|  |
| --- |
| Technical Specification (TS) |
| IP AES 256 |

**Table of distribution**

|  |  |  |
| --- | --- | --- |
| **Elsys Design** | **Name - function** | **Contact** |
|  | Killian Michaud – SoC Design/Verif Engineer | [killian.michaud@elsys-design.com](mailto:killian.michaud@elsys-design.com)  +33 6 29 47 54 13 |

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| 24/10/2024 | 0.1 | Document creation | Killian MICHAUD |

Table of content

[Table of content 4](#_Toc180748694)

[Table of figures 5](#_Toc180748695)

[Scope 6](#_Toc180748696)

[A. Mentioned documents 7](#_Toc180748697)

[1. Reference documents 7](#_Toc180748698)

[B. Acronyms and abbreviations 8](#_Toc180748699)

[C. Module Description 9](#_Toc180748700)

[1. Interfaces block diagram 9](#_Toc180748701)

[a. Interfaces description 9](#_Toc180748702)

[2. Functional description 10](#_Toc180748703)

[a. CLOCK and resets 10](#_Toc180748704)

[b. Encryption Algorithm 11](#_Toc180748705)

[c. Decryption Algorithm 13](#_Toc180748706)

[D. Functional specification 14](#_Toc180748707)

[1. Features 15](#_Toc180748708)

[a. AXI4-Lite Interface 15](#_Toc180748709)

[b. FIFO CIPHER TEXT 15](#_Toc180748710)

[c. FIFO CIPHER KEY 15](#_Toc180748711)

[d. FIFO PLAIN TEXT 15](#_Toc180748712)

[e. FIFO DECIPHER TEXT 15](#_Toc180748713)

[f. FIFO DECIPHER KEY 16](#_Toc180748714)

[g. FIFO TO\_DECIPHER TEXT 16](#_Toc180748715)

[h. ENCRYPT CORE 16](#_Toc180748716)

[i. DECRYPT CORE 16](#_Toc180748717)

[2. Mapping 17](#_Toc180748718)

[3. Registers 17](#_Toc180748719)

[4. Timings 22](#_Toc180748720)

[a. Encrypt text timing 22](#_Toc180748721)

[b. Decrypt text timing 22](#_Toc180748722)

Table of figures

[Figure 1 : Block Diagram IP AES 256 9](#_Toc180748723)

[Figure 2 : Pseudo-code for Encryption Algorithm from document [R1] 11](#_Toc180748724)

[Figure 3 : Pseudo-code for Key Expansion Algorithm from document [R1] 12](#_Toc180748725)

[Figure 4 : Pseudo-code for Decryption Algorithm from document [R1] 13](#_Toc180748726)

[Figure 5 : Functional Block Diagram 14](#_Toc180748727)

[Figure 6 : STATUS 17](#_Toc180748728)

[Figure 7 : CONTROL 18](#_Toc180748729)

[Figure 8 : VERSION 19](#_Toc180748730)

[Figure 9 : SCRPAD 19](#_Toc180748731)

[Figure 10 : KEY\_CIPHER 19](#_Toc180748732)

[Figure 11 : KEY\_DECIPHER 20](#_Toc180748733)

[Figure 12 : PLAIN\_WORD 20](#_Toc180748734)

[Figure 13 : TO\_DECIPHER\_WORD 20](#_Toc180748735)

[Figure 14 : CIPHER\_WORD 21](#_Toc180748736)

[Figure 15 : DECIPHER\_WORD 21](#_Toc180748737)

[Figure 16 : Encrypt text timing signals 22](#_Toc180748738)

[Figure 17 : Decrypt text timing signals 22](#_Toc180748739)

Scope

This document aims at providing the requirement specifications for the IP AES 256.

The **Advanced Encryption Standard (AES)** with a 256-bit key length, commonly known as **AES-256**, is a symmetric encryption algorithm used to secure data. It operates on a block size of 128 bits and uses a series of transformations, including substitution, permutation, and mixing, to encrypt and decrypt data. The process involves multiple rounds (14 for AES-256) of these transformations, making it highly secure against brute-force attacks. AES-256 is widely used in various applications, including securing sensitive data in financial transactions, communications, and data storage.

1. Mentioned documents
   1. Reference documents

|  |  |  |  |
| --- | --- | --- | --- |
| **Index** | **Title** | **Reference** | **Date** |
| [R1] | ADVANCED ENCRYPTION STANDARD (AES) | nist.fips.197.pdf | 26/11/2001 |

1. Acronyms and abbreviations

|  |  |
| --- | --- |
| Acronyms and abbreviations | Meaning |
| FPGA | Field Programmable Gate Array |
| AXI | Advanced eXtensible Interface |
| IP | Intellectual Property |
| FIFO | First In First Out |
| AES | Advanced Encryption Standard |

1. Module Description
   1. Interfaces block diagram

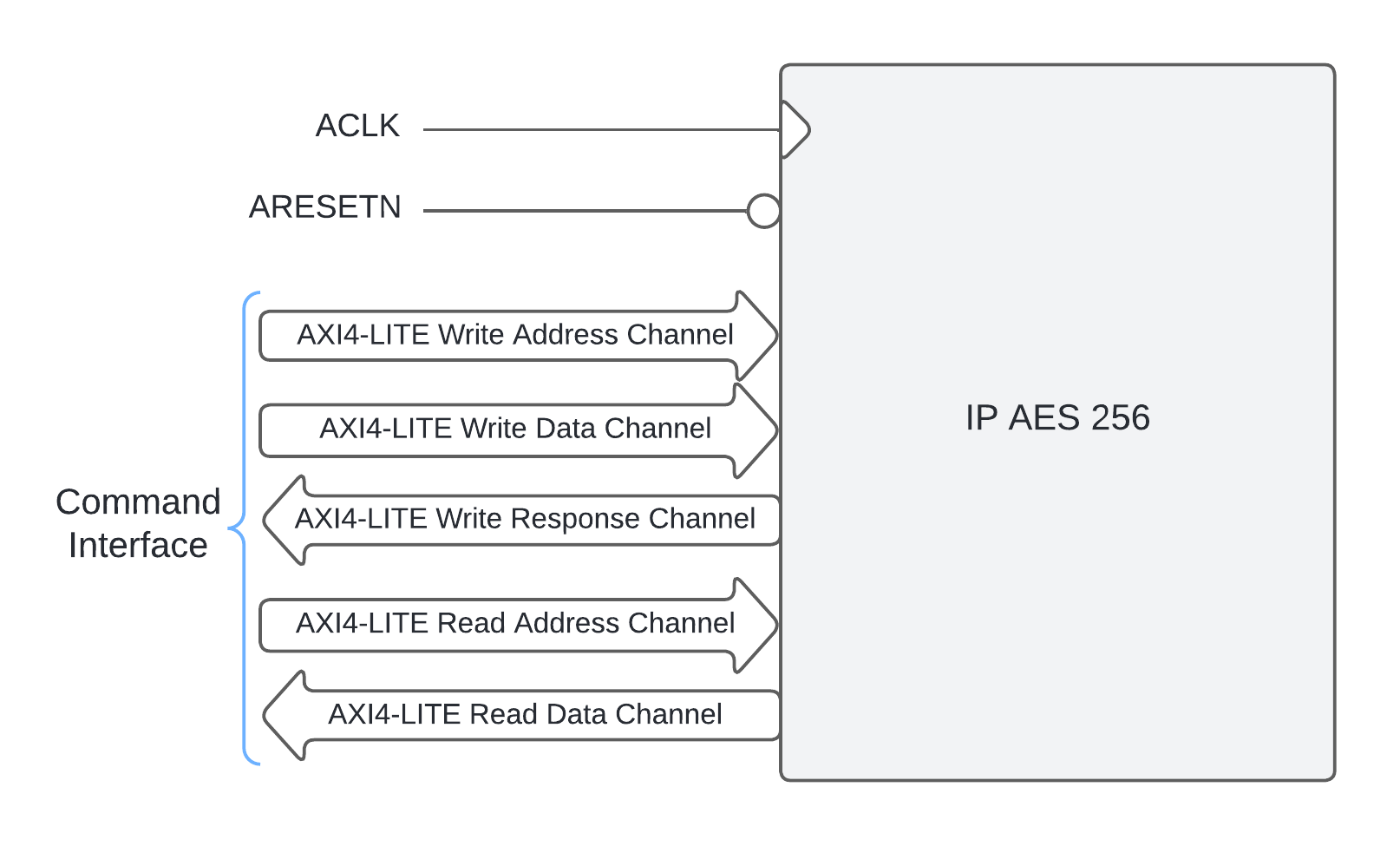


Figure 1 : Block Diagram IP AES 256

* + 1. Interfaces description

Table 1 : IP AES 256 interfaces signals

|  |  |  |  |
| --- | --- | --- | --- |
| **Signal Name** | **Length** | **Type** | **Signal description** |
| Clock Reset | | | |
| AXI4\_Lite\_Clk | 1 | INPUT | AXI Lite Clock |
| AXI4\_Lite\_Rst\_n | 1 | INPUT | Asynchronous global reset active low. |
| AXI4 LITE WRITE ADDRESS CHANNEL | | | |
| Awaddr | 32 | INPUT | Write address. The write address bus gives the address of the transaction. |
| Awvalid | 1 | INPUT | Write address valid. This signal indicates that the valid write address and control information are available. |
| Awready | 1 | OUTPUT | Write address ready. This signal indicates that the slave is ready to accept address and associated control signals. |
| AXI4 LITE WRITE DATA CHANNEL | | | |
| Wdata | 32 | INPUT | Write data. It’s a 32 bits bus. |
| Wvalid | 1 | INPUT | Write valid. This signal indicates that write data and strobes are available. |
| Wready | 1 | OUTPUT | Write ready. This signal indicates that the slave can accept the write data. |
| AXI4 LITE WRITE RESPONSE CHANNEL | | | |
| Bresp | 2 | OUTPUT | Write response. This signal indicates the status of the write transaction. The allowable responses are OKAY, EXOKAY, SLVERR and DECERR. |
| Bvalid | 1 | OUTPUT | Write response valid. This signal indicates that a valid write response is available. |
| Bready | 1 | INPUT | Response ready. This signal indicates that the master can accept the response information. |
| AXI4 LITE READ ADDRESS CHANNEL | | | |
| Araddr | 32 | INPUT | Read address. The read address bus gives the address of the transaction. |
| Arvalid | 1 | INPUT | Read address valid. This signal indicates that the valid read address and control information are available. |
| Arready | 1 | OUTPUT | Read address ready. This signal indicates that the slave is ready to accept address and associated control signals. |
| AXI4 LITE READ DATA CHANNEL | | | |
| Rdata | 32 | OUTPUT | Read data. It’s a 32 bit bus. |
| Rresp | 2 | OUTPUT | Read response. This signal indicates the status of the read transfer. The allowable responses are OKAY, EXOKAY, SLVERR and DECERR. |
| Rvalid | 1 | OUTPUT | Read valid. This signal indicates that the required read data is available and the transfer can complete. |
| Rready | 1 | INPUT | Read ready. This signal indicates that the master can accept the read data and response information. |

* 1. Functional description
     1. CLOCK and resets

SYS\_CLK: system clock. This clock is used for the AXI Lite interface.

RESET\_N: synchronous reset of the system clock. This input is subsequently used as an asynchronous reset for the various modules. Reset active in low state.

* + 1. Encryption Algorithm

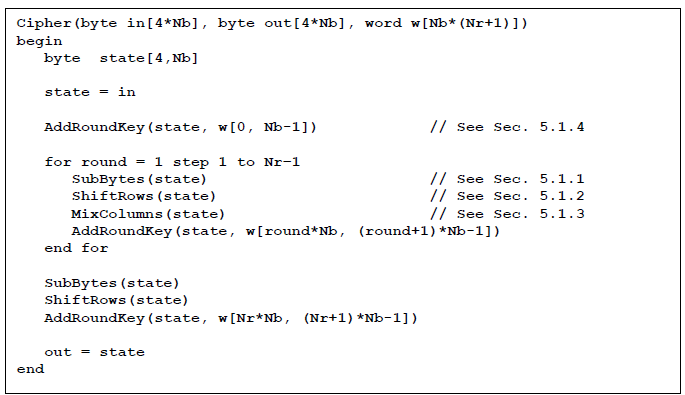


Figure 2 : Pseudo-code for Encryption Algorithm from document [R1]

In the Encryption Algorithm, the first step is to create all the 15 keys required to complete all the functions. This step is done with a new Algorithm, named Key Expansion ( Figure 3).

In AES-256, 15 rounds is needed to complete Encryption Algorithm. The first round is a XOR operation between the first key, create with Key Expansion, and plain text.

The round 2 to 14, there a succession of methods named :

* SubBytes
* ShiftRows
* MixColumns
* AddRoundKeys

Finally the last round is a succession of methods, like the previous rounds but the MixColumns method isn’t include in this round.

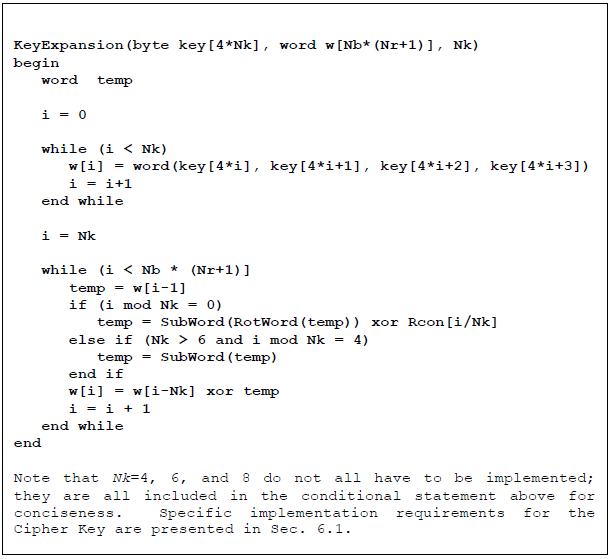


Figure 3 : Pseudo-code for Key Expansion Algorithm from document [R1]

* + 1. Decryption Algorithm

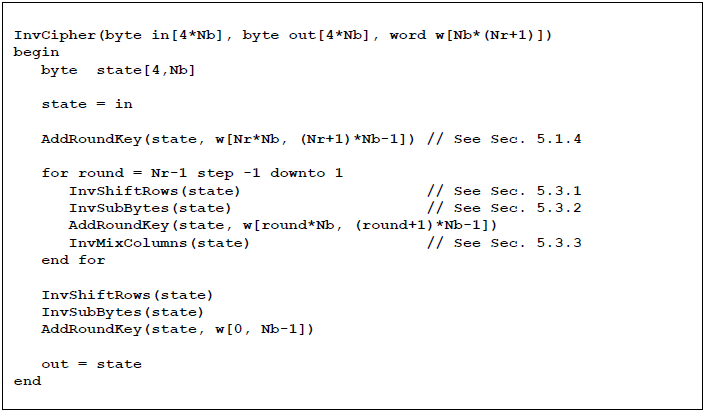


Figure 4 : Pseudo-code for Decryption Algorithm from document [R1]

In the Decryption Algorithm, the first step is to create all the 15 keys required to complete all the functions, the Key Expansion Algorithm is also use.

In AES-256, 15 rounds is needed to complete Encryption Algorithm. The first round is a XOR operation between the last key, create with Key Expansion, and cipher text.

The round 2 to 14, there a succession of methods named :

* InvShiftRows
* InvSubBytes
* AddRoundKeys
* InvMixColumns

Finally the last round is a succession of methods, like the previous rounds but the InvMixColumns method isn’t include in this round.

1. Functional specification

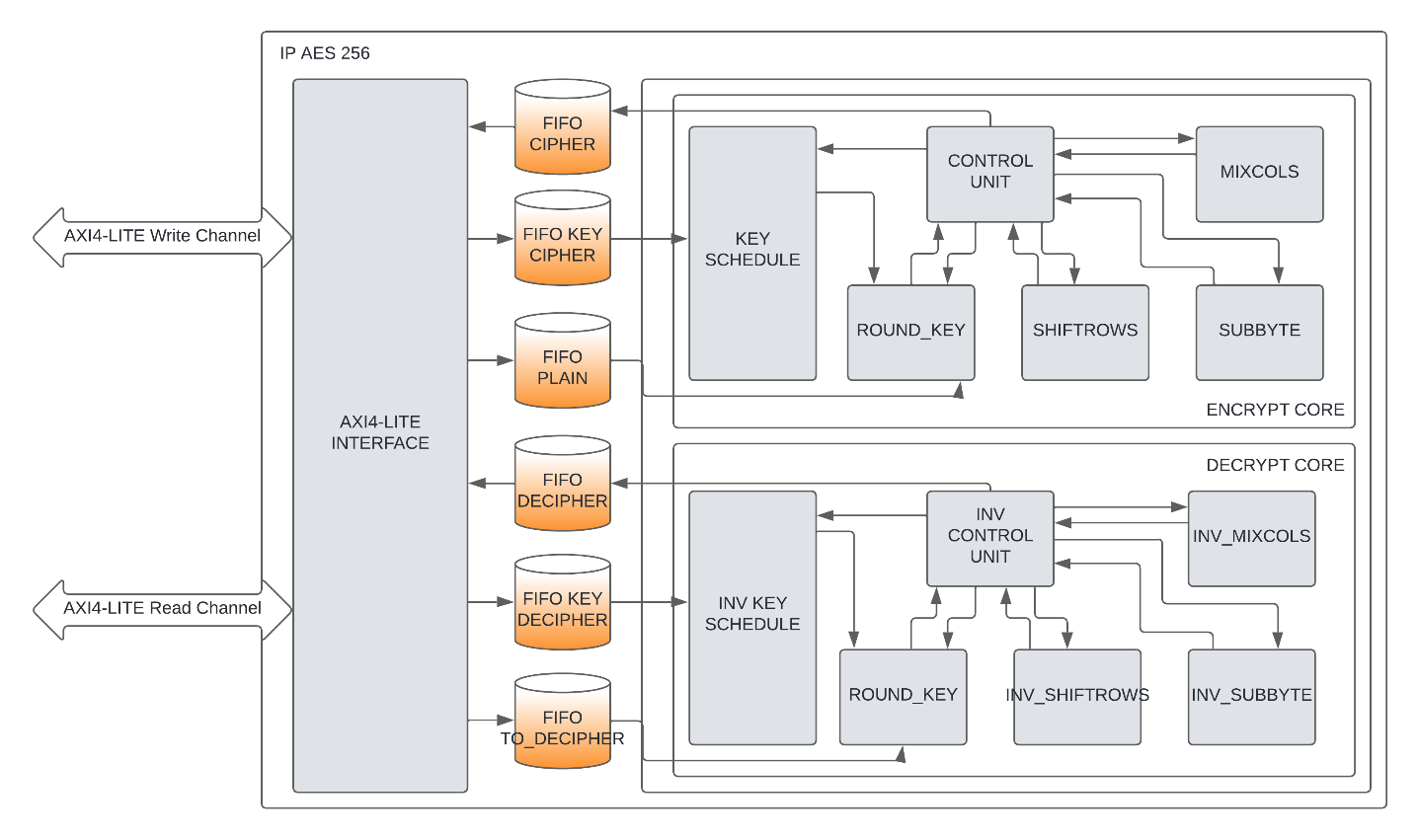


Figure 5 : Functional Block Diagram

This IP AES 256 is composed of 9 modules :

* AXI4-Lite Interface
* FIFO CIPHER TEXT
* FIFO CIPHER KEY
* FIFO PLAIN TEXT
* FIFO DECIPHER TEXT
* FIFO DECIPHER KEY
* FIFO TO\_DECIPHER TEXT
* ENCRYPT CORE
* DECRYPT CORE
  1. Features
     1. AXI4-Lite Interface
* Full forward and reverse direction flow control of AXI protocol-defined READY/VALID handshake.
* AXI4 memory mapped burst lengths of:
  + 1 to 256 bits for incrementing burst and
  + 1 to 16 bits for wrap burst
* For AXI4-Lite, the supported data width is 32 bits only.
* The use of Read/Write, Read-only, or Write-only interfaces.
* No support for locked transfers.
* The use of user bits is discouraged in general purpose due to interoperability concerns.
* Holding AXI ARESETN asserted for 16 cycles of the AXI clock is generally a sufficient reset pulse width.
  + 1. FIFO CIPHER TEXT
* First input data, first output data
* 128bits length input data
* 32bits length output data
  + 1. FIFO CIPHER KEY
* First input data, first output data
* 32bits length input data
* 256bits length output data
  + 1. FIFO PLAIN TEXT
* First input data, first output data
* 32bits length input data
* 128bits length output data
  + 1. FIFO DECIPHER TEXT
  + First input data, first output data
  + 128bits length input data
  + 32bits length output data
    1. FIFO DECIPHER KEY
    - First input data, first output data
    - 32bits length input data
    - 256bits length output data
    1. FIFO TO\_DECIPHER TEXT
* First input data, first output data
* 32bits length input data
* 128bits length output data
  + 1. ENCRYPT CORE
* Take a 256bits Cipher key and 128bits Plain text
* A start bit is set to enable the encrypt algorithm :
  + Follow the steps of the AES specification document :
    - Key Expansion
    - Add Round Keys
    - Sub byte
    - Shift rows
    - Mix columns
* A Control unit is there to insure the proper operation of the algorithm
* 128bits Cipher text output
* 1bit done status algorithm
  + 1. DECRYPT CORE
* Take a 256bits Decipher Key and 128bits Cipher text
* A start bit is set to enable the decrypt algorithm :
  + Follow the steps of the AES specification document :
    - Key Expansion
    - Add Round Keys
    - Inverse Shift Rows
    - Inverse Sub byte
    - Inverse Mix columns
* A Control unit is there to insure the proper operation of the algorithm
* 128bits Plain text output
* 1bit done status algorithm
  1. Mapping

Table 2 : Memory mapping IP AES 256

|  |  |  |  |
| --- | --- | --- | --- |
| Address Offset \* | Name | Access | Description |
| 00h | STATUS | RO | Status register |
| 04h | CONTROL | R/W | Control register |
| 08h | VERSION | RO | Version register |
| 0Ch | SCRPAD | R/W | Scratchpad register |
| 10h | KEY\_CIPHER | WO | Cipher key register |
| 14h | KEY\_DECIPHER | WO | Decipher key register |
| 18h | PLAIN\_WORD | WO | Plain text register |
| 1Ch | TO\_DECIPHER\_WORD | WO | To decipher text register |
| 20h | CIPHER\_WORD | RO | Cipher text register |
| 24h | DECIPHER\_WORD | RO | Decipher text register |

Notes: \* Address offset is relative to IP AES 256 base address

* 1. Registers

**STATUS (Status register Address – Offset 00h)**

This register provides the status signals of the IP AES 256.

|  |
| --- |
| 31 0 |
| STATUS |

Figure 6 : STATUS

Table 3 : STATUS details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits | Fields Name | Default Value | Access Type | Description |
| 0 | Done\_cipher | 0 | RO | Status of the Encrypt Algorithm |
| 1 | Done\_decipher | 0 | RO | Status of the Decrypt Algorithm |
| 2 | Cipher\_text\_empty | 0 | RO | Flag FIFO TO\_DECIPHER TEXT empty |
| 3 | Cipher\_text\_full | 0 | RO | Flag FIFO TO\_DECIPHER TEXT full |
| 4 | Plain\_text\_empty | 0 | RO | Flag FIFO PLAIN TEXT empty |
| 5 | Plain\_text\_full | 0 | RO | Flag FIFO PLAIN TEXT full |
| 6 | Cipher\_key\_empty | 0 | RO | Flag FIFO CIPHER KEY empty |
| 7 | Cipher\_key\_full | 0 | RO | Flag FIFO CIPHER KEY full |
| 8 | Decipher\_key\_empty | 0 | RO | Flag FIFO DECIPHER KEY empty |
| 9 | Decipher\_key\_full | 0 | RO | Flag FIFO DECIPHER KEY full |
| 10 | Decipher\_text\_empty | 0 | RO | Flag FIFO DECIPHER TEXT empty |
| 11 | Decipher\_text\_full | 0 | RO | Flag FIFO DECIPHER TEXT full |
| 12 | Enc\_text\_empty | 0 | RO | Flag FIFO CIPHER TEXT empty |
| 13 | Enc\_text\_full | 0 | RO | Flag FIFO CIPHER TEXT full |

**CONTROL (Control register Address – Offset 04h)**

This register provides the control signals of the IP AES 256.

|  |
| --- |
| 31 0 |
| CONTROL |

Figure 7 : CONTROL

Table 4 : CONTROL details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits | Fields Name | Default Value | Access Type | Description |
| 0 | Start\_cipher | 0 | RW | Enable a encrypt algorithm |
| 1 | Start\_decipher | 0 | RW | Enable a encrypt algorithm |
| 2 | Flush\_cipher | 0 | RW | Reset to zero FIFO TO\_DECIPHER TEXT |
| 3 | Flush\_plain | 0 | RW | Reset to zero FIFO PLAIN TEXT |
| 4 | Flush\_cipher\_key | 0 | RW | Reset to zero FIFO CIPHER KEY |
| 5 | Flush\_decipher\_key | 0 | RW | Reset to zero FIFO DECIPHER KEY |
| 6 | Flush\_enc | 0 | RW | Reset to zero FIFO CIPHER TEXT |
| 7 | Flush\_dec | 0 | RW | Reset to zero FIFO DECIPHER TEXT |
| 31 to 8 | Reserved | 0 | RW | N/A |

**VERSION (Version register Address – Offset 08h)**

This register provides the version of the IP AES 256.

|  |
| --- |
| 31 0 |
| Version |

Figure 8 : VERSION

Table 5 : VERSION details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits | Fields Name | Default Value | Access Type | Description |
| 31 to 0 | Version | 0 | RO | Number of version of the IP |

**SCRATCHPAD (Scratchpad register Address – Offset 0Ch)**

This register provides a scratchpad area for the IP AES 256.

|  |
| --- |
| 31 0 |
| SCRPAD |

Figure 9 : SCRPAD

Table 6 : SCRPAD details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits | Fields Name | Default Value | Access Type | Description |
| 31 to 0 | SCRPAD | 0 | R/W | Scratchpad data |

**KEY\_CIPHER (KEY\_CIPHER register Address – Offset 10h)**

This register provides the cipher key to the FIFO CIPHER KEY of the IP AES 256.

|  |
| --- |
| 31 0 |
| KEY\_CIPHER |

Figure 10 : KEY\_CIPHER

Table 7 : KEY\_CIPHER details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits | Fields Name | Default Value | Access Type | Description |
| 31 to 0 | KEY\_CIPHER | 0 | WO | Data transmitted to the ENCRYPT CORE module |

**KEY\_DECIPHER (KEY\_DECIPHER register Address – Offset 14h)**

This register provides the cipher key to the FIFO CIPHER KEY of the IP AES 256.

|  |
| --- |
| 31 0 |
| KEY\_DECIPHER |

Figure 11 : KEY\_DECIPHER

Table 8 : KEY\_DECIPHER details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits | Fields Name | Default Value | Access Type | Description |
| 31 to 0 | KEY\_DECIPHER | 0 | WO | Data transmitted to the DECRYPT CORE module |

**PLAIN\_WORD (Plain Text register Address – Offset 18h)**

This register provides the cipher key to the FIFO CIPHER KEY of the IP AES 256.

|  |
| --- |
| 31 0 |
| PLAIN\_WORD |

Figure 12 : PLAIN\_WORD

Table 9 : PLAIN\_WORD details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits | Fields Name | Default Value | Access Type | Description |
| 31 to 0 | PLAIN\_WORD | 0 | WO | Data transmitted to the ENCRYPT CORE module |

**TO\_DECIPHER\_WORD (To decipher text register Address – Offset 1Ch)**

This register provides the cipher key to the FIFO CIPHER KEY of the IP AES 256.

|  |
| --- |
| 31 0 |
| TO\_DECIPHER\_WORD |

Figure 13 : TO\_DECIPHER\_WORD

Table 10 : TO\_DECIPHER\_WORD details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits | Fields Name | Default Value | Access Type | Description |
| 31 to 0 | TO\_DECIPHER\_WORD | 0 | WO | Data transmitted to the DECRYPT CORE module |

**CIPHER\_WORD (Cipher text register Address – Offset 20h)**

This register provides the cipher key to the FIFO CIPHER KEY of the IP AES 256.

|  |
| --- |
| 31 0 |
| CIPHER\_WORD |

Figure 14 : CIPHER\_WORD

Table 11 : CIPHER\_WORD details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits | Fields Name | Default Value | Access Type | Description |
| 31 to 0 | CIPHER\_WORD | 0 | RO | Data from the ENCRYPT CORE module |

**DECIPHER\_WORD (Decipher text register Address – Offset 24h)**

This register provides the cipher key to the FIFO CIPHER KEY of the IP AES 256.

|  |
| --- |
| 31 0 |
| DECIPHER\_WORD |

Figure 15 : DECIPHER\_WORD

Table 12 : DECIPHER\_WORD details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits | Fields Name | Default Value | Access Type | Description |
| 31 to 0 | DECIPHER\_WORD | 0 | RO | Data from the DECRYPT CORE module |

* 1. Timings
     1. Encrypt text timing

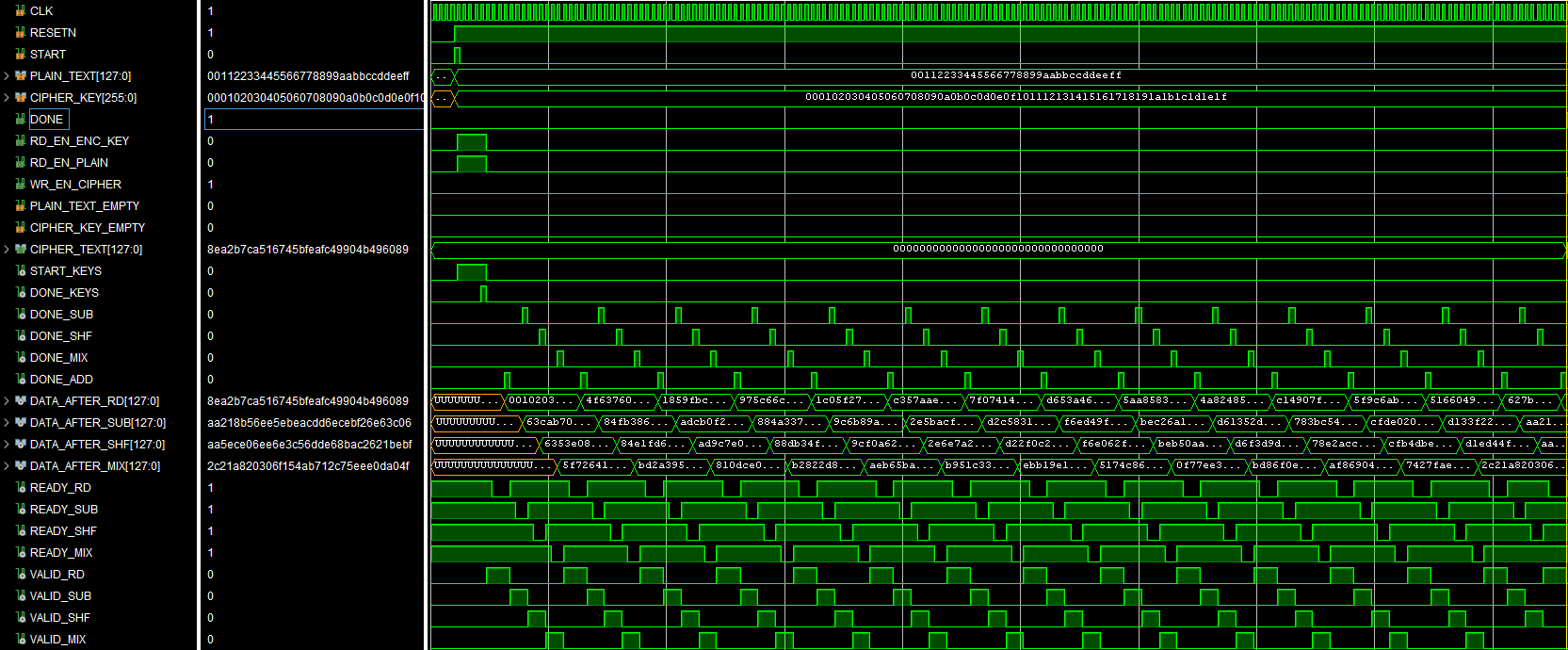


Figure 16 : Encrypt text timing signals

* + 1. Decrypt text timing

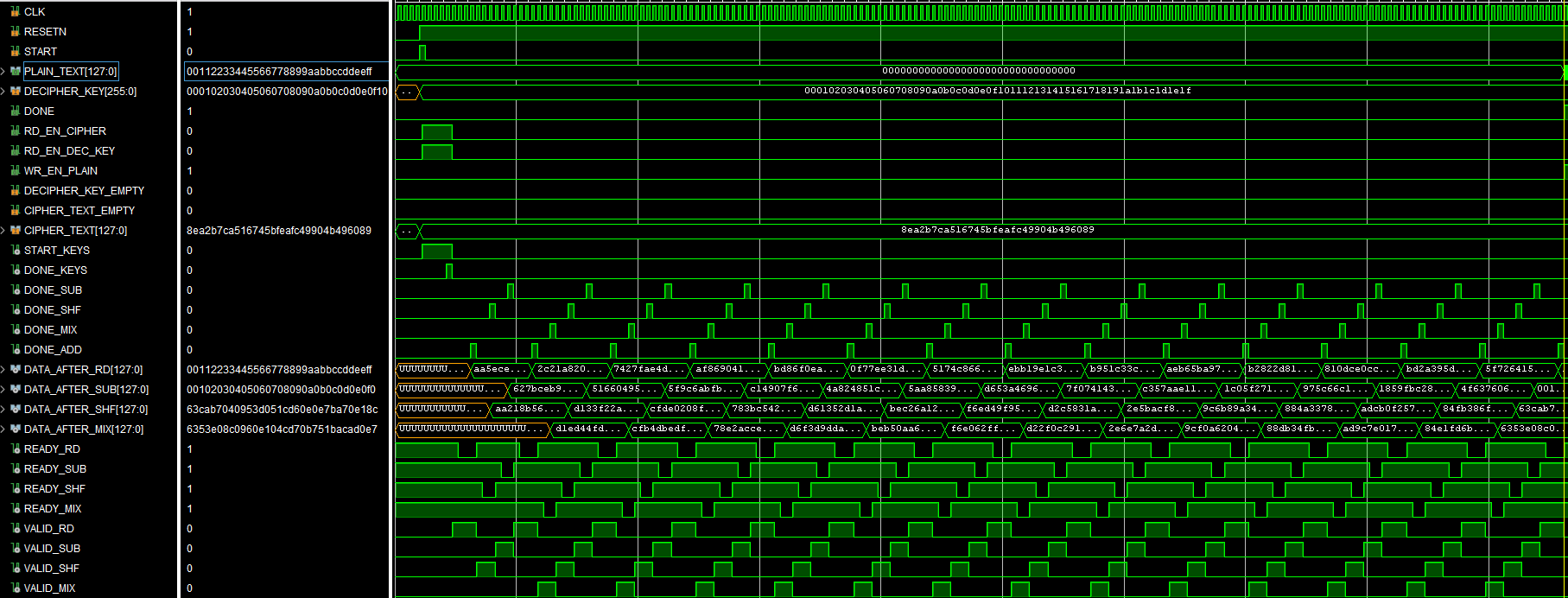


Figure 17 : Decrypt text timing signals