Design Gateway Co.,Ltd

E-mail: ip-sales@design-gateway.com
URL: design-gateway.com

Features

- Support AES-GCM mode standard.
- Support 256-bit key size, 96-bit iv size.
- Support zero-length AAD or data input.
- Peak throughput rate at 128 Mbits/MHz.
- Speed up to 28.16 Gbps @220MHz.

Core Facts

Provided with Core	
Documentation	User Guide, Design Guide
Design File Formats	Encrypted HDL
Instantiation Templates	VHDL
Reference Designs & Application Notes	Vivado Project, See Reference design manual
Additional Items	Demo on ZCU106
Support	
Support Provided by Design Gateway Co., Ltd.	

Table 1: Example Implementation Statistics

Family	Example Device	Fmax (MHz)	CLB Regs	CLB LUTs	CLB[1]	IOB	BRAMTile[2]	Design Tools
Zynq-Ultrascale+	xczu7ev-ffvc1156-2-e	220	4700	15509	1696	-	-	Vivado2021.1

Notes:

1) Actual logic resource dependent on percentage of unrelated logic

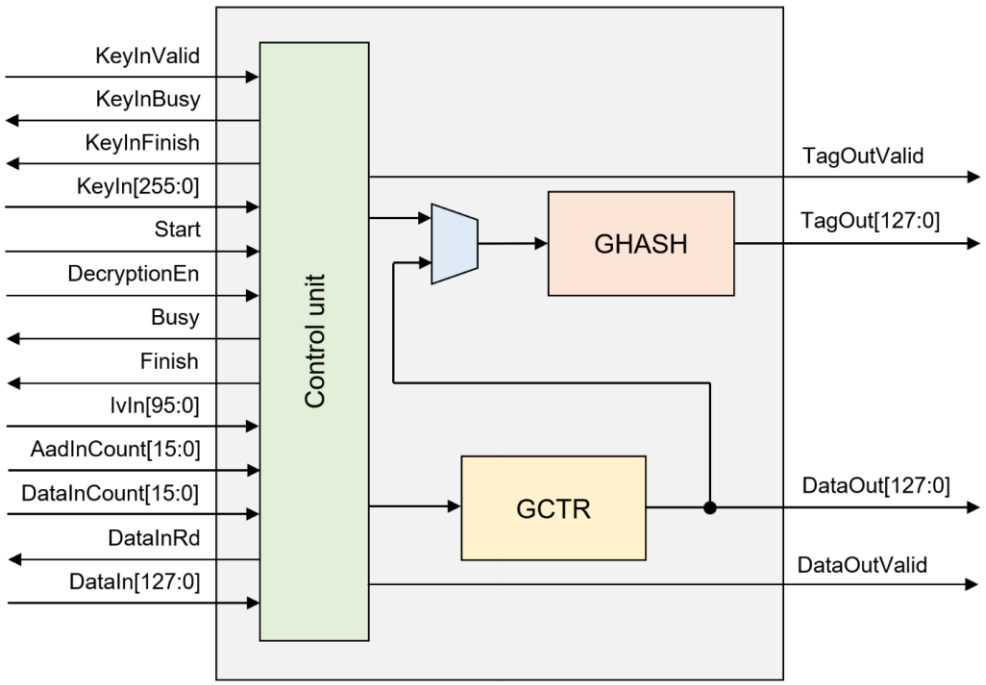

Figure 1: Block Diagram

General Description

AES256-GCM-10G25G IP Core (AES256GCM10G25GIP) implement the advanced encryption standard (AES) with 256-bit key in Galois/Counter Mode (GCM) which is widely used for Authenticated Encryption with Associated Data (AEAD) application, including IPSEC, MACSEC and TLS (Transport Layer Security) versions 1.2 and 1.3. Additionally, AES-GCM is used in fiber channel communications and storage applications.

AES256GCM10G25GIP works with 256-bit AES-key and 96-bit Initialization Vector (IV). It can provide confidentiality and data authentication by using Additional Authenticated Data (AAD) and authentication tag. It is designed to support zero-length plaintext/ciphertext input which is the special case of GCM mode, called GMAC, and also support zero-length AAD.

There are 2 main operations in AES-GCM, AES encryption/decryption by GCTR and tag calculation by GHASH algorithm. AES256GCM10G25GIP can operate 128-bit data every clock cycle, as a result, it can operate at speeds up to 28.16Gbps at 220MHz, which can be used effectively on 10G/25G Ethernet.

Functional Description

AES256GCM10G25G interface signals can be divided into 3 parts, i.e., Key setting signals, parameter setting signals and data control signals.

Table 2: Interface signals of AES256GCM10G25GIP

Signal name	Dir	Description
RstB	In	IP core system reset. Active low.
Clk	In	IP core system clock.
version[31:0]	Out	32-bit version number of AES256GCM10G25GIP.
Key setting signals		
KeyInValid	In	KeyInValid is a user signal to specify data valid of KeyIn. Assert to '1' to set up KeyIn into AES256GCM10G25GIP.
KeyInBusy	Out	KeyInBusy specifies busy status of Key setting. Assert to '1' after user set KeyInValid, until the last cycle of operation. KeyInValid or Start will be ignored while KeyInBusy is '1'.
KeyInFinish	Out	KeyInFinish specifies finish status of Key setting. Assert to '1' at the last cycle of operation.
KeyIn[255:0]	In	KeyIn is 256-bit key data for AES block cipher in CTR mode of operation. KeyIn must be valid when KeyInValid is asserted to '1'.
Parameter setting signals		
Start	In	Start is a user signal to start AES256GCM10G25GIP operation.
DecryptionEn	In	DecryptionEn is a user signal to specify mode of operation. DecryptionEn='0' for encryption, DecryptionEn='1' for decryption. DecryptionEn must be valid during operation.
Busy	Out	Busy specifies busy status of operation. Busy is active after user set Start, until operation is done. KeyInValid or Start will be ignored while Busy is '1'.
Finish	Out	Finish specifies finish status of AES256GCM10G25GIP. Assert to '1' at the last cycle of operation.
IvIn[95:0]	In	IvIn is 96-bit IV data for AES block cipher in CTR mode of operation. IvIn must be valid during operation.
AadInCount[15:0]	In	AadInCount is the number of AAD in byte. AadInCount must be valid during operation.
DataInCount[15:0]	In	DataInCount is the number of input data in byte. DataInCount must be valid during operation.

Data control signals		
DataInRd	Out	DataInRd is a control signal to read DataIn.
DataIn[127:0]	In	DataIn is 128-bit input data, both of AAD and data. DataIn must be valid when DataInRd is asserted to ‘1’.
DataOutValid	Out	DataOutValid specifies data valid for DataOut. Assert to ‘1’ when cipher data is valid for encryption mode or plain data is valid for decryption mode.
DataOut[127:0]	Out	DataOut is 128-bit data output of AES256GCM10G25GIP. Valid when DataOutValid is asserted to ‘1’.
TagOutValid	Out	TagOutValid specifies tag valid. Assert to ‘1’ when operation is done, after Busy signal is reset.
TagOut[127:0]	Out	TagOut is 128-bit tag output of AES256GCM10G25GIP. Valid when TagOutValid is asserted to ‘1’.

1. Key setting

Key setting is the first step to use AES256GCM10G25G. As shown in Figure 2, AES256GCM10G25G is started key setting process when KeyInValid='1' and takes 14 clocks cycles to finish the process (KeyInBusy='0'). After that, this KeyIn is used for every process and can be changed via KeyInValid is asserted to '1'.

2. Parameter setting

After key setting, AES256GCM10G25G starts the process when Start is asserted to '1'. DecryptionEn, KeyIn, IvIn, AadInCount and DataInCount must be valid when Start='1' and be hold during operation. User can set DecryptionEn to '0' for operating in encryption mode as shown in Figure 2 or set DecryptionEn to '1' for operating in decryption mode as shown in Figure 3.

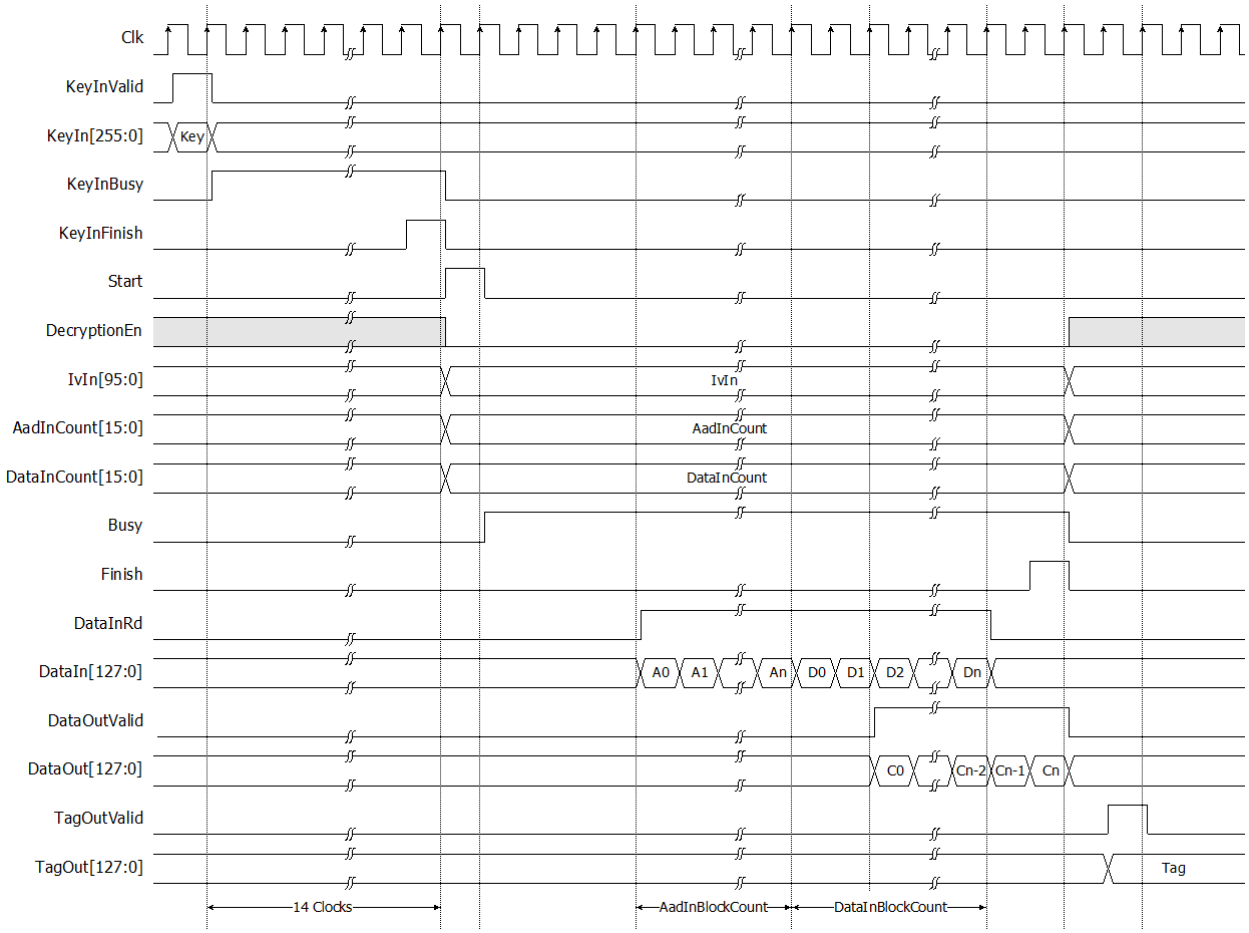

Figure 2: AES256GCM10G25G timing diagram in encryption mode

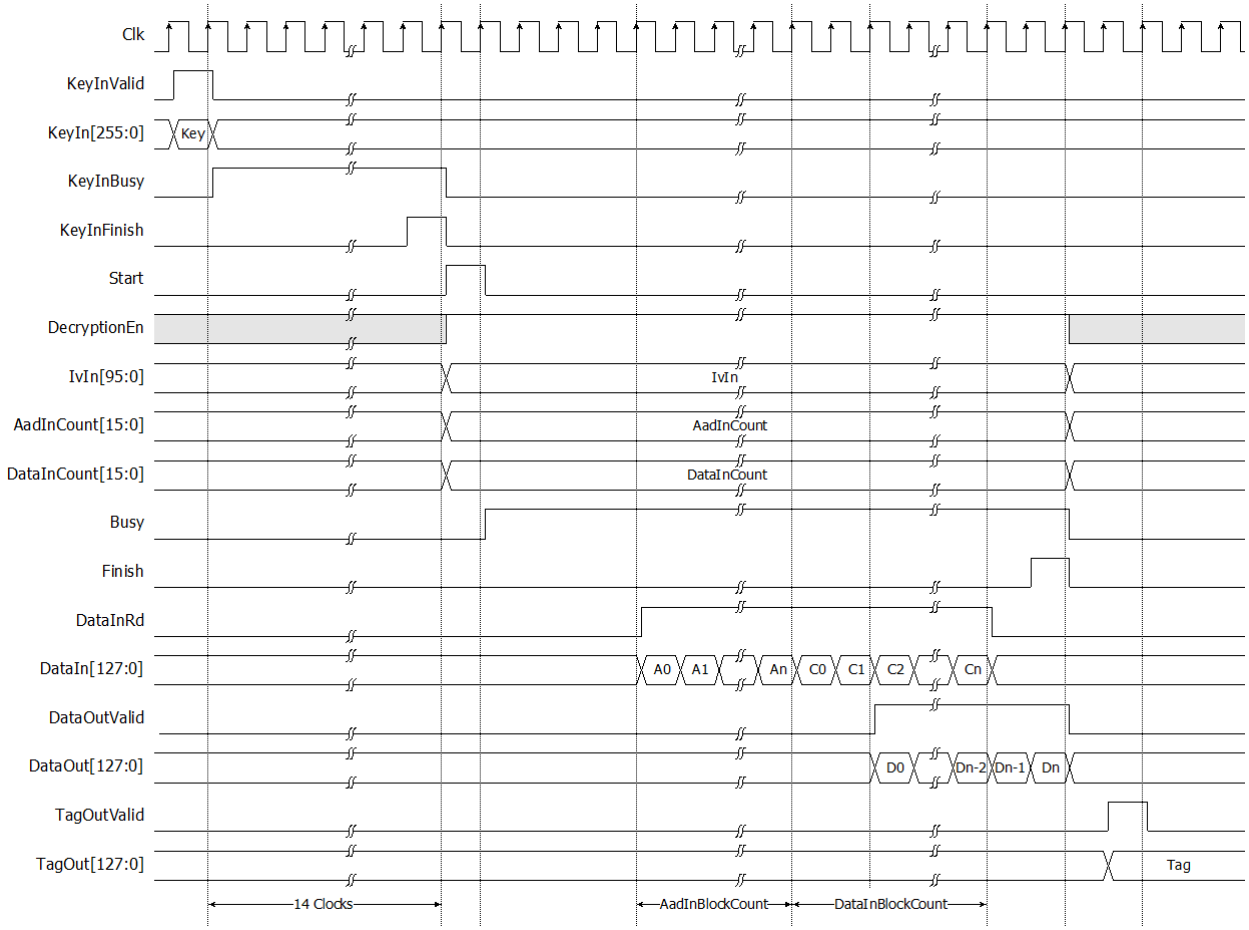

Figure 3: AES256GCM10G25G timing diagram in decryption mode

For the best performance of process, Figure 4 shows the timing diagram of continuous and pipelining process. User can used Finish signal as a trigger signal for setting new parameters and sending new start command in next cycle.

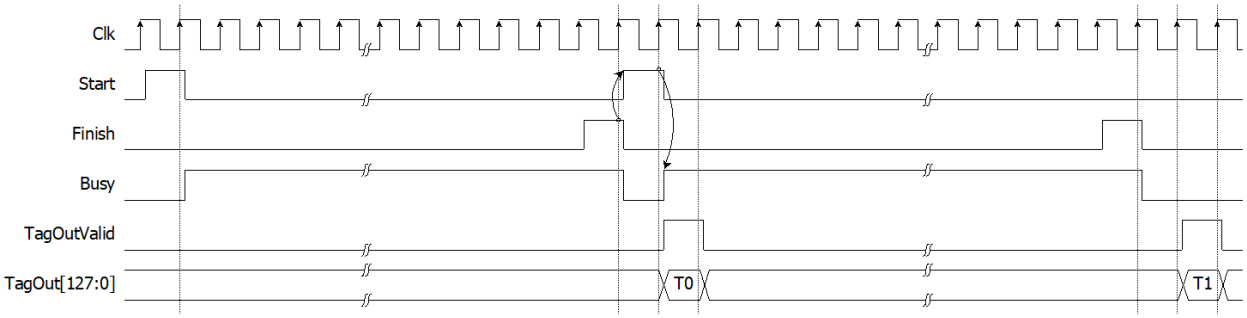

Figure 4: Continuous and pipelining operation

3. Data control

After starting operation, DataIn[127:0] must be set and valid when DataInRd is asserted to '1'. User need to prepare 128-bit DataIn. In case of non-zero length AAD, if AadInCount is not aligned to 128 bits, the last 128-bit data of AAD must be right-padded with zeros. If DataInCount is non-zero, the next 128-bit data will be plain/cipher data. AES256GCM10G25G is designed to read DataIn every clock cycle after read the first data. User may use DataInRd as a condition to prepare next 128-bit data.

As shown in Figure 2, after the first DataIn is read, the DataOut is valid in the next 2 clock cycles. In case of zero-length data, DataOutValid is not active during operation. Authentication tag is valid after finished operation. As shown in Figure 3, TagOutValid is actived only one clock on the next clock after Busy is cleared to '0'.

Verification Methods

AES256-GCM-10G25G IP functionality were verified on real board design by using ZCU106 Evaluation Board.

Recommended Design Experience

The user must be familiar with HDL design methodology to integrate this IP into system.

Ordering Information

This product is available directly from Design Gateway Co., Ltd. Please contact Design Gateway Co., Ltd. For pricing and additional information about this product using the contact information on the front page of this datasheet.

Revision History

Revision	Date	Description
1.00	21/Jun/2022	New release
1.02	20/Sep/2022	New design to improve performance
1.03	27/Sep/2022	Update pictures and description