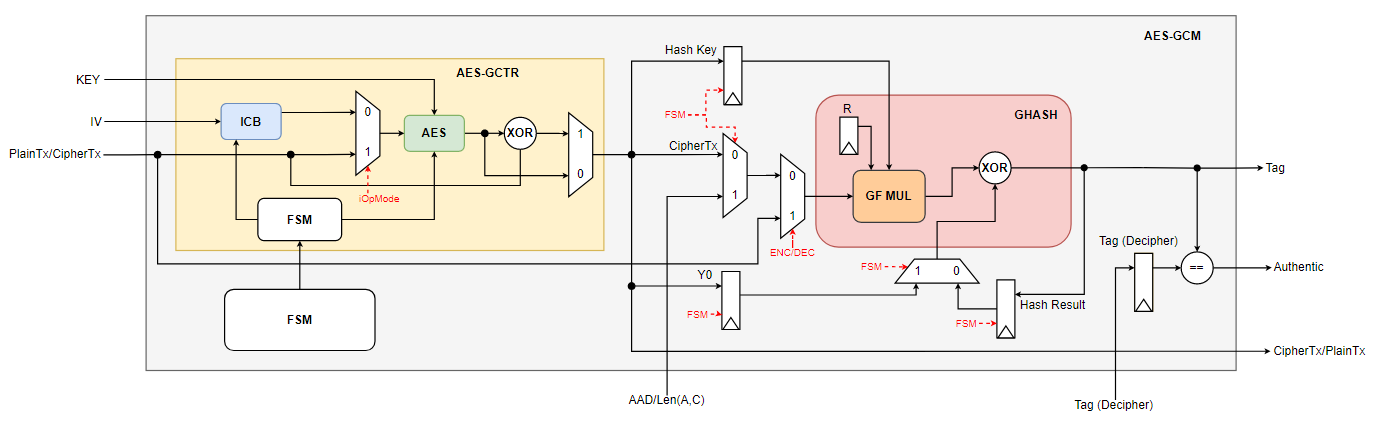
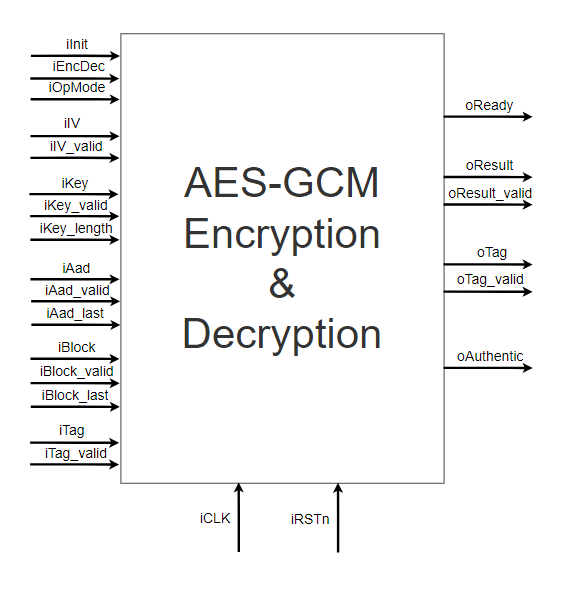
AES GCM

BLOCK DIAGRAM

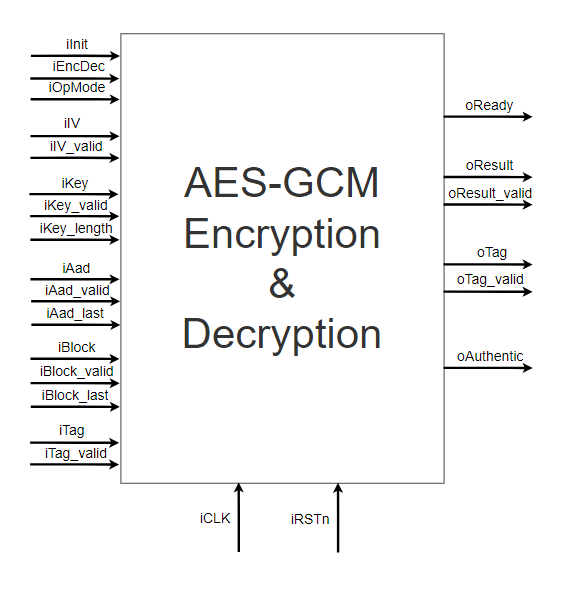
and STATE MACHINE

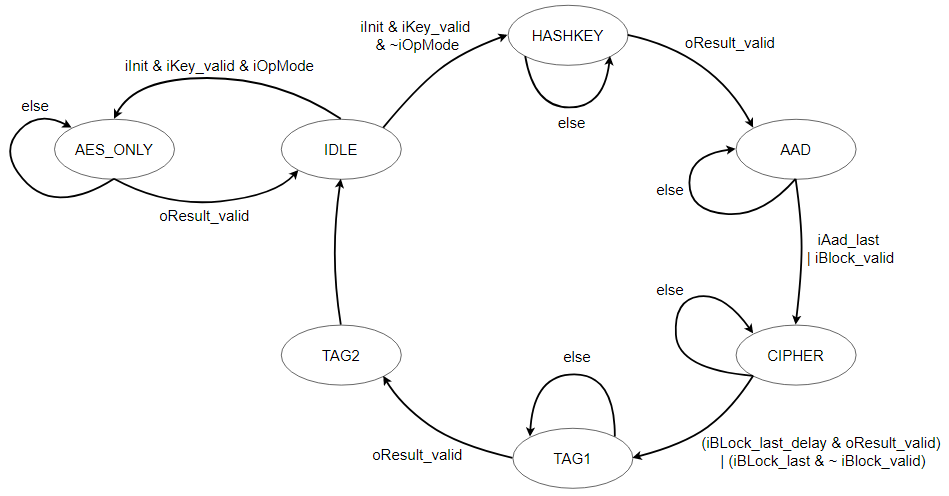
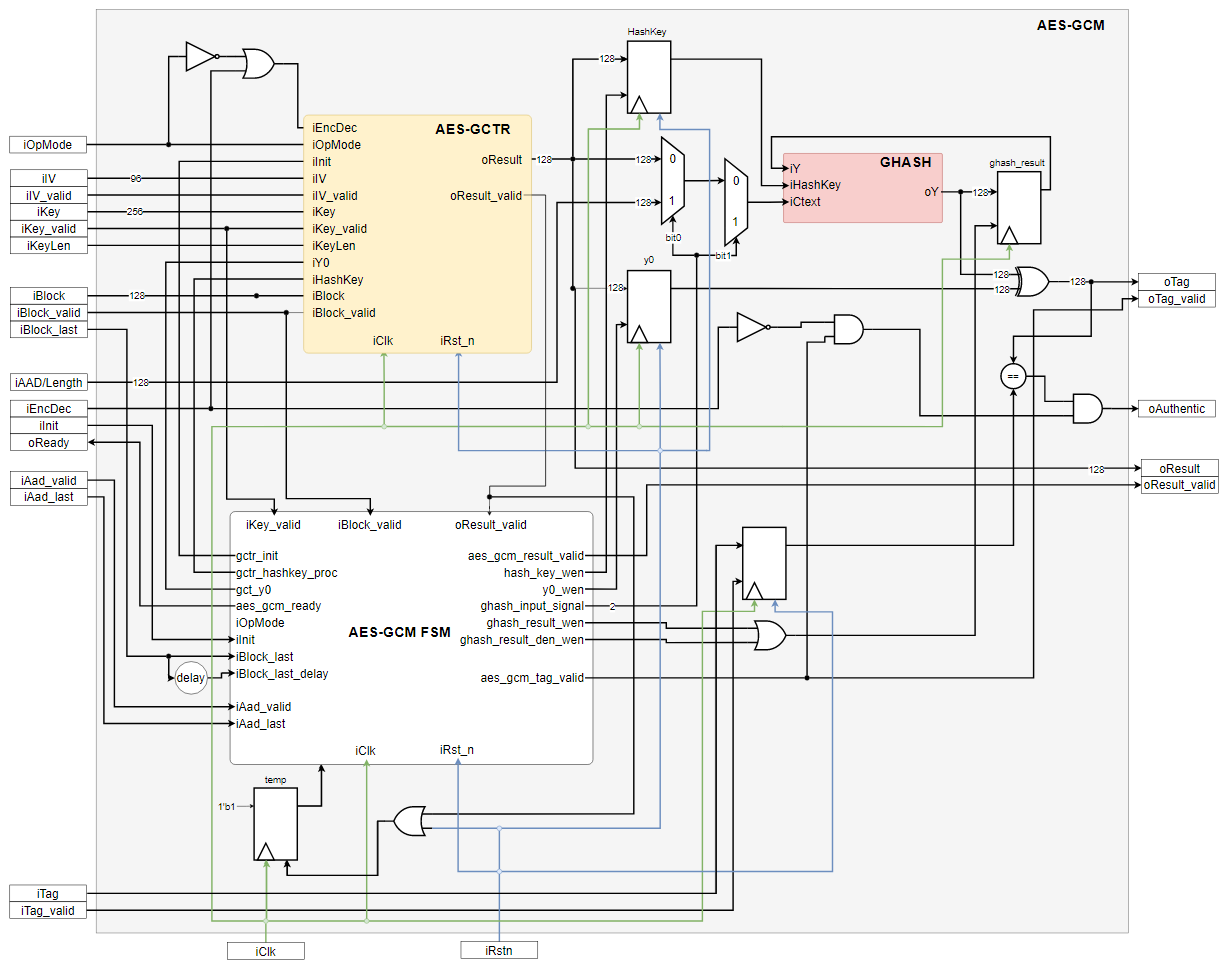


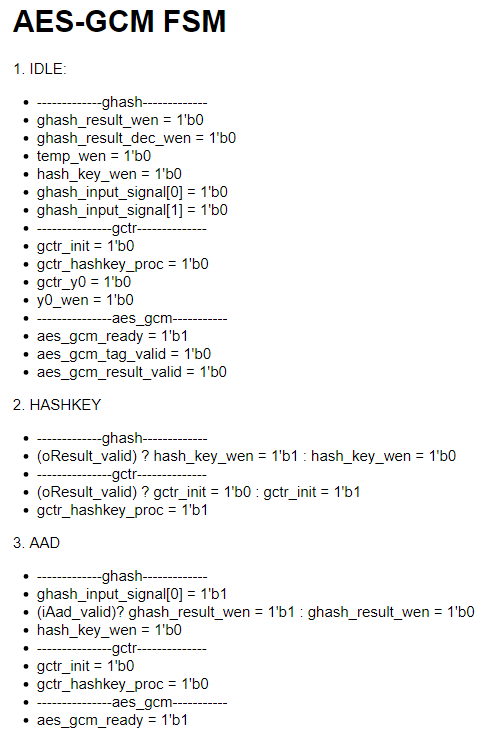
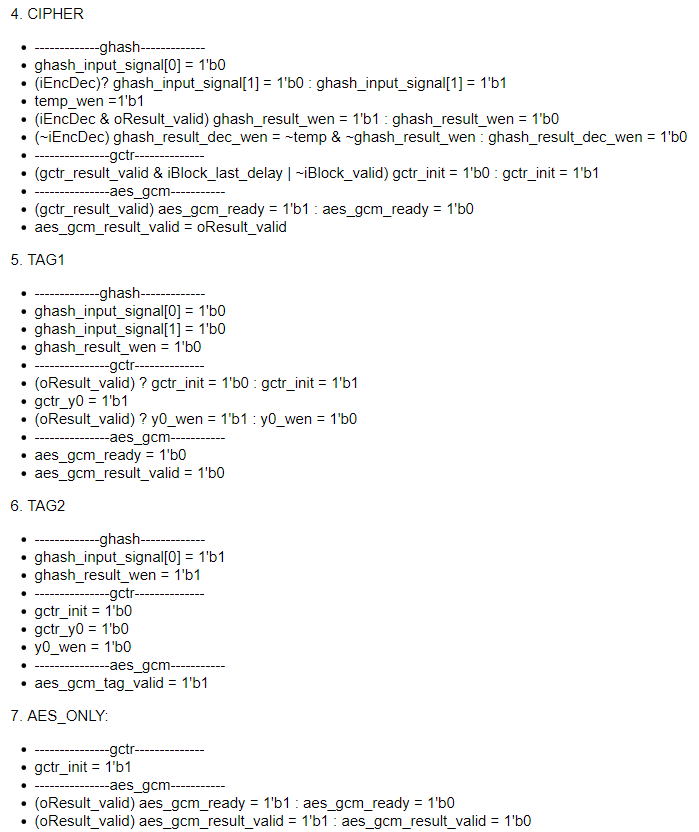
|  |  |  |  |
| --- | --- | --- | --- |
| PIN | Direction | Width | Description |
| iClk | Input | 1 | Clock |
| iRstn | Input | 1 | Negative edge reset: reset after using the core |
| iInit | Input | 1 | Initialize signal: assert when using the core |
| iEncDec | Input | 1 | Assert for Encryption, deassert for Decryption |
| iOpMode | Input | 1 | Operation Mode: assert for AES-GCM, deassert for AES only |
| oReady | Output | 1 | Output ready signal: input new data when ready is asserted |
| iIV | Input | 96 | 96-bit length IV |
| iIV\_valid | Input | 1 | When asserted, IV is valid |
| iKey | Input | 256 | Key |
| iKey\_valid | Input | 1 | When asserted, Key is valid |
| iKey\_len | Input | 1 | When asserted, Key length is 256-bit.  When deasserted, Key length is 128-bit. |
| iAad | Input | 128 | Additional Authentic Data or Length(A,C): when Ready = 1, change data every clock cycle |
| iAad\_valid | Input | 1 | When asserted, AAD is valid. |
| iAad\_last | Input | 1 | Asserted when input the last AAD data. |
| iBlock | Input | 128 | Input Plaintext or Ciphertext. |
| iBlock\_valid | Input | 1 | When asserted, Plaintext or Ciphertext is valid. |
| iBlock\_last | Input | 1 | Asserted when input the last Block data. |
| iTag | Input | 128 | Input Tag for authentication in Decryption mode |
| iTag\_valid | Input | 1 | When asserted, Tag is valid |
| oResult | Output | 128 | Output Ciphertext or Ciphertext |
| oResult\_valid | Output | 1 | When asserted, Result is valid |
| oTag | Output | 128 | Output Tag in Encryption mode. |
| oTag\_valid | Output | 1 | When asserted, output Tag is valid |
| oAuthentic | Output | 1 | When asserted, indicating authentic Block in Decryption mode. |

|  |  |
| --- | --- |
| Name | AES\_GCM |
| File | aes\_gcm.v |

|  |  |
| --- | --- |
| Submodule | File |
| AES\_GCTR | aes\_gcm.v |
| GHASH | ghash\_block.v |

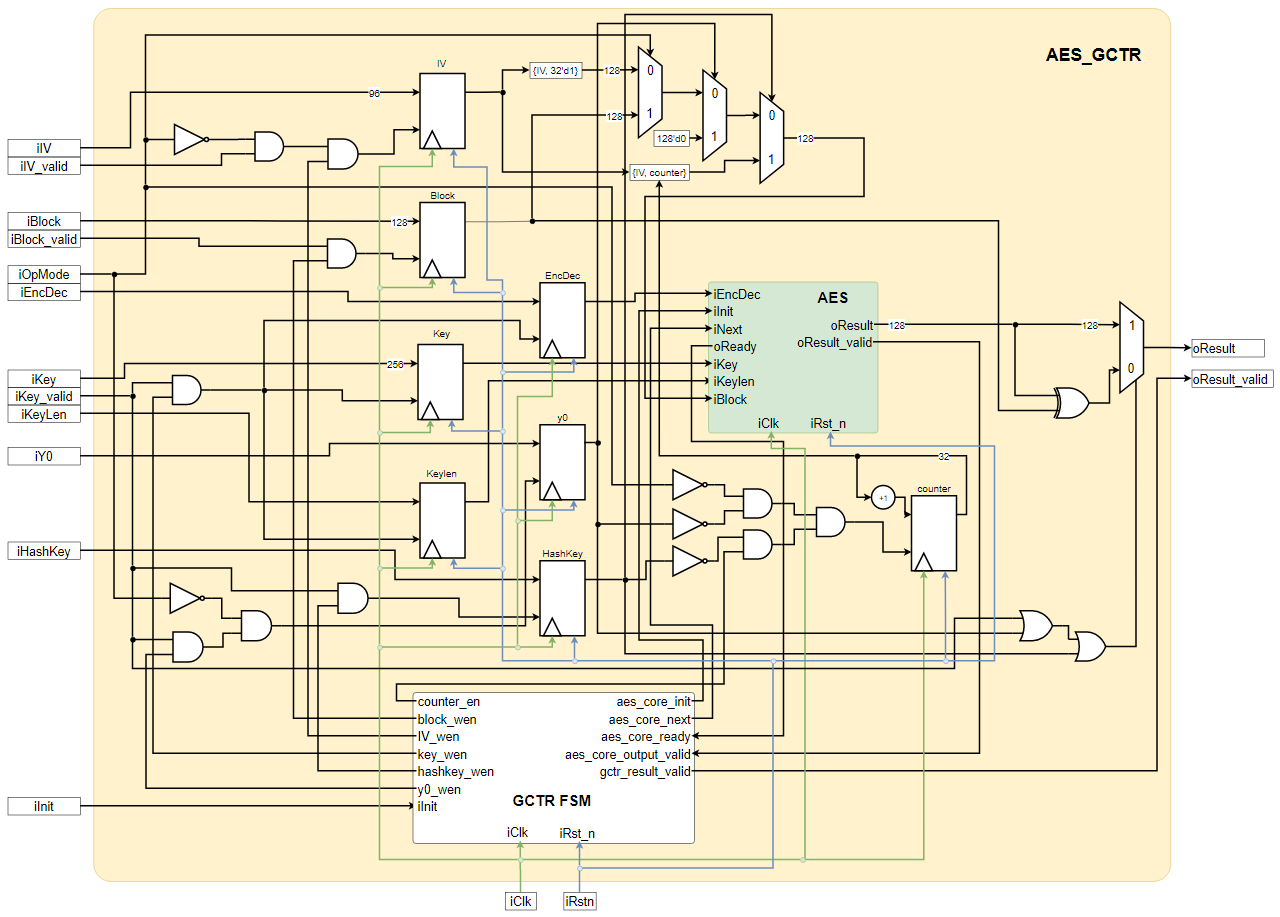
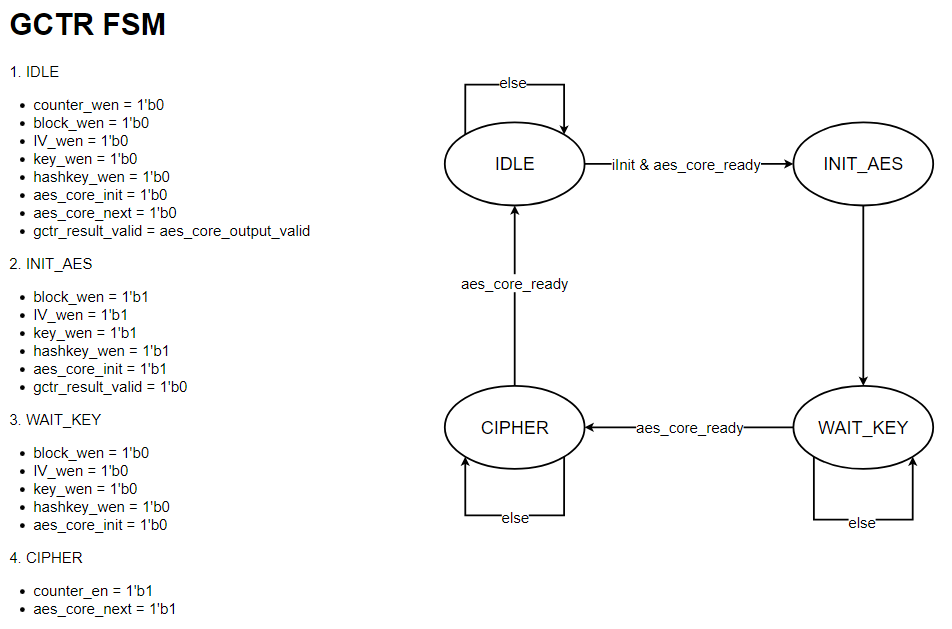
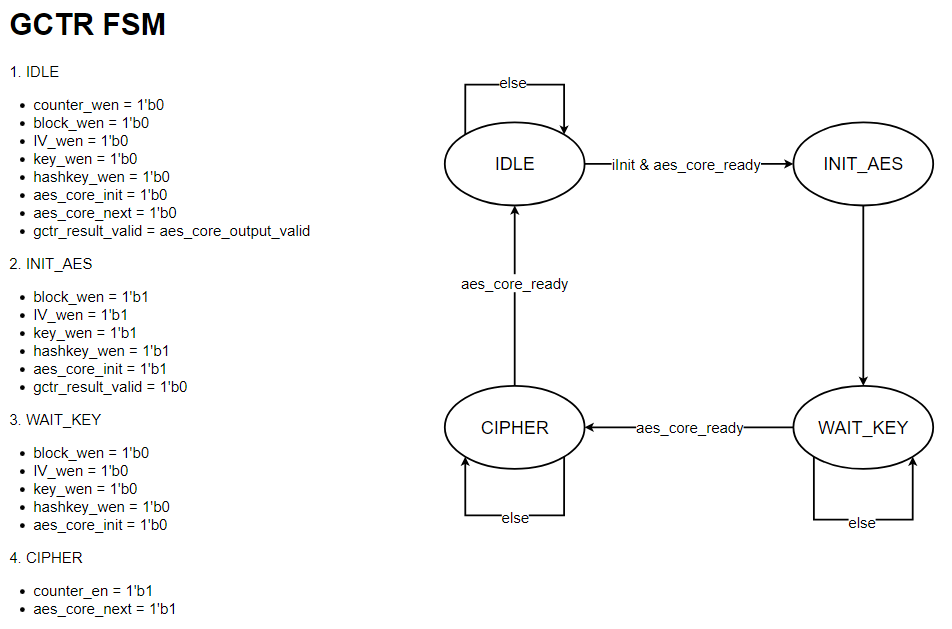
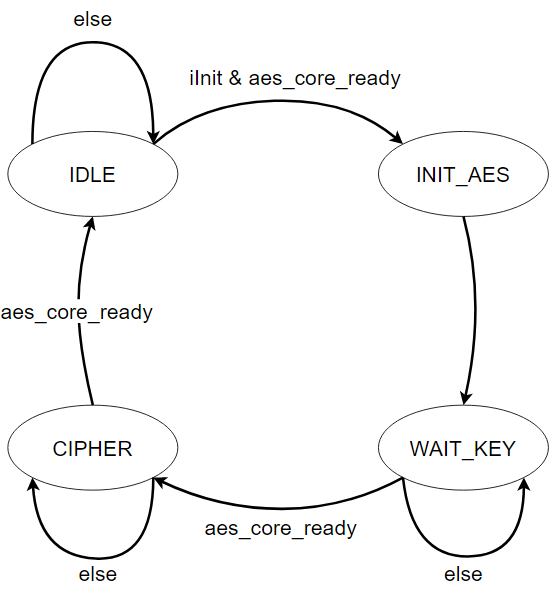
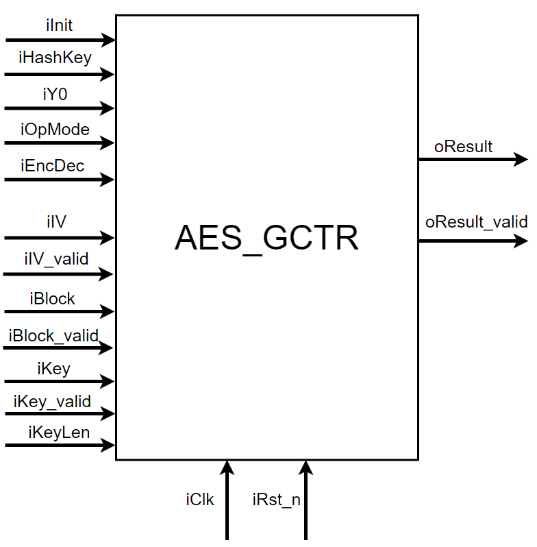


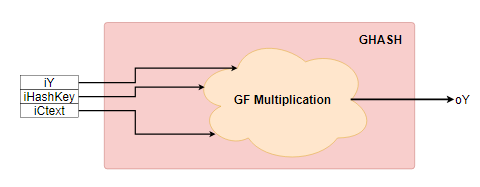


|  |  |
| --- | --- |
| Submodule | File |
| AES\_CORE | aes\_core.v |

|  |  |
| --- | --- |
| Name | AES\_GCM |
| File | aes\_gcm.v |

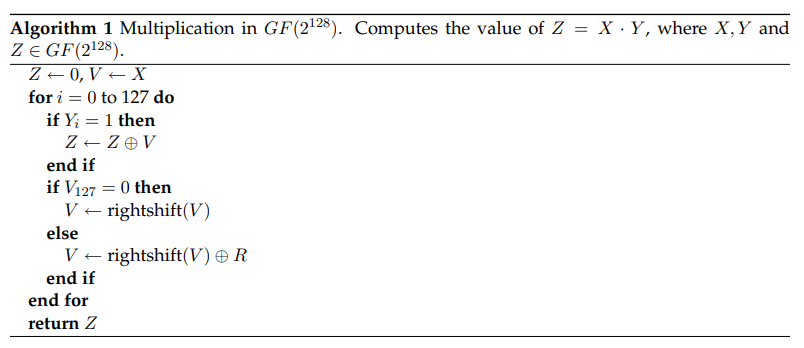


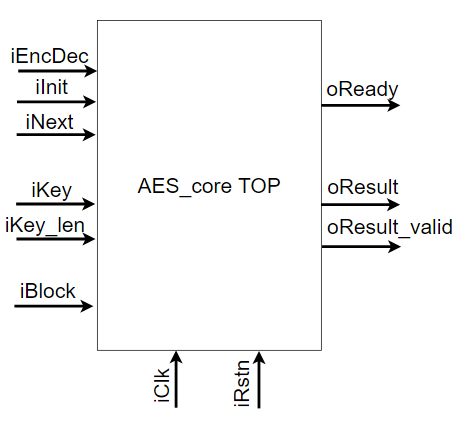


Multiplication in ***GF(2128)***

Each element is a vector of 128 bits. The **ith** bit of an element **X** is denoted as **X­­i**. The leftmost bit is **X­­i** and the rightmost bit is X127. The multiplication operation uses the special element **R = 1110001||0**, and is defined in Algorithm 1. The argument **rightshift()** moves the bits of its argument one bit to the right. More formally, whenever **W** = **rightshift(V)**, then **Wi** = **Vi-1**for 1 <= i <= 127 and **W0** = 0.

What we want to compute:



URL: [tee-hardware/hardware/teehw/optvsrc/AES at master · uec-hanken/tee-hardware (github.com)](https://github.com/uec-hanken/tee-hardware/tree/master/hardware/teehw/optvsrc/AES)