
Spartan-3™	XC3S200-5	100	321	105	1	3	0	0	290	ISE 8.1.01i
Spartan-3E™	XC3ES250-5	100	341	105	1	3	0	0	290	ISE 8.1.01i
Virtex-II Pro™	XC2VP2-5	130	311	105	1	3	0	0	378	ISE 8.1.01i
Virtex-4™	XC4VLX15-12	180	380	105	1	3	0	0	523	ISE 8.1.01i

Notes:

- 1) Actual slice count dependent on percentage of unrelated logic – see Mapping Report File for details
- 2) Assuming all core I/Os and clocks are routed off-chip, which is not the intended usage. The core interface is designed to provide flexibility inside a larger FPGA design. 'Processor Interface' reference design interfaces the core to a data bus and substantially reduces pin count.

Core Facts	
Provided with Core	
Documentation	User Manual
Design File Formats	VHDL or EDIF Netlist
Verification	Test Bench, Test Vectors
Instantiation templates	VHDL
Reference designs & application notes	'Getting Started', Processor Interface
Additional Items	'Getting Started' Sample design demonstrates core on Xilinx Spartan 3 Eval Board
Simulation Tool Used	
Model Tech ModelSim XE, Aldec Active HDL	
Support	
Support provided by Algotronix	

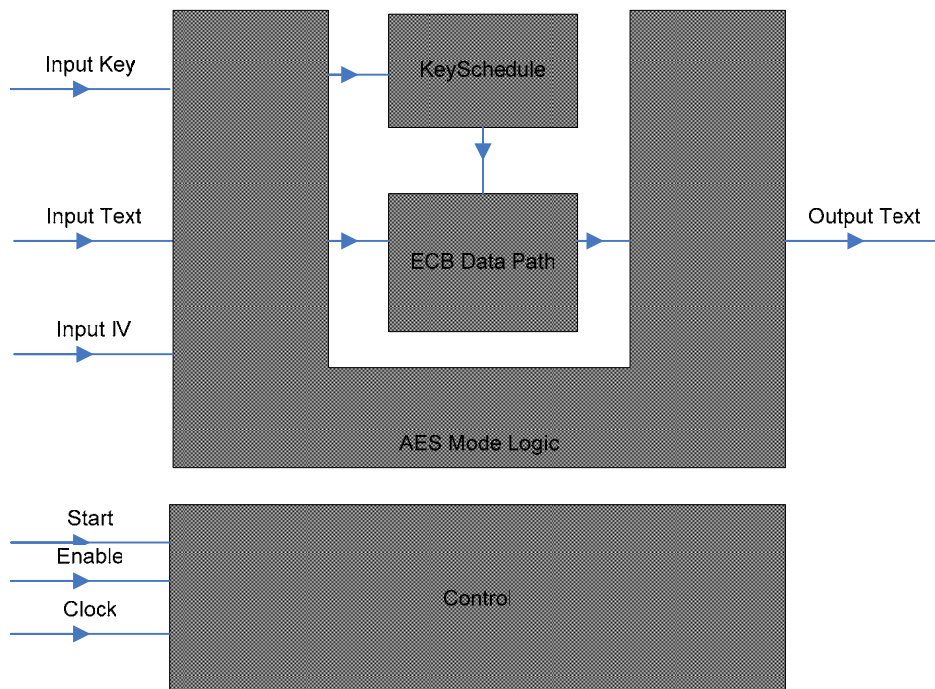


Figure 1: AES Core Block Diagram

Applications

Secure Wireless Communications

- Government/Military
- IEEE 802.11 Wireless LAN, 802.15 PAN and 802.16 MAN
- Satellite

Secure Wireline Communications

- Virtual Private Network (VPN)
- Voice over IP (VoIP)
- Powerline networks

Secure Computer Systems

- Gaming Machines
- Storage Area Networks (SAN)
- Digital Rights Management (DRM)
- Financial Applications

General Description

The Algotronix G2 AES Core is the second generation of a comprehensive, production tested, medium speed (32 bit internal data path) implementation of the NIST Federal Information Processing Standard 197 (FIPS197). It supports all the key lengths specified in the standard (128, 192 and 256 bits) and all the modes of use specified in NIST SP800-38A – ECB, CBC, OFB, CTR, CFB1, CFB8 and CFB128. The core is supplied with a comprehensive testbench which implements the NIST AESAVS test suite for AES. The testbench can be used in regression mode to verify changes to the source code or in Qualification mode to generate response files for a NIST approved laboratory.

The Algotronix AES core is supplied as VHDL source code and can be configured using a number of VHDL generic parameters to select only those features which are required in order to conserve area. The core can be configured as Encryptor, Decryptor or Encryptor/Decryptor and the maximum key length and supported modes can also be selected. The core can be configured to generate the key schedule in hardware or to save area a software generated key schedule can be loaded. This level of flexibility makes it easy to experiment with area/performance/functionality tradeoffs and makes it highly likely that the core will be useful in multiple projects. The flexible nature of the core makes multi-project site licences particularly attractive.

The AES core is an easy to use fully synchronous design with a single clock and an enable signal to allow the core to be started and stopped on a clock cycle by clock cycle basis to match up with external data sources. The core has been designed for efficiency in Xilinx FPGAs and makes full use of FPGA specific features such as dual port memory blocks.

Functional Description

The main functional blocks as shown in Figure 1 block diagram.

ECB Data Path

This block implements the ECB mode of the AES Algorithm. All other modes of AES are built on top on this basic encryption operation.

Key Schedule

This block calculates the round keys for each stage of the AES algorithm based on the key supplied by the user. A compilation option allows the user to omit this unit to save area in which case the core must be supplied with the complete keyschedule. This option may make sense if the key changes relatively infrequently and there is a microprocessor available elsewhere in the system to calculate the keyschedule.

AES Mode Logic

This block contains the feedback paths and additional logic required to implement the more complex modes of AES – CBC, OFB, CFB1, CFB8, CFB128 and CTR. Compilation parameters are supplied so only the logic for those modes which are required by the user will be instantiated.

Core Modifications

The core can be configured easily using a set of VHDL generic parameters. Normally, it is unnecessary for users to modify the design source code although the code is supplied and they are free to do so if they wish. Algotronix can also customise the core as a service for users with particular requirements which are not met by the standard product.

The following compilation options are specified by editing constant definitions in the `aes_parameters_package` file. This is the only file in the AES core release which will normally require to be edited by the user.

- **Cipher_function** - specifies whether an Encryptor, Decryptor or Encryptor/Decryptor is required.
- **Max_Crypt_Size** – specifies the maximum key length the core should implement. The user can select any key length up to and including this using control signals. For example, if `Max_Crypt_Size` is `aes256` then the core would deal with 256, 192 and 128 bit keys.
- **Implement_SBoxes_in_RAM** – specifies that FPGA RAM blocks rather than logic gates should be used to implement SBoxes and Inverse SBoxes. This is the most efficient option if RAM blocks are available after mapping the remainder of the user design.
- **Omit_ECB_Mode, Omit_CBC_Mode, Omit_OFB_Mode, Omit_CTR_Mode, Omit_CFB1_Mode, Omit_CFB8_Mode, Omit_CFB128_Mode** - Used to request that logic to support cipher modes that will not be required is omitted from the design. The CTR and CFB modes require quite large amounts of additional logic.
- **User_Calculates_Keyschedule** – specifies that the Keyschedule datapath should be omitted. Rather than providing a key the user will load a complete key schedule (i.e. all round keys) into the design. This can be a useful way to save area if the user's system has a microprocessor available to calculate the keyschedule and the key changes relatively infrequently so the time taken to calculate the keyschedule is not an issue.
- **Keyschedule_Shares_Sboxes** – specifies that the same SBoxes are used for the encryption datapath and the keyschedule unit. When this option is selected the encryption key schedule must be pre-calculated in the same way as decryption keys causing additional latency when the key is changed.
- **Force_output_low_until_valid** – When true the core will hold the output low at all times when valid output data is not present. When this signal is false the circuitry to hold the output zero will be omitted, saving some area. In this case the core output 'output_text' will show the values at intermediate rounds of the cipher as well as the final round. This data is not fully encrypted and, if available to an attacker, could compromise security of both the key and data. Therefore, this parameter should only be set to false if the user design which contains the core can guarantee that an attacker will not be able to monitor the core output directly.

Core I/O Signals

The core signal I/O have not been fixed to specific device pins to provide flexibility for interfacing with user logic. Descriptions of all signal I/O are provided in Table 2.

Table 2: Core I/O Signals.

Signal	Signal Direction	Description
clock	input	Clock – active on rising edge
clear	input	Synchronous clear of controller state and most registers (Some shift registers do not use clear to allow a more area efficient implementation).
reset	input	Asynchronous reset – active high. Usually connected to FPGA global reset.
enable	input	Module clock enable – 0: module is inactive, 1: module runs
mode	input	Mode signal – specifies which mode of AES is to be implemented. See also the omit_* compilation options in the section below. If compilation options have specified that logic for a particular mode should be omitted then incorrect behaviour will result if that mode is selected.
KeyLength	input	Specifies the length of the key that is being used – 128, 192 or 256 bits. See also the max_crypt_size compilation option. Only keys up to the size specified in max_crypt_size may be specified e.g. if max_crypt_size generates hardware for a 192 bit key then KeyLength may be 128 or 192 bits but not 256 bits.
Do_Encrypt	input	Specifies whether the core should operate in Encrypt or Decrypt mode. This input is only significant if the compilation option cipher_function is set to EncryptDecrypt i.e. hardware for both encryption and decryption has been included.
Start	input	Starts a new encryption operation or block of operations in the chained modes. The control signals Mode, KeyLength and Do_Encrypt are sampled and the parameters fixed for the next operation. The key is assumed to have changed and the keyschedule is recalculated (or loaded if the compilation option User_Calculates_Keyschedule is active).
load_text	output	Load flag – high when input_text is being loaded
Load_key	output	Load flag – high when the key is being loaded
Output_Valid	output	Valid flag – high when output_text is valid.
Advanced_Output_Valid	output	High on the four clock cycles immediately preceding output_valid. This signal gives advanced warning that the core is about to input and output data and can be used by external control circuitry to stop the core using the enable signal until the system is ready to provide new input data and accept output data.
Input_Text[31:0]	input	Data input: current 32-bit word of the 128-bit plain text
Output_Text[31:0]	output	Data output: current 32-bit word of the 128-bit cipher text
Initial_value [31:0]	input	Current 32-bit word of the 128-bit initial value for the chained modes of operation (ECB mode does not use the initial value).
Input_Key[31:0]	input	Current 32-bit word of the key – it takes 4, 6 or 8 clock cycles to load a complete key. If the compilation option User_Calculates_Keyschedule is specified the entire keyschedule is input through this signal.

Verification Methods

Algotronix supplies a comprehensive VHDL testbench for the core which supports the standard AESAVS test suite. The testbench allows simulation of the design source code and also post place and route timing simulation. The testbench can be used in Regression mode to confirm the functionality of the core against known 'golden' test vectors provided by Algotronix or in Qualification mode to generate response files from vectors supplied by a NIST approved certification laboratory.

To provide immediate confidence that the core works correctly in hardware the 'Getting Started' Application note provided with the core supplies with VHDL code and design files to demonstrate the core running on a Xilinx Spartan 3 evaluation board. This low cost board is available directly from Xilinx.

Recommended Design Experience

It is recommended that the user is familiar with the VHDL language and with the Xilinx design flow. The core can also be instantiated inside a wrapper to allow use with a Verilog design flow.

Selection of the cipher mode of use of AES has implications for overall security, ease of use and performance and it is recommended that if the user is not a specialist in cryptography advice should be taken when selecting the appropriate mode for the application.

Available Support Products

Algotronix supplies two application notes and associated source code free of charge with the core:

Getting Started: This application note is intended to be the equivalent of 'Hello World' in C – it is a very simple wrapper providing the minimum logic required to instantiate the core on an evaluation board and carry out an encryption. The results are displayed on the seven segment LEDs on the Spartan evaluation board. The getting started design is also useful as an initial 'confidence test' when bringing up the core on a new circuit board designed by the user since it requires that the board supply only a clock, a reset signal and LEDs to display the result.

Processor Interface: This application note illustrates how to control the core through a register based interface to a microprocessor. The interface also provides flow control so that the core processing will wait for the microprocessor to supply more data or read results. The processor interface design is configurable for 8, 16 or 32 bit external data busses and multiplexes several 32 bit signals on the G2 core interface onto a single data bus reducing pin requirements.

Ordering Information

This product is available directly from Algotronix under the terms of the SignOnce IP License. Please contact Algotronix for pricing and additional information about this product using the contact information on the front page of this datasheet. To learn more about the SignOnce IP License program, contact Algotronix or visit the web:

Email: commonlicense@xilinx.com
URL: www.xilinx.com/ipcenter/signonce

Export Control

Strong encryption technology such as AES is the subject of international export regulations. Algotronix is located in the United Kingdom and export of this core is regulated by the UK government.

The core is freely available within the European Union and in addition can be supplied immediately to the following countries: United States, Australia, New Zealand, Canada, Norway, Switzerland, Japan.

Export to other countries requires an export licence. The UK Department of Trade and Industry publishes information on their website (www.dti.gov.uk) which gives an indication of average export licence processing times for various countries and the percentage of licence requests which are granted. For many countries obtaining an export licence can be done relatively quickly and with only a small amount of additional paperwork.

It is the responsibility of the customer to comply with all applicable requirements with respect to re-export of products containing the AES technology.

Related Information

Industry Information

The AES standard documents FIPS197, SP800-38A and AESAVS are available from the National Institute of Standards and Technology, Computer Security Resource Center website (www.csrc.nist.gov).

Xilinx Programmable Logic

For information on Xilinx programmable logic or development system software, contact your local Xilinx sales office, or:

Xilinx, Inc.
2100 Logic Drive
San Jose, CA 95124
Phone: +1 408-559-7778
Fax: +1 408-559-7114
URL: www.xilinx.com

Copyright © 2002-2006 Algotronix Ltd., All Rights Reserved.

Algotronix® is a registered trademark of Algotronix Ltd. in the United States and United Kingdom and a trademark of Algotronix Ltd. in other countries.

The supply of the product described in this document is the subject of a separate license agreement with Algotronix Ltd. which defines the legal terms and conditions under which the product is supplied. This product description does not constitute an offer for sale, a warranty of any aspects of the product described or a license under the intellectual property rights of Algotronix or others. Algotronix products are continuously being improved and are subject to change without notice. Algotronix products are supplied 'as is' without further warranties, including warranties as to merchantability or suitability for a given purpose. Algotronix' products are not intended for use in safety critical applications.

URL: www.algotronix.com