Design Gateway Co.,Ltd

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

Core Facts

Provided with Core	
Documentation	User Guide, Design Guide
Design File Formats	Encrypted File
Instantiation Templates	VHDL
Reference Designs & Application Notes	Quartus Project, See Reference Design Manual
Additional Items	Demo on A10SoC, Agilex F-Series development kit
Support	
Support Provided by Design Gateway Co., Ltd.	

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 512Mbits/MHz.
- Speed up to 112.64 Gbps @220MHz.

Table 1: Example Implementation Statistics

Family	Example Device	Fmax (MHz)	ALMs	Registers[1]	Design Tools
Agilex F-Series	AGFB014R24A2E2VR0	220	60202.4	33663	Quartus 20.4
Arria10 SX	10AS066N3F40E2SGE2	150	60627.0	14653	Quartus 20.4
Stratix10 GX[2]	1SG280HU2F50E1VG	160	58922.1	22549	Quartus 20.4

Notes:

1) Actual logic resource is dependent on percentage of unrelated logic.
2) The results were obtained from implementation in the same environment, but have not been tested on the actual board.

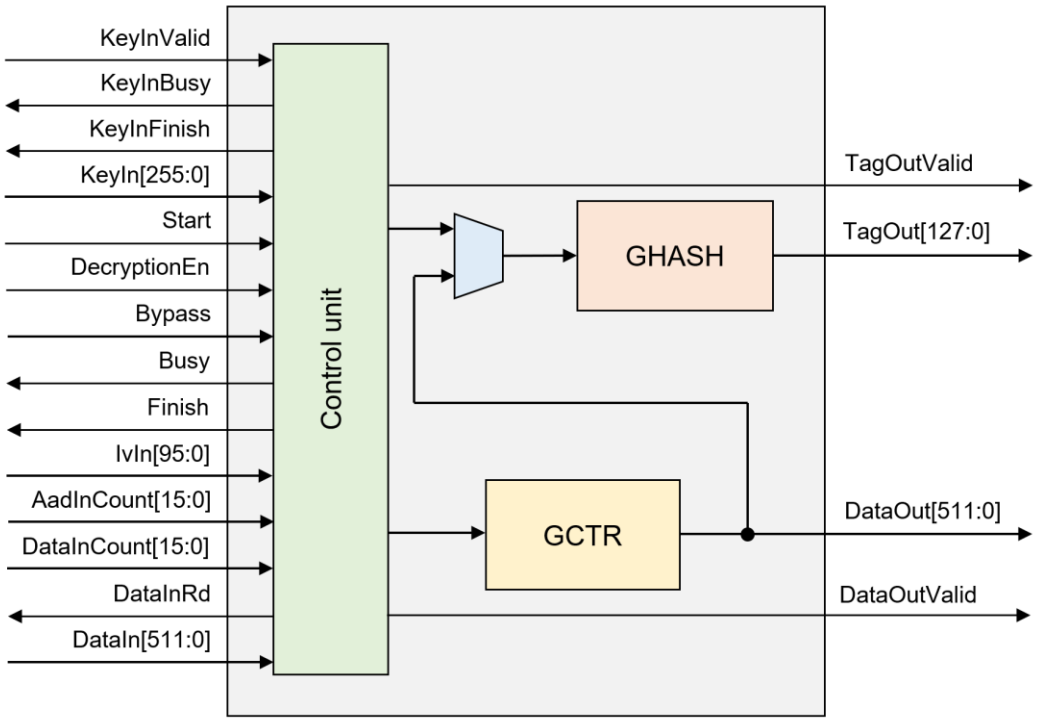

Figure 1: Block Diagram

General Description

AES256-GCM-100G IP Core (AES256GCM100GIP) 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.

AES256GCM100GIP 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. AES256GCM100GIP can operate 512-bit data every clock cycle, as a result, it can operate at speed up to 112.64Gbps at 220MHz, which can be used effectively on 100G Ethernet.

Functional Description

AES256GCM100G 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 AES256GCM100GIP

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 AES256GCM100GIP.
Key setting signals		
KeyInValid	In	KeyInValid is a user signal to specify data valid of KeyIn. Assert to '1' to set up KeyIn into AES256GCM100GIP.
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 AES256GCM100GIP 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.
Bypass	In	Bypass is a user signal to specify bypass mode of operation. Bypass='0' for encryption/decryption mode, Bypass='1' for bypass mode. Bypass 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 AES256GCM100GIP. 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[511:0]	In	DataIn is 512-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[511:0]	Out	DataOut is 512-bit data output of AES256GCM100GIP. Valid when DataOutValid is asserted to ‘1’.
TagOutValid	Out	TagOutValid specifies tag valid. Assert to ‘1’ when tag calculation is done.
TagOut[127:0]	Out	TagOut is 128-bit tag output of AES256GCM100GIP. Valid when TagOutValid is asserted to ‘1’.

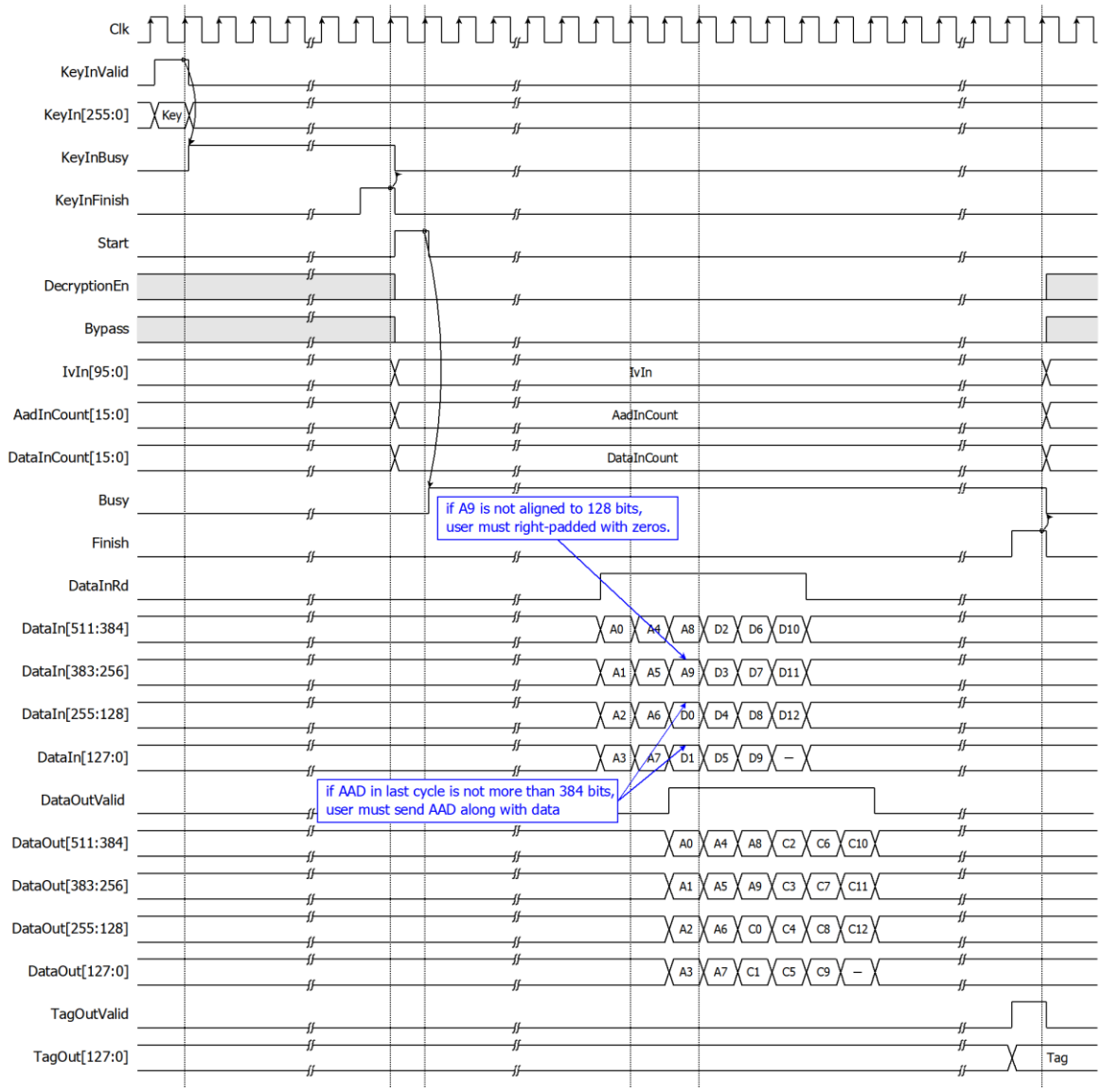

Figure 2: AES256GCM100G timing diagram in encryption mode

AES256GCM100G operation is as simple as 3 step to use as below.

1. Key setting

Key setting is the first step to use AES256GCM100G. As shown in Figure 2, AES256GCM100G is started key setting process when KeyInValid='1'. KeyInBusy is set to be '1' in the next cycle. KeyInFinish is active only one clock at the last cycle of process and KeyInBusy is cleared to '0' in the next cycle. 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, AES256GCM100G starts the process when Start is asserted to '1'. DecryptionEn, Bypass, KeyIn, IvIn, AadInCount and DataInCount must be valid when Start='1' and be hold during operation. User can set DecryptionEn to '0' and Bypass to '0' for operating in encryption mode as shown in Figure 2 or set DecryptionEn to '1' and Bypass to '0' for operating in decryption mode as shown in Figure 3. And set Bypass to '1' for operating in Bypass mode as shown in Figure 4.

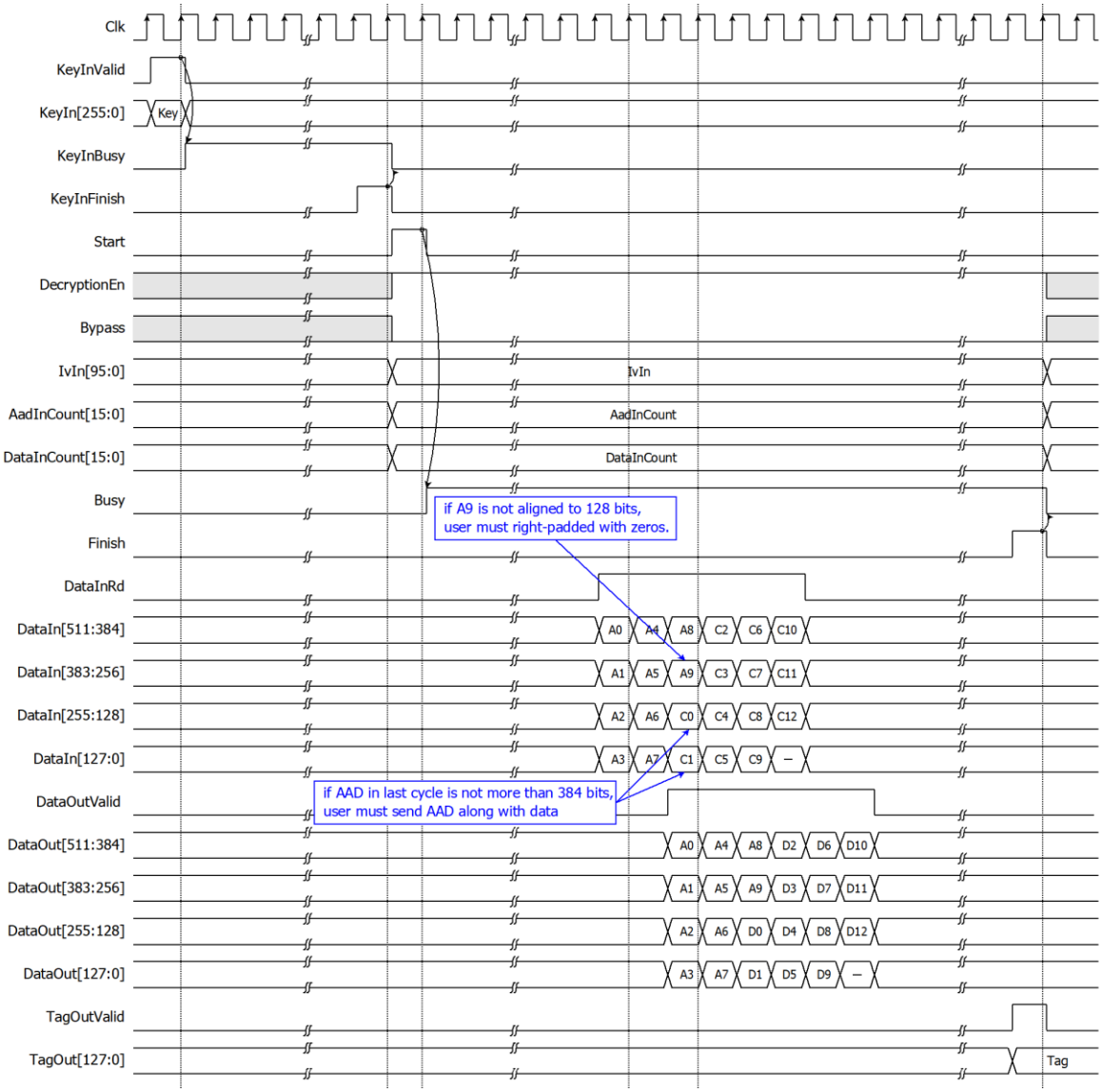

Figure 3: AES256GCM100G timing diagram in decryption mode

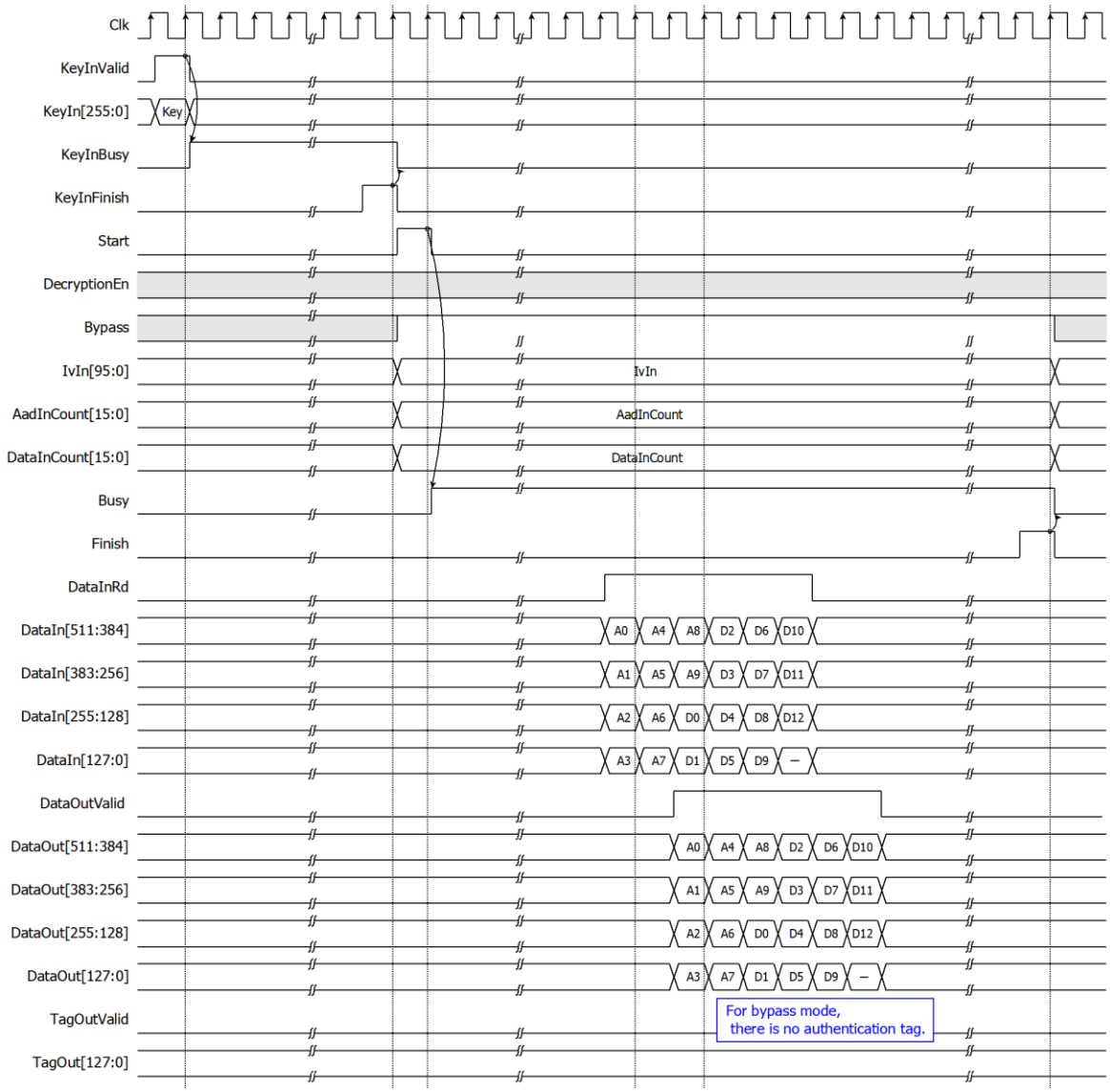

Figure 4: AES256GCM100G timing diagram in Bypass mode

For the best performance of process, Figure 5 shows the timing diagram of continuous and pipelining process. User can use Finish signal as a trigger signal for setting new parameters and sending new start command in next cycle.

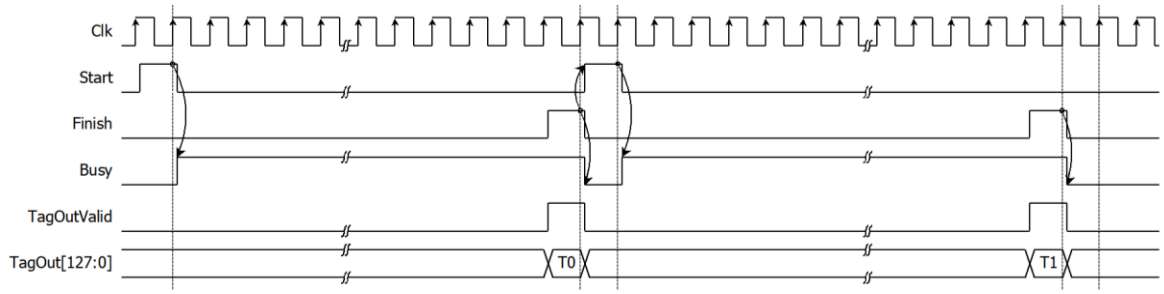

Figure 5: Continuous and pipelining operation

3. Data control

According to DataIn width is 512 bits (64 bytes) and AES256GCM100G is designed to read DataIn every clock cycle when AES256GCM100G is ready to start encryption/decryption process. After Start is set to begin the operation, user must prepare first valid DataIn[511:0]. Then user can use DataInRd signal as a trigger signal for setting the next DataIn continuously.

Even if DataIn width is 512 bits, but AAD and data is designed to process 128 bits each. If AadInCount is not aligned to 128 bits (16 bytes), the last 128-bit AAD must be right-padded with zeros. And if last cycle of AAD is not more than 384 bits(48 bytes), user must send the next 128-bit data in same clock cycle with AAD.

bit	511 504	503 496	495 400	399 392	391 384	383 16	15 8	7 0
DataIn0	AAD_{Byte0}	AAD_{Byte1}	$AAD_{Byte2 - Byte13}$	AAD_{Byte14}	AAD_{Byte15}	$AAD_{Byte16 - Byte61}$	AAD_{Byte62}	AAD_{Byte63}
DataIn1	AAD_{Byte64}	AAD_{Byte65}	$AAD_{Byte66 - Byte77}$	0x00	0x00	$DATA_{Byte0 - Byte45}$	$DATA_{Byte46}$	$DATA_{Byte47}$
DataIn2	$DATA_{Byte48}$	$DATA_{Byte49}$	$DATA_{Byte50 - Byte61}$	$DATA_{Byte62}$	$DATA_{Byte63}$	$DATA_{Byte64 - Byte109}$		

Figure 6: DataIn arrangement for 78-byte AAD and 110-byte data

Figure 6 is a detailed example of 78-byte AAD and 110-byte data preparation. DataIn0, DataIn1 and DataIn2 is represent as DataIn[511:0] in the first, second and third clock cycle respectively. The first 64-byte of AAD (AAD_{Bytes0}-$AAD_{Bytes63}$) is set as DataIn0[511:504], ..., DataIn0[7:0]. The remained 14-byte of AAD ($AAD_{Bytes64}$-$AAD_{Bytes77}$) is set as DataIn1[511:504], ..., DataIn1[407:400] and DataIn1[399:384] must be zeros. The first 48-byte data ($DATA_{Bytes0}$-$DATA_{Bytes47}$) must be set as DataIn1[383:0]. Then the remained 62-byte data ($DATA_{Bytes48}$-$DATA_{Bytes109}$) must be set as DataIn2[511:16].

As shown in Figure 2 and Figure 3, at last operation cycle, the TagOutValid is asserted to ‘1’ in the same clock cycle with the Finish signal is asserted to ‘1’. Then Busy signal is cleared to ‘0’ in the next cycle. In case of Bypass mode is active as shown in Figure 4, the TagOut is not calculated and TagOutValid is not active.

Verification Methods

AES256-GCM-100G IP Core functionality were verified on real board design by using Agilex F-Series development kit and Arria10 SoC development 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	9/Mar/2023	New release