GCM-AES Block Specification

Version 1.0.10.05.2010

By

Tariq Bashir Ahmad

Supervisor: Guy Hutchison

1.1 Introduction and Overview

GCM-AES (Galois Counter Mode – Advanced Encryption Standard) is an authenticated encryption mode designed by David McGrew and John Viega. The details of this mode of operation can be found in [2].

This document aims to explore hardware implementation of GCM-AES mode of operation specifically targeting FPGA [1] (Field Programmable Gate Arrays). The aim of such an implementation is to benchmark GCM-AES on FPGA in terms of area, power and speed.

1.2 Theory of Operation

GCM-AES has been implemented as a full duplex block which means that the design consists of separate encryption-authentication and decryption-verification blocks. Thus, it can carry out encryption-authentication and decryption-verification operations simultaneously.

1.2.1 Encryption and Authentication Block

A. The GCM-AES encryption block works on one single frame (Message + AAD) at any given time. A frame consists of one or more AAD blocks or zero or more message blocks. Specifically, the encryption block works on one message block or AAD block at any time.

B. The default block length is 128 bits.

C. A single control word starts the operation of GCM-AES encryption block with the *Setup* phase. This phase is done once per frame. After twenty clock cycles of latency incurred from the setup phase, the encryption block is ready to accept a message or AAD block.

D. The encryption block expects one or more AAD blocks where the last AAD's block length need not be 128 bits. It should however be a multiple of a byte. Similarly, the encryption block expects zero or more message blocks where the last message block length need not be the default block length. It should as well be a multiple of a byte.

E. The design requires one or more AAD blocks to be input first and then zero or more plain text blocks.

F. The current implementation is capable of handling any message or AAD blocks per frame. It takes 10 clock cycles to encrypt a message block (default block length or less than that) with 10 cycle AES-128 implementation [3] when the corresponding encrypted cipher text is produced. The GCM-AES encryption block relies on AES-128 encryption block for encryption and Galois Field multiplication for authentication. Galois Field Multiplier used in this implementation produces result in 8 clock cycles. Cipher text is not produced in case of AAD block.

G. The length of the frame does not need to be known by the encryption block. The encryption block works on a frame with the following format:

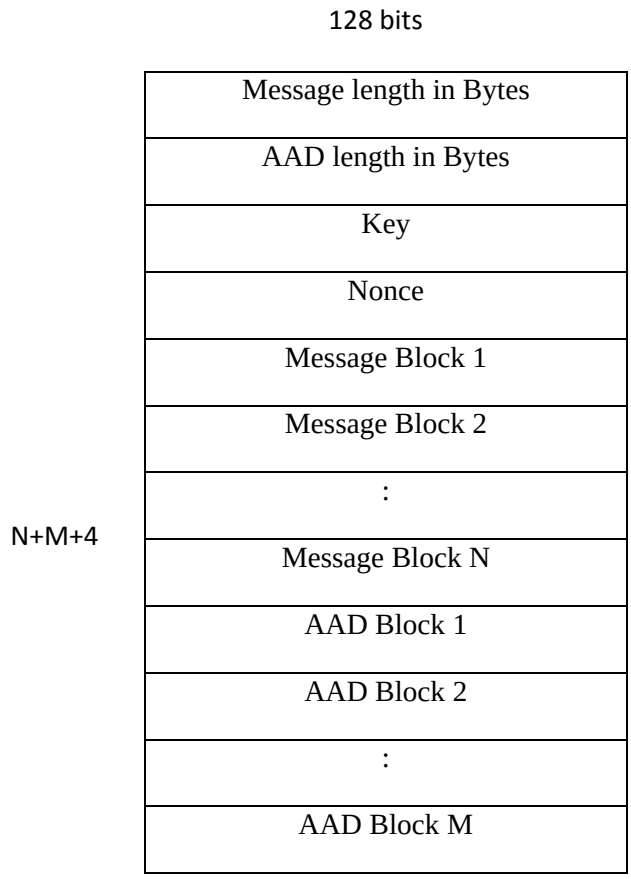

Figure 1. Frame format GCM-AES Encryption

1.2.2 Decryption and Verification Block

1. The GCM-AES decryption block is similar to GCM-AES encryption block. Thanks to Counter Mode. Tag calculation is exactly the same as GCM-AES encryption. The computed tag is compared against the provided tag. If the tags match, decrypted plain texts are considered valid.
2. The GCM-AES decryption block works on the similar frame format as GCM-AES encryption block where now Message Blocks are replaced by zero or more Cipher text blocks.

2 Interface Diagram

2.1 GCM-AES Encryption and Authentication

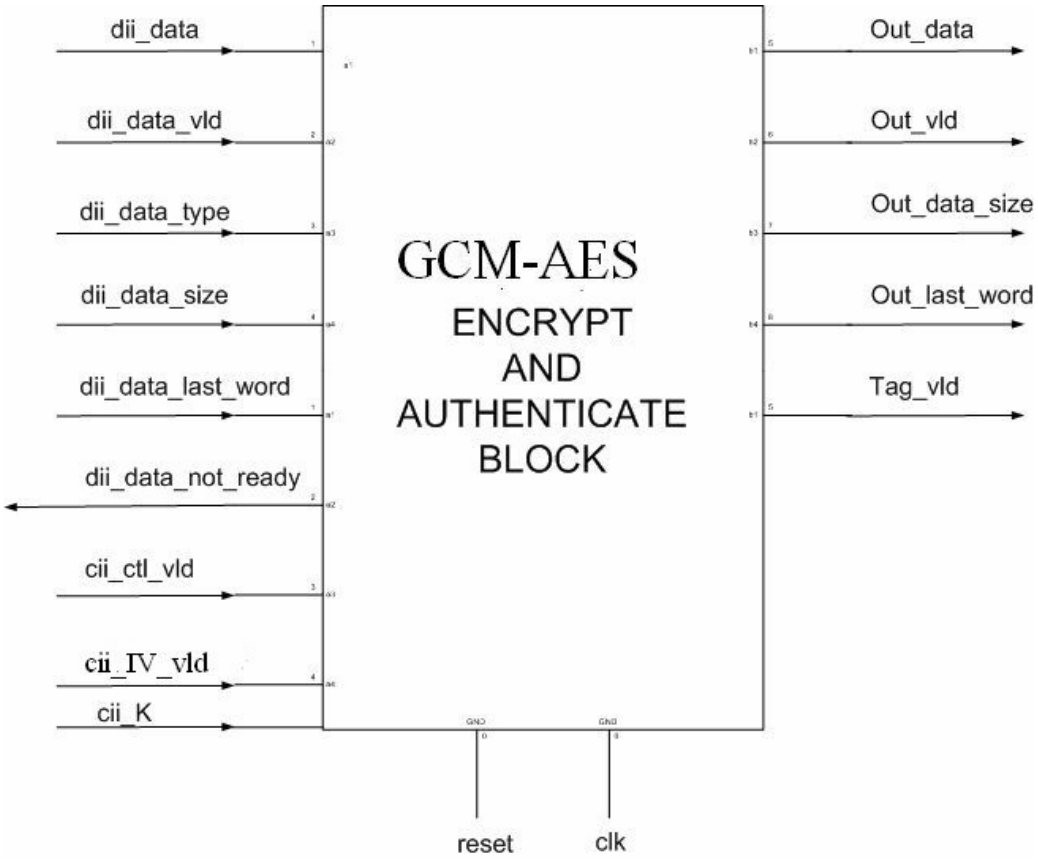

Figure 2. Interface diagram GCM-AES Encryption block

PIN	Direction	Size (bits)	Description
clk	Input	1	Design clock
reset	Input	1	Design reset
dii_data dii stands for data input interface.	Input	128	Data input that is either Nonce, message or AAD block
dii_data_vld	Input	1	When asserted (=1), dii_data contains either message or AAD block
dii_data_type	Input	1	When asserted, dii_data contains AAD block. When deasserted (= 0), dii_data contains message block
dii_data_size	Input	4	Describes the size of valid dii_data. It ranges from 0-15 where 0 indicates valid message consists of 1 byte in the LSB of dii_data and 15 indicate full block length. Its value may change from 15 on the last message or AAD block
dii_data_last_word	Input	1	When asserted, dii_data contains the last message or AAD block
dii_data_not_ready	Output	1	It is asserted by the GCM-AES indicating that it currently in the Setup phase or working with one message or AAD block and cannot accept an additional message or AAD block.
cii_ctl_vld cii stands for control input interface	Input	1	When asserted, starts the execution of GCM-AES encryption block and triggers Setup phase
cii_IV_vld	Input	1	When asserted, dii_data contains IV value
cii_K	Input	128	It contains secret key used in GCM-AES block
Out_data	Output	128	It contains either the cipher text or Tag_data
Out_vld	Output	1	When asserted, it indicates Out_data contains cipher text
Out_data_size	Output	4	It describes the number valid bytes in Out_data
Out_last_word	Output	1	It describes whether the cipher text is the last cipher text

Tag_vld	Output	1	When asserted, Out_data contains Tag data.

2.2 GCM-AES Decryption and Verification

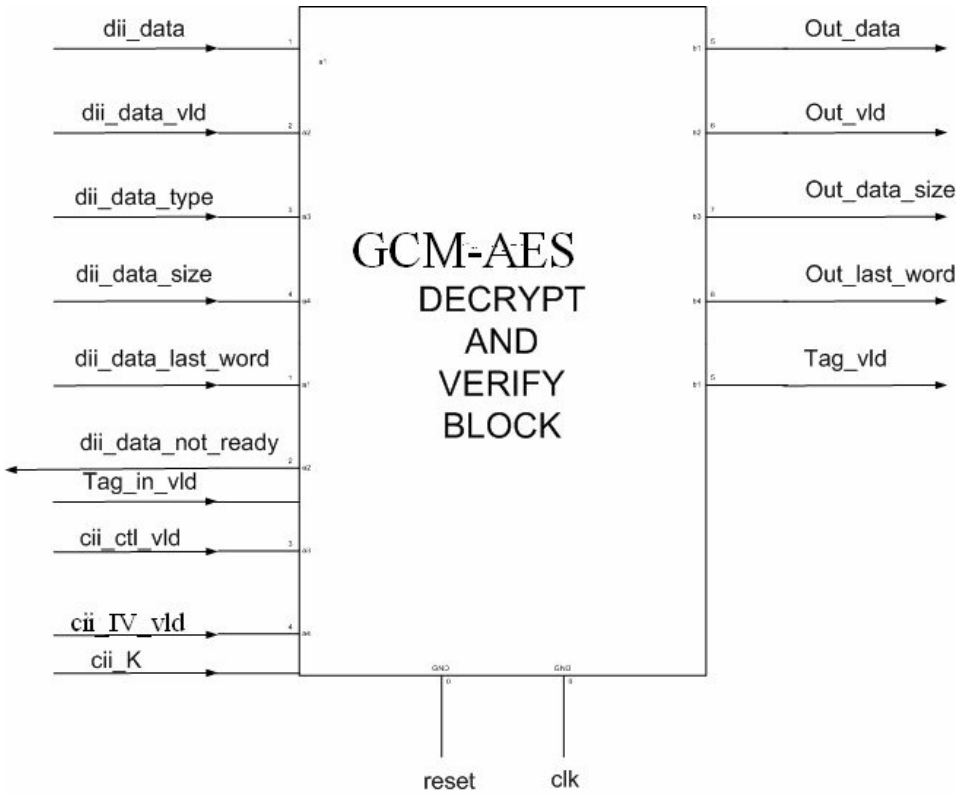

Figure 3. Interface diagram GCM-AES Decryption block

PIN	Direction	Size (bits)	Description
clk	Input	1	Design clock
reset	Input	1	Design reset
dii_data dii stands for data	Input	128	Data input that is Nonce, cipher text or AAD block. dii stands for data input interface

input interface			
dii_data_vld	Input	1	When asserted, dii_data contains either cipher text or AAD block
dii_data_type	Input	1	When asserted, dii_data contains AAD block. When deasserted, dii_data contains cipher text block
dii_data_size	Input	4	Describes the size of valid dii_data. It ranges from 0-15 where 0 indicates valid cipher text consists of 1 byte in the LSB of dii_data and 15 indicate full block length. Its value may change from 15 on the last cipher text or AAD block
dii_data_last_word	Input	1	When asserted, dii_data contains the last cipher text or AAD block
dii_data_not_ready	Output	1	It is asserted by the GCM-AES indicating that it currently in the Setup phase or working with one cipher text or AAD block and cannot accept an additional cipher text or AAD block.
Tag_in_vld	Input	1	When asserted, dii_data contains Tag that need to verified.
cii_ctl_vld cii stands for control input interface	Input	1	When asserted, starts the execution of GCM-AES encryption block and triggers Setup phase. cii stands for control input interface
cii_IV_vld	Input	1	When asserted, dii_data contains IV value
cii_K	Input	128	It contains secret key used in GCM-AES block
Out_data	Output	128	It contains plain text
Out_vld	Output	1	When asserted, it indicates Out_data contains plain text
Out_data_size	Output	4	It describes the number valid bytes in Out_data
Out_last_word	Output	1	It describes whether the plain text is the last plain text
Tag_vld	Output	1	When asserted, describes that the tag verification has been successful and plain text is valid

3 FPGA Design Flow of GCM-AES

GCM-AES design as described in the previous sections is coded in Verilog hardware descriptive language HDL. All simulations are done in Mentor Graphic's ModelSim. XILINX ISE 11.4 is used for FPGA design flow using Virtex 6 technology (Family = Virtex6, Device = XC6VLX240T, Package = FF1156, Speed = -1). The following figure shows the FPGA design flow. Default options are chosen for each stage of the FPGA design flow to allow fair benchmarking.

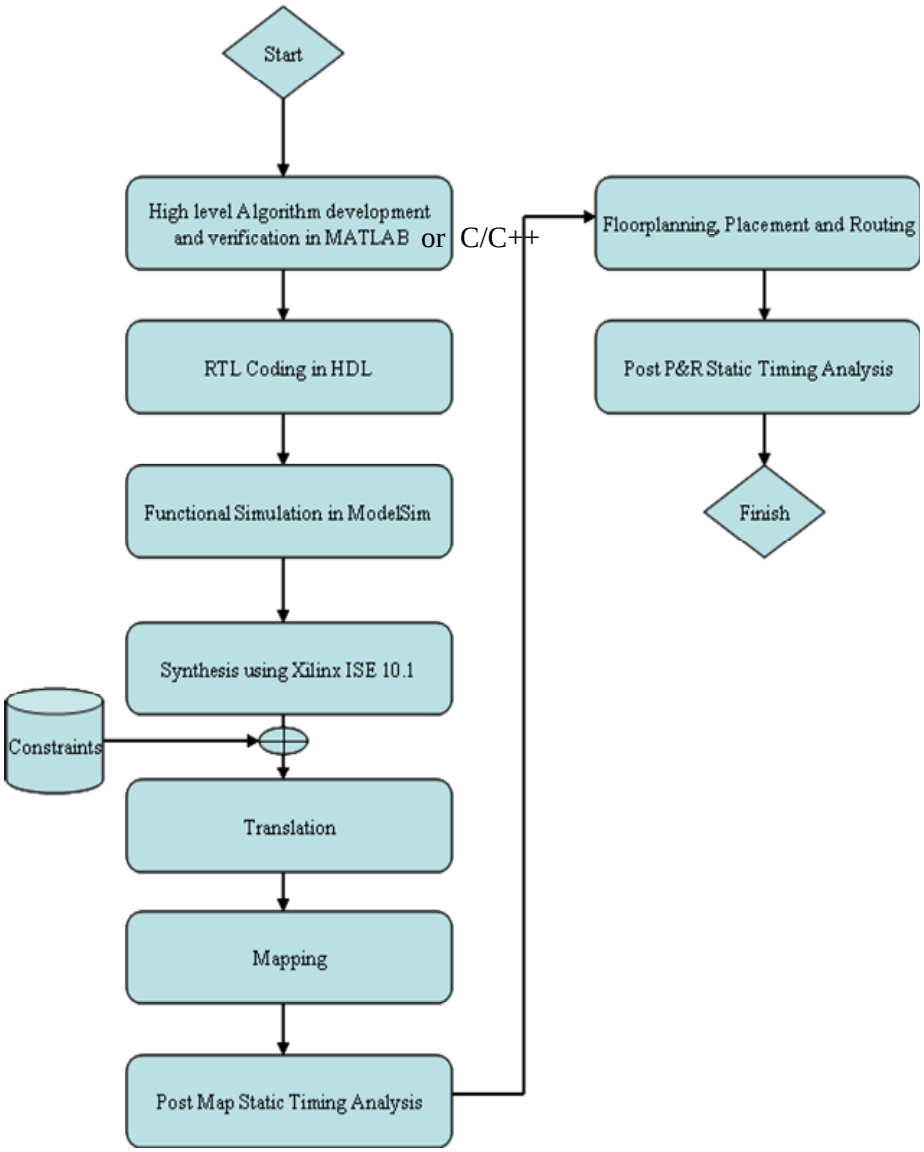

Figure 4 XILINX FPGA Design Flow

We use test case 4 in [2] for GCM-AES Encryption-Auth simulations. It is reproduced here for convenience

K = feffe9928665731c6d6a8f9467308308

P = d9313225f88406e5a55909c5aff5269a
86a7a9531534f7da2e4c303d8a318a72
1c3c0c95956809532fcf0e2449a6b525
b16aedf5aa0de657ba637b39A

AAD= feedfacedeadbeeffeedfacedeadbeef
abaddad2

IV = cafebabefacedbaddecaf888

The corresponding cipher text and Tag is

CT = 42831ec2217774244b7221b784d0d49c
e3aa212f2c02a4e035c17e2329aca12e
21d514b25466931c7d8f6a5aac84aa05
1ba30b396a0aac973d58e091

Tag = 5bc94fbc3221a5db94fae95ae7121a47

Figure 5 shows simulation of GCM-AES Encryption-Authentication block. Note that Decryption-Verify block is exactly the same. Thus, only simulation of Encryption-Authentication block suffices.

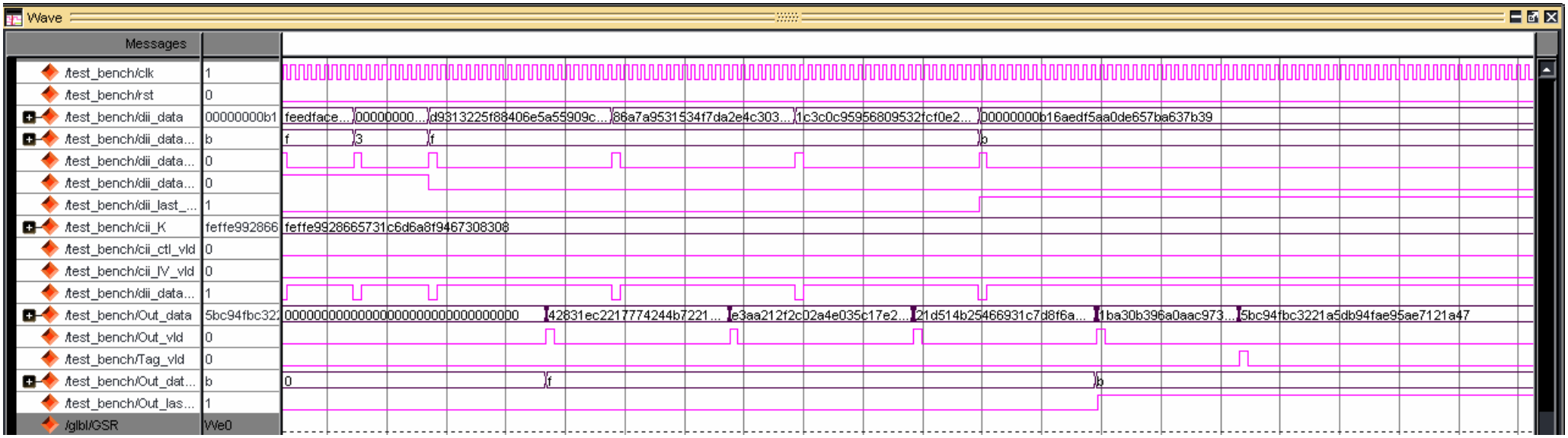

Figure 5 Simulation of GCM-AES Enc-Auth block

Table 1 shows the resources and performance figures of GCM-AES Enc-Auth blocks.

Virtex6	Flip Flops (ff)	Look up tables (LUTS)	Critical Path	Number of I/O pins	Time period reported by Xilinx ISE	Time period determined by post Place and Route Simulation	Estimated Total Power
GCM-AES Enc-Auth	1697	4169	FSM ff to gfm_cnt ff	403	7.5ns	14ns=71 MHZ	2.26 W

4 References

[1] Field Programmable Gate Array, http://en.wikipedia.org/wiki/Field-programmable_gate_array.

[2] McGrew, D. and J. Viega, "The Galois/Counter Mode of Operation (GCM)", Submission to NIST. http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-spec.pdf, January 2004.

[3] Rudolph Usselmann, “AES (Rijndael) IP core,” http://opencores.org/project,aes_core.

[4] Advanced Encryption standard AES, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf