

# AES256-SS IP Core

October 26, 2022

Product Specification

Rev1.02



## Design Gateway Co.,Ltd

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

URL: design-gateway.com

## Features

- Support AES ECB mode standard.
- Support 256-bit key size.
- Support input data width 128-bit.
- Throughput rate at 128Mbits/MHz.
- Speed up to 51.2 Gbps @400MHz.
- Operate 128-bit data every clock cycle.

| 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. |   |

**Table 1: Example Implementation Statistics for Encryption**

| Family          | Example Device     | Fmax (MHz) | ALMs    | Registers <sup>(1)</sup> | Design Tools |
|-----------------|--------------------|------------|---------|--------------------------|--------------|
| Agilex F-Series | AGFB014R24A2E2VR0  | 400        | 11525.9 | 8339                     | Quartus 20.4 |
| Arria10 SX      | 10AS066N3F40E2SGE2 | 300        | 11108.8 | 4569                     | Quartus 20.4 |

**Table 2: Example Implementation Statistics for Decryption**

| Family          | Example Device     | Fmax (MHz) | ALMs    | Registers <sup>(1)</sup> | Design Tools |
|-----------------|--------------------|------------|---------|--------------------------|--------------|
| Agilex F-Series | AGFB014R24A2E2VR0  | 400        | 13300.2 | 14407                    | Quartus 20.4 |
| Arria10 SX      | 10AS066N3F40E2SGE2 | 300        | 12330.3 | 5119                     | Quartus 20.4 |

Notes:

(1) Actual logic resource is dependent on percentage of unrelated logic.

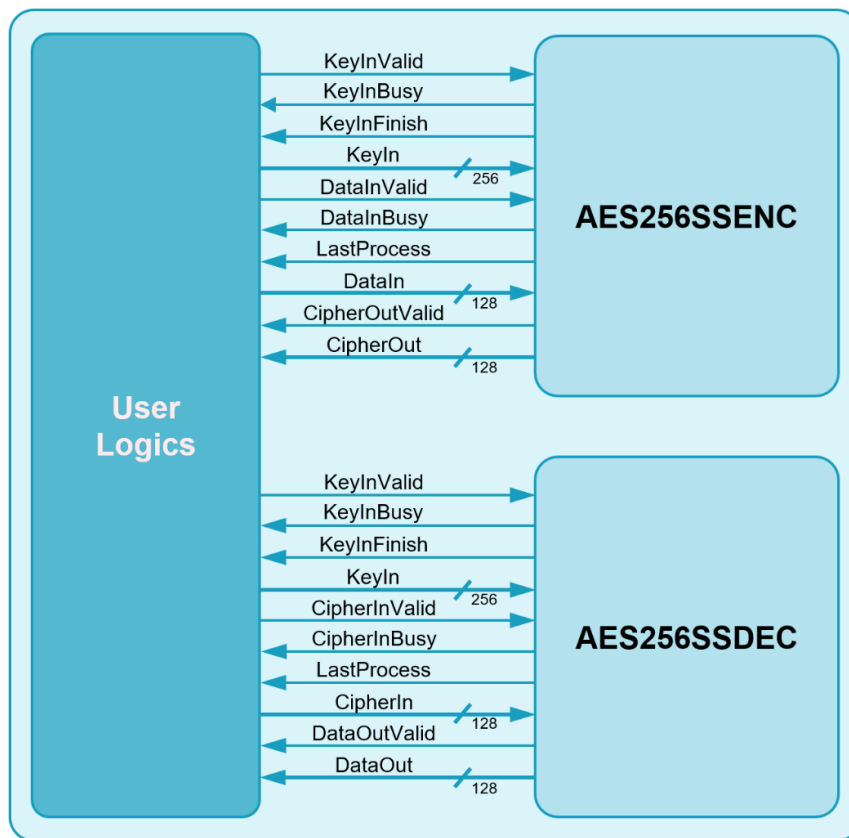


Figure 1: Block Diagram

## General Description

AES256-SS IP Core (AES256SSIP) implement the advanced encryption standard (AES) algorithm which is widely used in many applications like file encryption, processor security, and secure file transfer protocol.

AES is a symmetric block cipher algorithm of the Rijndael family. Please find more details in the Federal Information Processing Standards Publication (FIPS PUB) 197.

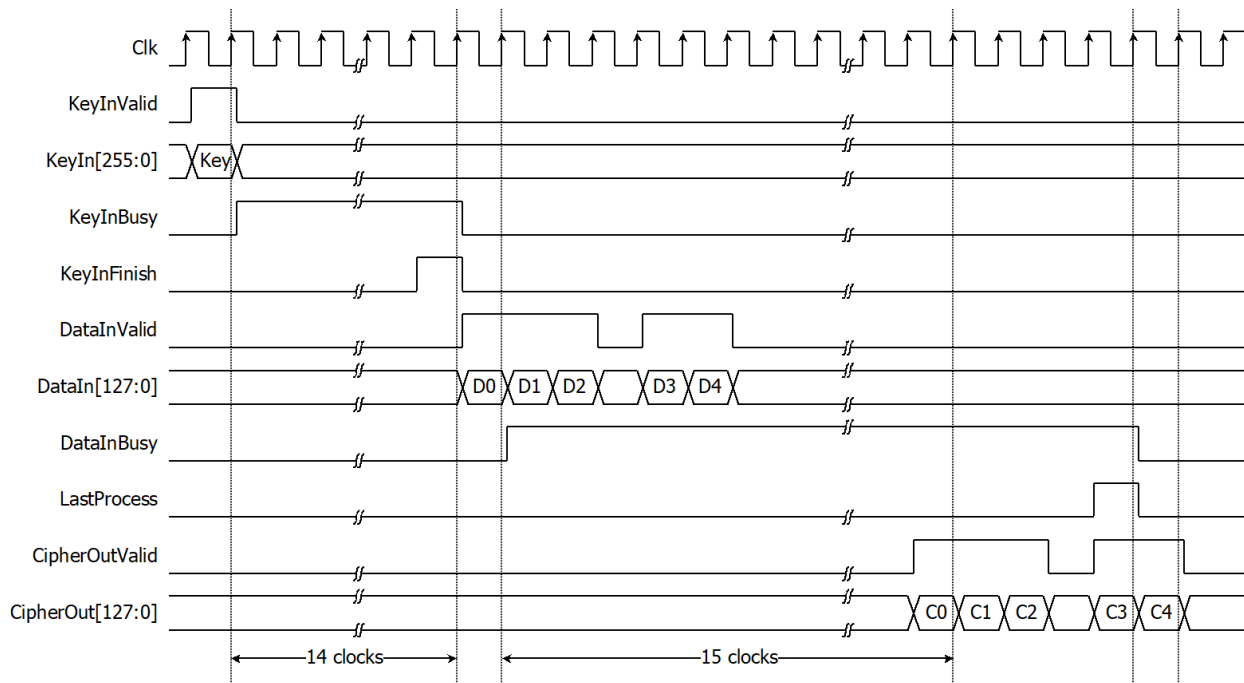
AES256SSIP or AES256 Super-Speed IP is consists of AES256SSENC module which that is encryption module and AES256SSDEC module which is decryption module as shown in Figure 1. Both module start with key setting use 15 clock cycles, After key setting user can operate 128-bit data every clock cycle.

## Functional Description

### 1. AES256SSENC

**Table 3: Interface signals of AES256SSENC**

| 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 AES256SSENC.   |
| Key setting signals        |     |   |
| KeyInValid                 | In  | KeyInValid is a user signal to specify data valid of KeyIn.<br>Assert to '1' to indicate that KeyIn is valid and start key setting.   |
| KeyInBusy                  | Out | KeyInBusy specifies busy status of key setting.<br>Assert to '1' after user set KeyInValid, until the last cycle of operation.<br>KeyInValid or DataInValid will be ignored while KeyInBusy is '1'. |
| KeyInFinish                | Out | KeyInFinish specifies finish status of key setting.<br>Assert to '1' at the last cycle of operation.  |
| KeyIn[255:0]               | In  | KeyIn is 256-bit key data for encryption.<br>KeyIn must be valid when KeyInValid is asserted to '1'.  |
| Encryption control signals |     |   |
| DataInValid                | In  | DataInValid is a user signal to specify data valid of DataIn.<br>Assert to '1' to indicate that DataIn is valid and start encryption process.   |
| DataInBusy                 | Out | DataInBusy specifies busy status of encryption.<br>Assert to '1' after user set DataInValid, until the last cycle of operation.<br>KeyInValid will be ignored while DataInBusy is '1'.              |
| LastProcess                | Out | LastProcess specifies the finish status of the last data.<br>After the user does not send DataInValid='1' for 14 clock cycles<br>LastProcess is asserted to '1' at the last cycle of operation.     |
| DataIn[127:0]              | In  | DataIn is 128-bit input data.<br>DataIn must be valid when DataInValid is asserted to '1'.  |
| CipherOutValid             | Out | CipherOutValid specifies data valid for CipherOut.<br>Assert to '1' when encryption finished.   |
| CipherOut[127:0]           | Out | CipherOut is 128-bit data output of encryption.<br>Valid when CipherOutValid is asserted to '1'.  |



**Figure 2: AES256SSENC operation timing diagram**

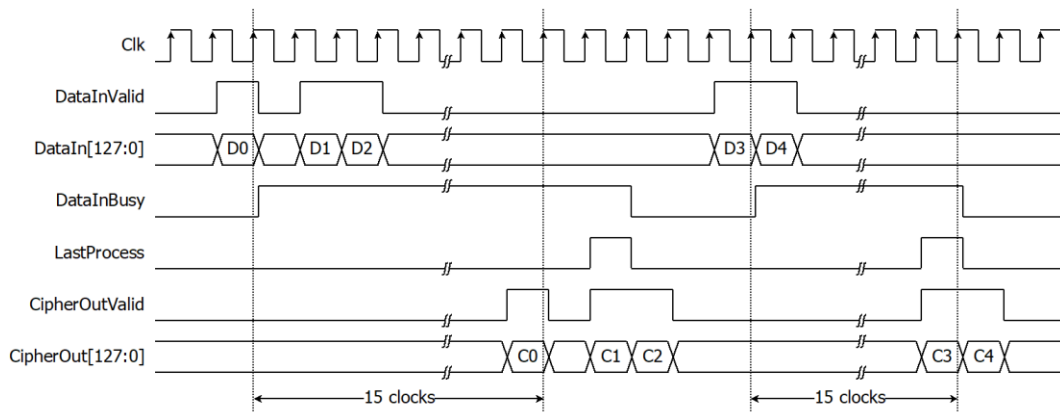
AES256SSENC operation is as simple as 2 steps to use as below.

### 1.1. Key setting

Key setting is the first step to use AES256SSENC. As shown in Figure 2, AES256SSENC 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 encryption and can be changed via KeyInvalid is asserted to '1'.

### 1.2. Encryption control

As shown in Figure 2. After key setting, AES256SSENC can operate data every clock cycle. DataIn[127:0] is encrypted when DataInvalid='1', DataInBusy is set to be '1' in the next cycle. Encrypted data is set to CipherOut[127:0] signal, while CipherOutValid signal is set to be '1' after 15 clock cycles. After the user does not send DataInvalid='1' for 14 clock cycles, LastProcess is active only one clock at the last cycle of operation and DataInBusy is cleared to '0' in the next cycle.



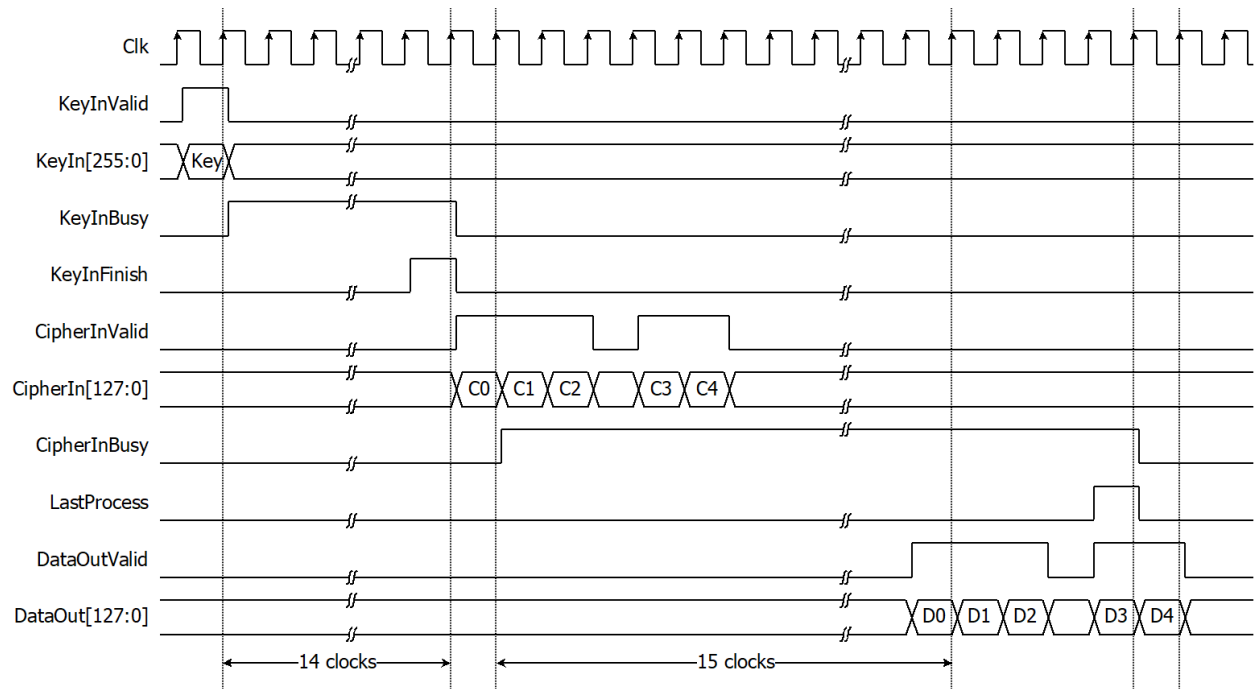
**Figure 3: Timing diagram of encryption process**

As shown in Figure 3, DataInBusy will be cleared when the user does not send DataInValid='1' more than 14 clock cycles, If the user wants to encrypt with the same key as the previous operation, user can send DataInValid='1' to encrypt DataIn[127:0] without key setting.

## 2. AES256SSDEC

**Table 4: Interface signals of AES256SSDEC**

| 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 AES256SSDEC.   |
| Key setting signals        |     |   |
| KeyInValid                 | In  | KeyInValid is a user signal to specify data valid of KeyIn. Assert to '1' to indicate that KeyIn is valid and start key setting.  |
| KeyInBusy                  | Out | KeyInBusy specifies busy status of key setting. Assert to '1' after user set KeyInValid, until the last cycle of operation. KeyInValid or CipherInValid 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 decryption. KeyIn must be valid when KeyInValid is asserted to '1'.   |
| Decryption control signals |     |   |
| CipherInValid              | In  | CipherInValid is a user signal to specify data valid of CipherIn. Assert to '1' to indicate that CipherIn is valid and start decryption process.  |
| CipherInBusy               | Out | CipherInBusy specifies busy status of decryption. Assert to '1' after user set CipherInValid, until the last cycle of operation. KeyInValid will be ignored while CipherInBusy is '1'.          |
| LastProcess                | Out | LastProcess specifies the finish status of the last data. After the user does not send CipherInValid='1' for 14 clock cycles LastProcess is asserted to '1' at the last cycle of operation.     |
| CipherIn[127:0]            | In  | CipherIn is 128-bit encrypted input data. CipherIn must be valid when CipherInValid is asserted to '1'.   |
| DataOutValid               | Out | DataOutValid specify data valid for DataOut. Assert to '1' when decryption finished.  |
| DataOut[127:0]             | Out | DataOut is 128-bit data output of decryption. Valid when DataOutValid is asserted to '1'.   |



**Figure 4: AES256DEC operation timing diagram**

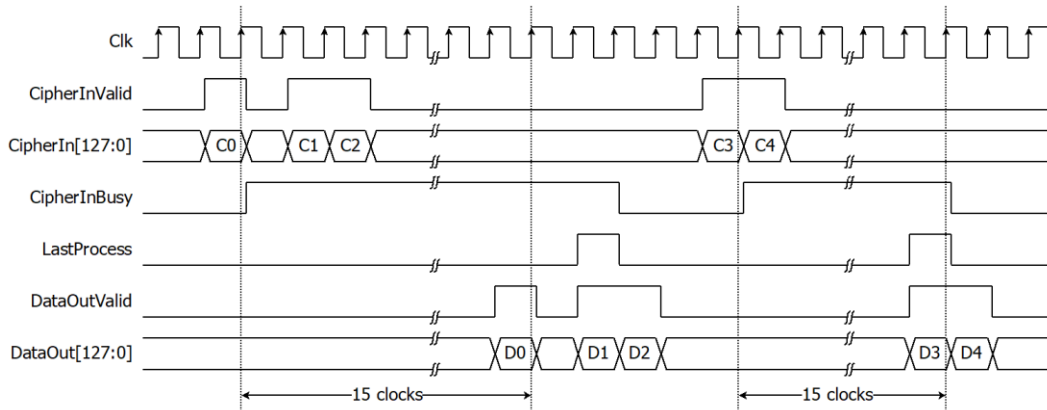
AES256DEC operation is as simple as 2 steps to use as below.

## 2.1. Key setting

Key setting is the first step to use AES256SSDEC. As shown in Figure 4, AES256SSDEC 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 decryption and can be changed via KeyInvalid is asserted to '1'.

## 2.2. Decryption control

As shown in Figure 4. After key setting, AES256SSDEC can operate data every clock cycle. Cipher[127:0] is decrypted when CipherInvalid='1', CipherInBusy is set to be '1' in the next cycle. Decrypted data is set to DataOut[127:0] signal, while DataOutValid signal is set to be '1' after 15 clock cycles. After the user does not send CipherInvalid='1' for 14 clock cycles, LastProcess is active only one clock at the last cycle of operation and CipherInBusy is cleared to '0' in the next cycle.



**Figure 5: Timing diagram of decryption process**

As shown in Figure 5, CipherInBusy will be cleared when the user does not send CipherInvalid='1' more than 14 clock cycles, If the user wants to decrypt with the same key as the previous operation, user can send CipherInvalid='1' to decrypt Cipher[127:0] without key setting.



## Verification Methods

AES256-SS 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     | 1/Oct/2021  | New release                       |
| 1.02     | 26/Oct/2022 | New design to improve performance |