AES256GCM10G25G-IP Demo Instruction

AES256GCM10G25G-IP Demo Instruction

Rev2.01 1-Nov-2024

This document describes the instruction to demonstrate the operation of AES256GCM10G25G-IP on FPGA development boards. In the demonstration, AES256GCM10G25G-IP, called AESGCM-IP, is used to encrypt and decrypt data between two memories in FPGA and provide authentication tag. User can fill memory with Additional Authenticated Data (AAD), DataIn patterns, set encryption/decryption key, Initialization Vector (IV), and control test operation via Nios II Command Shell.

1 Environment Setup

To operate AESGCM-IP demo, please prepare following test environment.

1) FPGA development board (Arria10 SoC Development board).
2) Test PC.
3) Micro USB cable for JTAG connection between FPGA board and Test PC.
4) Quartus programmer for programming FPGA and Nios II command shell, installed on PC.
5) Demo configuration file (To download this file, please visit our web site at www.design-gateway.com).

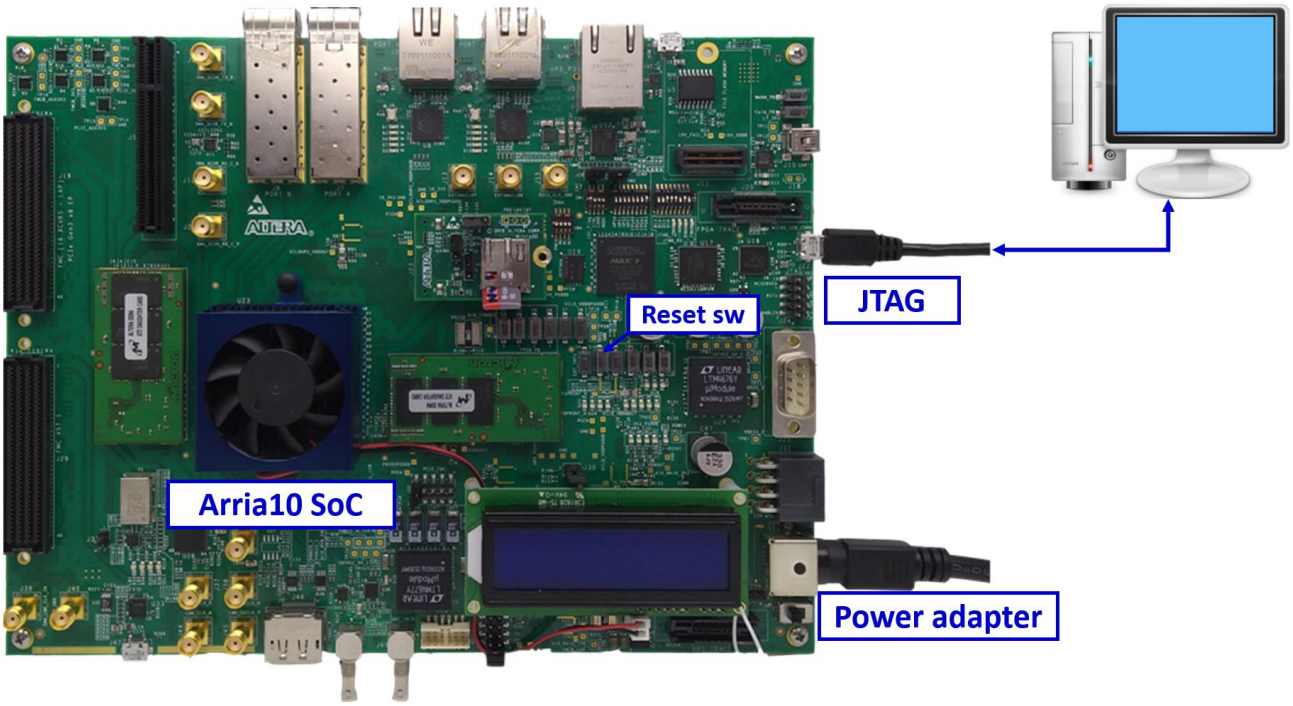

Figure 1 AESGCM-IP demo environment on Arria10 SoC board

2 FPGA development board setup

1) Make sure power switch is off and connect power supply to FPGA development board.
2) Connect USB cables between FPGA board and PC via micro-USB ports.
3) Turn on power switch for FPGA board.
4) Open Quartus Programmer to program FPGA through USB-1 by following step.
   i). Click “Hardware Setup…” to select
      – USB-BlasterII [USB-1] for Arria10 SoC
   ii). Click “Auto Detect” and select FPGA number.
   iii). Select FPGA device icon.
   iv). Click “Change File” button, select SOF file in pop-up window and click “open” button.
   v). Check “program”.
   vi). Click “Start” button to program FPGA.
   vii). Wait until Progress status is equal to 100%.

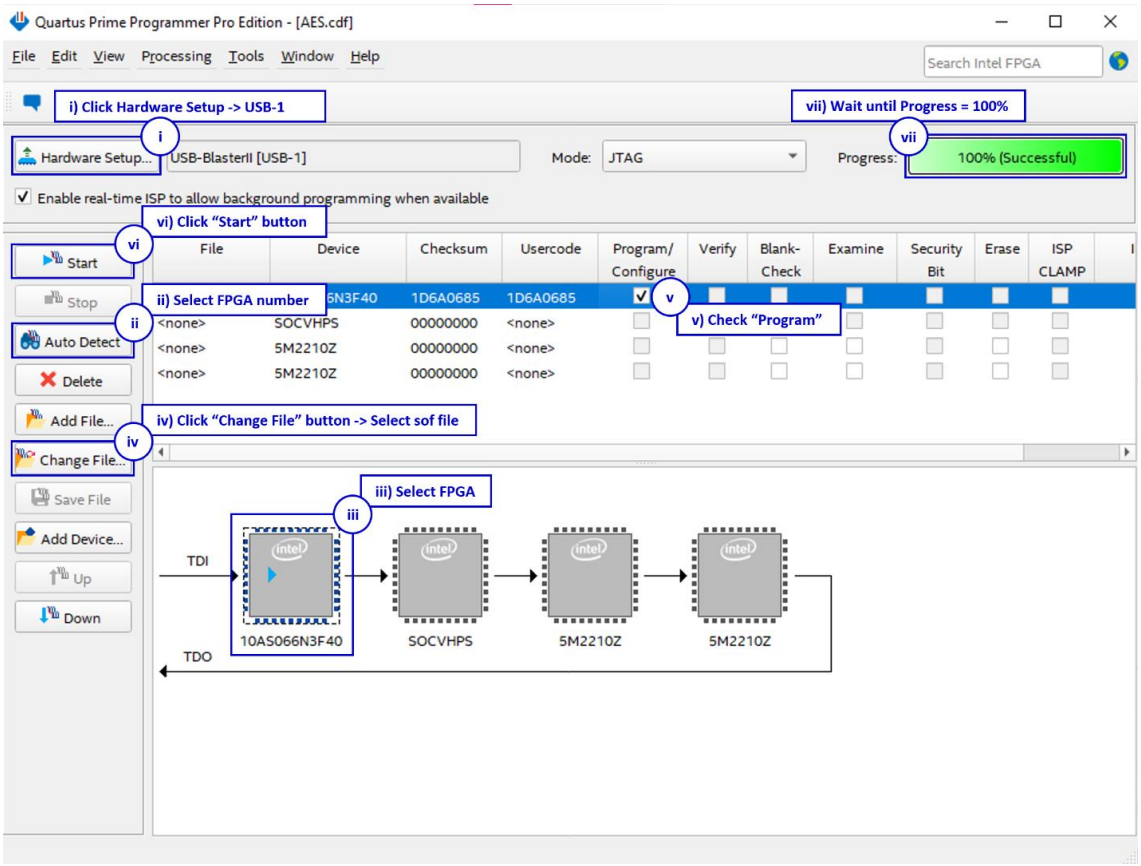

Figure 2 Program Device

For A10SoC after program SOF file complete, Quartus Prime will show popup message of Intel FPGA IP Evaluation Mode Status as shown in Figure 3. Please do not press cancel button.

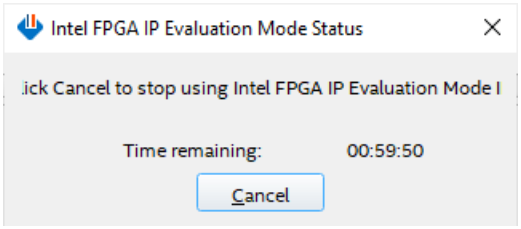

Figure 3 Intel FPGA IP Evaluation Mode Status

3 Nios II Command Shell

User can fill RAMs with AAD, plain or cipher data patterns, set encryption/decryption key, IV and control test operation via Nios II Command Shell. When configuration is completed, AESGCM-IP demo command menu will be displayed as shown in Figure 4. The detailed information of each menu is described in topic 4.

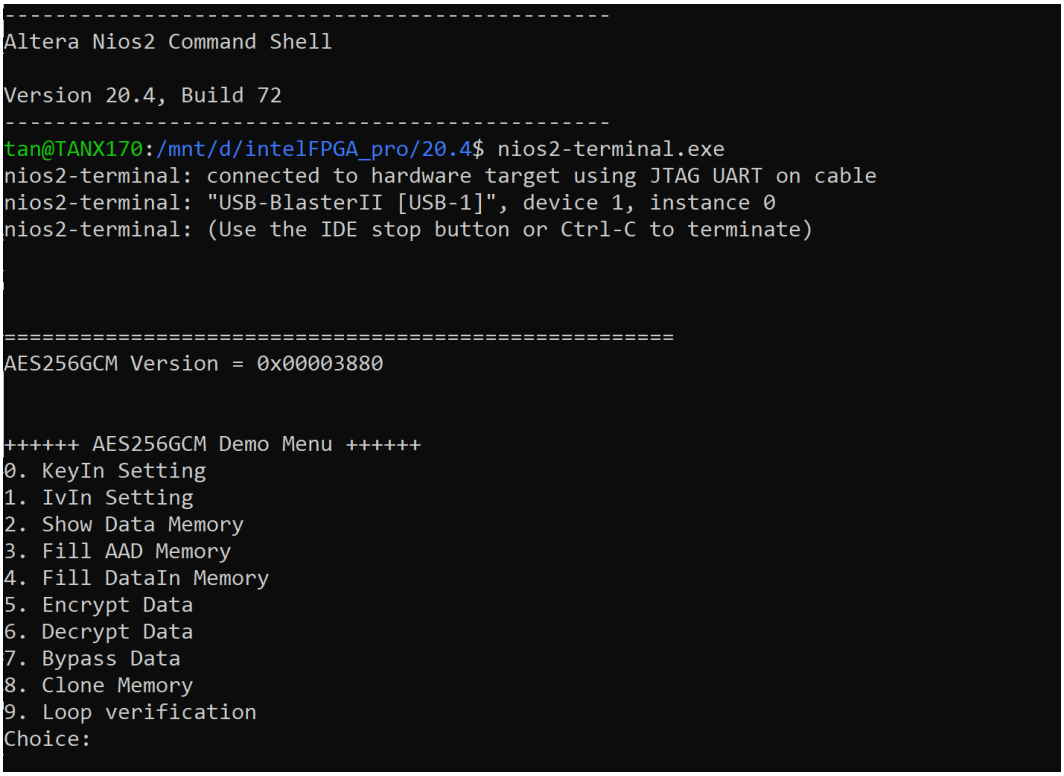

Figure 4 Nios II Command Shell

4 Command detail and testing result

4.1 KeyIn Setting

Step to set key as follows

a) Select “KeyIn Setting”.
b) Choose Key Size:
   - Enter 0 for 128-bit key.
   - Enter other for 256-bit key.
c) Current key will be displayed on Nios II Command Shell as shown in Figure 5.
d) Set new key: User is allowed to input new key in hex format or press “enter” to skip setting new key. Then the current key is printed again.

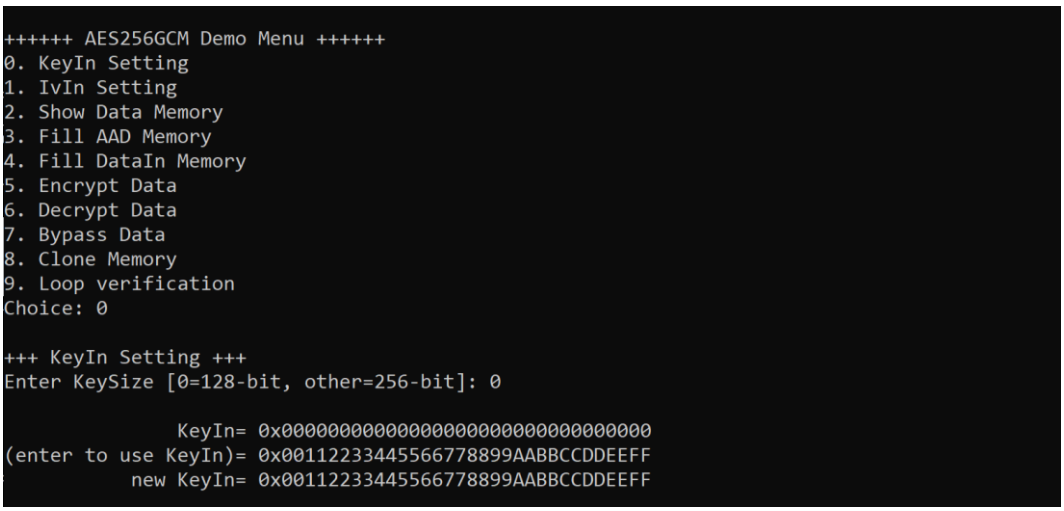

Figure 5 KeyIn setting example for 128-bit Key

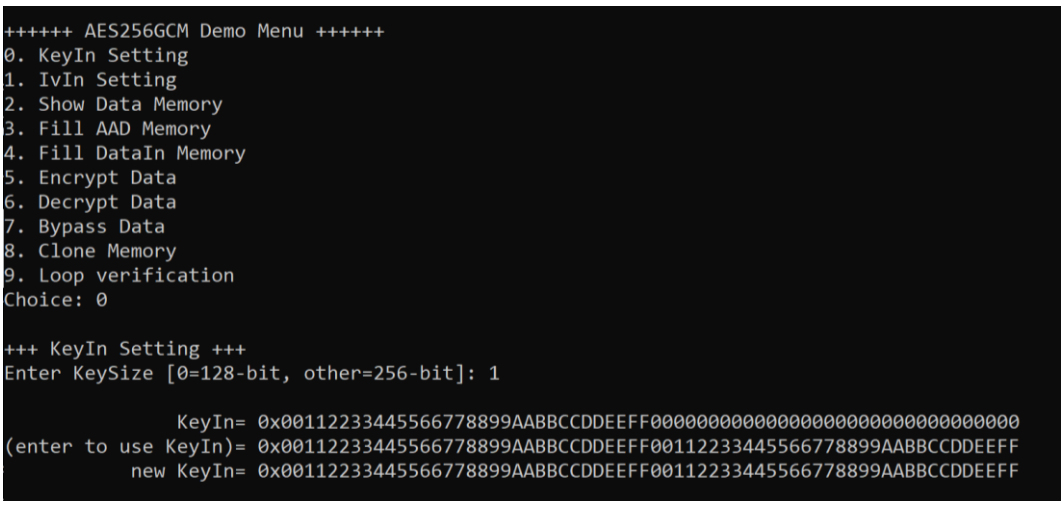

Figure 6 KeyIn setting example for 256-bit Key

4.2 IvIn Setting

Step to set IV as follows

a) Select “IvIn Setting”.
b) Current IV will be displayed on Nios II Command Shell as shown in Figure 7.
c) Set new IV: User is allowed to input new IV in hex format or press “enter” to skip setting new IV. Then the current IV is printed again.

```
++++++ AES256GCM Demo Menu ++++++
0. KeyIn Setting
1. IvIn Setting
2. Show Data Memory
3. Fill AAD Memory
4. Fill DataIn Memory
5. Encrypt Data
6. Decrypt Data
7. Bypass Data
8. Clone Memory
9. Loop verification
Choice: 1

+++ IvIn Setting +++
              IvIn= 0x00000000000000000000000
(enter to use IvIn)= 0x1001200f0011000f20003400
          new IvIn= 0x1001200F0011000F20003400
```

Figure 7 IvIn setting example

4.3 Show Data Memory

To show data in memory, user can select “Show Data Memory”. User can input the desired length of data in byte to show. The data length will be aligned to 128 bits. DataIn and DataOut will be displayed in table-form as shown in Figure 8. User can press “enter” to use 80 bytes as default value.

```
++++++ AES256GCM Demo Menu ++++++
0. KeyIn Setting
1. IvIn Setting
2. Show Data Memory
3. Fill AAD Memory
4. Fill DataIn Memory
5. Encrypt Data
6. Decrypt Data
7. Bypass Data
8. Clone Memory
9. Loop verification
Choice: 2

+++ Show Data Memory +++
Number of Data in byte (enter = 80):

               DataIn Memory                       DataOut Memory
Addr#  .0.....3 .4.....7 .8.....B .C.....F  .0.....3 .4.....7 .8.....B .C.....F
0000:  00000000 00000000 00000000 00000000  00000000 00000000 00000000 00000000
0001:  00000000 00000000 00000000 00000000  00000000 00000000 00000000 00000000
0002:  00000000 00000000 00000000 00000000  00000000 00000000 00000000 00000000
0003:  00000000 00000000 00000000 00000000  00000000 00000000 00000000 00000000
0004:  00000000 00000000 00000000 00000000  00000000 00000000 00000000 00000000
```

Figure 8 Displayed data when input the desired length of data

4.4 Fill AAD Memory

Step to set AAD as follows

a) Select “Fill AAD Memory”.
b) Input the desired length of AAD in byte. In case of zero-length AAD operation, user can input “0” or press “enter” then end process of this menu. In case of non-zero-length AAD, user can select AAD pattern as shown in Figure 9.
c) There are four pattern to fill AAD memory.
   a. zero pattern
   b. 8-bit counter
   c. 16-bit counter
   d. 32-bit counter
d) AAD memory will be filled with selected pattern by the number of AAD and zero-padding to become 128-bit padded data.

```
++++++ AES256GCM Demo Menu ++++++
0. KeyIn Setting
1. IvIn Setting
2. Show Data Memory
3. Fill AAD Memory
4. Fill DataIn Memory
5. Encrypt Data
6. Decrypt Data
7. Bypass Data
8. Clone Memory
9. Loop verification
Choice: 3

+++ Fill AAD Memory +++
Length of AAD in byte (enter = 0): 123
Choose AAD pattern
a. zero pattern
b. 8-bit counter
c. 16-bit counter
d. 32-bit counter
Choice: b

                DataIn Memory                          DataOut Memory
Addr#   .0.....3 .4.....7 .8.....B .C.....F   .0.....3 .4.....7 .8.....B .C.....F
0000:   00010203 04050607 08090A0B 0C0D0E0F   00000000 00000000 00000000 00000000
0001:   10111213 14151617 18191A1B 1C1D1E1F   00000000 00000000 00000000 00000000
0002:   20212223 24252627 28292A2B 2C2D2E2F   00000000 00000000 00000000 00000000
0003:   30313233 34353637 38393A3B 3C3D3E3F   00000000 00000000 00000000 00000000
0004:   40414243 44454647 48494A4B 4C4D4E4F   00000000 00000000 00000000 00000000
0005:   50515253 54555657 58595A5B 5C5D5E5F   00000000 00000000 00000000 00000000
0006:   60616263 64656667 68696A6B 6C6D6E6F   00000000 00000000 00000000 00000000
0007:   70717273 74757677 78797A00 00000000   00000000 00000000 00000000 00000000
```

Figure 9 Displayed data when set AAD pattern

4.5 Fill DataIn Memory

Step to fill DataIn in memory as follows

a) Select “Fill DataIn Memory”.
b) Input the desired length of data in byte. In case of zero-length DataIn operation, user can input “0” or press “enter” on keyboard then end process of this menu. In case of non-zero-length DataIn, user can select data pattern.
c) There are four pattern to fill memory.
   a. zero pattern
   b. 8-bit counter
   c. 16-bit counter
   d. 32-bit counter
d) Whole DataIn memory is filled with selected pattern after AAD according to the number of input data length as displayed in Figure 10.

```
++++++ AES256GCM Demo Menu ++++++
0. KeyIn Setting
1. IvIn Setting
2. Show Data Memory
3. Fill AAD Memory
4. Fill DataIn Memory
5. Encrypt Data
6. Decrypt Data
7. Bypass Data
8. Clone Memory
9. Loop verification
Choice: 4

+++ Fill DataIn Memory +++
Length of DataIn in byte (enter = 0): 112
Choose DataIn pattern
a. zero pattern
b. 8-bit counter
c. 16-bit counter
d. 32-bit counter
Choice: c

               DataIn Memory                        DataOut Memory
Addr#  .0.....3 .4.....7 .8.....B .C.....F  .0.....3 .4.....7 .8.....B .C.....F
0000:  00010203 04050607 08090A0B 0C0D0E0F  00000000 00000000 00000000 00000000
0001:  10111213 14151617 18191A1B 1C1D1E1F  00000000 00000000 00000000 00000000
0002:  20212223 24252627 28292A2B 2C2D2E2F  00000000 00000000 00000000 00000000
0003:  30313233 34353637 38393A3B 3C3D3E3F  00000000 00000000 00000000 00000000
0004:  40414243 44454647 48494A4B 4C4D4E4F  00000000 00000000 00000000 00000000
0005:  50515253 54555657 58595A5B 5C5D5E5F  00000000 00000000 00000000 00000000
0006:  60616263 64656667 68696A6B 6C6D6E6F  00000000 00000000 00000000 00000000
0007:  70717273 74757677 78797A00 00000000  00000000 00000000 00000000 00000000
0008:  00000001 00020003 00040005 00060007  00000000 00000000 00000000 00000000
0009:  00080009 000A000B 000C000D 000E000F  00000000 00000000 00000000 00000000
000A:  00100011 00120013 00140015 00160017  00000000 00000000 00000000 00000000
000B:  00180019 001A001B 001C001D 001E001F  00000000 00000000 00000000 00000000
000C:  00200021 00220023 00240025 00260027  00000000 00000000 00000000 00000000
000D:  00280029 002A002B 002C002D 002E002F  00000000 00000000 00000000 00000000
000E:  00300031 00320033 00340035 00360037  00000000 00000000 00000000 00000000
```

Figure 10 Displayed data when set DataIn length and data pattern

4.6 Encrypt Data

Select “Encrypt Data” to encrypt DataIn in memory. Current length of AAD and length of DataIn are printed on Nios II Command Shell. When the encryption process is finished, both DataIn and DataOut will be displayed in table-form and 128-bit encryption tag will be printed as shown in Figure 11.

```
++++++ AES256GCM Demo Menu ++++++
0. KeyIn Setting
1. IvIn Setting
2. Show Data Memory
3. Fill AAD Memory
4. Fill DataIn Memory
5. Encrypt Data
6. Decrypt Data
7. Bypass Data
8. Clone Memory
9. Loop verification
Choice: 5

+++ Encrypt Data +++
Length of encrypt-AAD : 123 byte
Length of encrypt-Data : 112 byte

               DataIn Memory                         DataOut Memory
Addr#  .0.....3 .4.....7 .8.....B .C.....F  .0.....3 .4.....7 .8.....B .C.....F
0000:  00010203 04050607 08090A0B 0C0D0E0F  00010203 04050607 08090A0B 0C0D0E0F
0001:  10111213 14151617 18191A1B 1C1D1E1F  10111213 14151617 18191A1B 1C1D1E1F
0002:  20212223 24252627 28292A2B 2C2D2E2F  20212223 24252627 28292A2B 2C2D2E2F
0003:  30313233 34353637 38393A3B 3C3D3E3F  30313233 34353637 38393A3B 3C3D3E3F
0004:  40414243 44454647 48494A4B 4C4D4E4F  40414243 44454647 48494A4B 4C4D4E4F
0005:  50515253 54555657 58595A5B 5C5D5E5F  50515253 54555657 58595A5B 5C5D5E5F
0006:  60616263 64656667 68696A6B 6C6D6E6F  60616263 64656667 68696A6B 6C6D6E6F
0007:  70717273 74757677 78797A00 00000000  70717273 74757677 78797A00 00000000
0008:  00000001 00020003 00040005 00060007  DDF0CA11 4C764E96 86BE4884 96BDCDBF
0009:  00080009 000A000B 000C000D 000E000F  7042B8F5 E7992D9D 7E05B475 BCFAE8A0
000A:  00100011 00120013 00140015 00160017  404C4651 0009B5EC FC8DE8D5 4A474C9C
000B:  00180019 001A001B 001C001D 001E001F  A8C9D384 D9D9AF2E BCDAC47C 56D4D92E
000C:  00200021 00220023 00240025 00260027  61B102ED 06055796 7FB29D51 B7D7B39E
000D:  00280029 002A002B 002C002D 002E002F  A6BF1270 D6CD8386 87C0E35B EB06EB91
000E:  00300031 00320033 00340035 00360037  8BDDCDD5 AD42B614 7FA7BFBB 3EAD73F9


Tag : 32E2954A01B49F9D94C8FE237A510D36
```

Figure 11 Nios II Command Shell after finished encryption process

4.7 Decrypt Data

Select “Decrypt Data” to decrypt DataIn in memory. Current length of AAD and length of DataIn are printed on Nios II Command Shell. When the decryption process is finished, both DataIn and DataOut will be displayed in table-form and 128-bit decryption tag will be printed as shown in Figure 12.

```
++++++ AES256GCM Demo Menu ++++++
0. KeyIn Setting
1. IvIn Setting
2. Show Data Memory
3. Fill AAD Memory
4. Fill DataIn Memory
5. Encrypt Data
6. Decrypt Data
7. Bypass Data
8. Clone Memory
9. Loop verification
Choice: 6

+++ Decrypt Data +++
Length of decrypt-AAD : 123 byte
Length of decrypt-Data : 112 byte

                DataIn Memory                          DataOut Memory
Addr#  .0.....3 .4.....7 .8.....B .C.....F  .0.....3 .4.....7 .8.....B .C.....F
0000:  00010203 04050607 08090A0B 0C0D0E0F  00010203 04050607 08090A0B 0C0D0E0F
0001:  10111213 14151617 18191A1B 1C1D1E1F  10111213 14151617 18191A1B 1C1D1E1F
0002:  20212223 24252627 28292A2B 2C2D2E2F  20212223 24252627 28292A2B 2C2D2E2F
0003:  30313233 34353637 38393A3B 3C3D3E3F  30313233 34353637 38393A3B 3C3D3E3F
0004:  40414243 44454647 48494A4B 4C4D4E4F  40414243 44454647 48494A4B 4C4D4E4F
0005:  50515253 54555657 58595A5B 5C5D5E5F  50515253 54555657 58595A5B 5C5D5E5F
0006:  60616263 64656667 68696A6B 6C6D6E6F  60616263 64656667 68696A6B 6C6D6E6F
0007:  70717273 74757677 78797A00 00000000  70717273 74757677 78797A00 00000000
0008:  00000001 00020003 00040005 00060007  DDF0CA11 4C764E96 86BE4884 96BDCDBF
0009:  00080009 000A000B 000C000D 000E000F  7042B8F5 E7992D9D 7E05B475 BCFAE8A0
000A:  00100011 00120013 00140015 00160017  404C4651 0009B5EC FC8DE8D5 4A474C9C
000B:  00180019 001A001B 001C001D 001E001F  A8C9D384 D9D9AF2E BCDAC47C 56D4D92E
000C:  00200021 00220023 00240025 00260027  61B102ED 06055796 7FB29D51 B7D7B39E
000D:  00280029 002A002B 002C002D 002E002F  A6BF1270 D6CD8386 87C0E35B EB06EB91
000E:  00300031 00320033 00340035 00360037  8BDDCDD5 AD42B614 7FA7BFBB 3EAD73F9


Tag : 38D40A66DE0401DA37C47D215A4FF9C4
```

Figure 12 Nios II Command Shell after finished decryption process

4.8 Bypass Data

Select “Bypass Data” to Bypass DataIn in memory. Current length of AAD and length of DataIn are printed on Nios II Command Shell. When the Bypass process is finished, both DataIn and DataOut will be displayed in table-form as shown in Figure 13.

```
++++++ AES256GCM Demo Menu ++++++
0. KeyIn Setting
1. IvIn Setting
2. Show Data Memory
3. Fill AAD Memory
4. Fill DataIn Memory
5. Encrypt Data
6. Decrypt Data
7. Bypass Data
8. Clone Memory
9. Loop verification
Choice: 7

+++ Bypass Data +++
Length of decrypt-AAD : 123 byte
Length of decrypt-Data : 112 byte

               DataIn Memory                          DataOut Memory
Addr#  .0.....3 .4.....7 .8.....B .C.....F  .0.....3 .4.....7 .8.....B .C.....F
0000:  00010203 04050607 08090A0B 0C0D0E0F  00010203 04050607 08090A0B 0C0D0E0F
0001:  10111213 14151617 18191A1B 1C1D1E1F  10111213 14151617 18191A1B 1C1D1E1F
0002:  20212223 24252627 28292A2B 2C2D2E2F  20212223 24252627 28292A2B 2C2D2E2F
0003:  30313233 34353637 38393A3B 3C3D3E3F  30313233 34353637 38393A3B 3C3D3E3F
0004:  40414243 44454647 48494A4B 4C4D4E4F  40414243 44454647 48494A4B 4C4D4E4F
0005:  50515253 54555657 58595A5B 5C5D5E5F  50515253 54555657 58595A5B 5C5D5E5F
0006:  60616263 64656667 68696A6B 6C6D6E6F  60616263 64656667 68696A6B 6C6D6E6F
0007:  70717273 74757677 78797A00 00000000  70717273 74757677 78797A00 00000000
0008:  00000001 00020003 00040005 00060007  00000001 00020003 00040005 00060007
0009:  00080009 000A000B 000C000D 000E000F  00080009 000A000B 000C000D 000E000F
000A:  00100011 00120013 00140015 00160017  00100011 00120013 00140015 00160017
000B:  00180019 001A001B 001C001D 001E001F  00180019 001A001B 001C001D 001E001F
000C:  00200021 00220023 00240025 00260027  00200021 00220023 00240025 00260027
000D:  00280029 002A002B 002C002D 002E002F  00280029 002A002B 002C002D 002E002F
000E:  00300031 00320033 00340035 00360037  00300031 00320033 00340035 00360037
```

Figure 13 Nios II Command Shell after finished Bypass process

4.9 Clone Memory

Select “Clone Memory” for copy DataOut memory to DataIn memory. When the process is finished, both DataIn and DataOut will be displayed in table-form as shown in Figure 14.

```
++++++ AES256GCM Demo Menu ++++++
0. KeyIn Setting
1. IvIn Setting
2. Show Data Memory
3. Fill AAD Memory
4. Fill DataIn Memory
5. Encrypt Data
6. Decrypt Data
7. Bypass Data
8. Clone Memory
9. Loop verification
Choice: 8

+++ Clone Memory +++

                DataIn Memory                          DataOut Memory
Addr#  .0.....3 .4.....7 .8.....B .C.....F  .0.....3 .4.....7 .8.....B .C.....F
0000:  00010203 04050607 08090A0B 0C0D0E0F  00010203 04050607 08090A0B 0C0D0E0F
0001:  10111213 14151617 18191A1B 1C1D1E1F  10111213 14151617 18191A1B 1C1D1E1F
0002:  20212223 24252627 28292A2B 2C2D2E2F  20212223 24252627 28292A2B 2C2D2E2F
0003:  30313233 34353637 38393A3B 3C3D3E3F  30313233 34353637 38393A3B 3C3D3E3F
0004:  40414243 44454647 48494A4B 4C4D4E4F  40414243 44454647 48494A4B 4C4D4E4F
0005:  50515253 54555657 58595A5B 5C5D5E5F  50515253 54555657 58595A5B 5C5D5E5F
0006:  60616263 64656667 68696A6B 6C6D6E6F  60616263 64656667 68696A6B 6C6D6E6F
0007:  70717273 74757677 78797A00 00000000  70717273 74757677 78797A00 00000000
0008:  00000001 00020003 00040005 00060007  00000001 00020003 00040005 00060007
0009:  00080009 000A000B 000C000D 000E000F  00080009 000A000B 000C000D 000E000F
000A:  00100011 00120013 00140015 00160017  00100011 00120013 00140015 00160017
000B:  00180019 001A001B 001C001D 001E001F  00180019 001A001B 001C001D 001E001F
000C:  00200021 00220023 00240025 00260027  00200021 00220023 00240025 00260027
000D:  00280029 002A002B 002C002D 002E002F  00280029 002A002B 002C002D 002E002F
000E:  00300031 00320033 00340035 00360037  00300031 00320033 00340035 00360037
```

Figure 14 Nios II Command Shell after finished Clone Memory process

4.10 Loop verification

Select “Loop verification”, to check both encryption and decryption. In this menu, DataIn in memory will be encrypted/decrypted with all current parameters (key, IV, AAD and data in DataIn memory).

The function begins by read and store data from the DataIn memory as an original data and clear the DataOut memory before encryption, then start encryption process. After the encryption is completed, the data from the DataOut memory is cloned to the DataIn memory and decryption process is performed. Once the decryption is completed, the decrypted data is compared with the original data, and the encryption tag is compared with the decryption tag.

If the decrypted data and decryption tag match with original data and encryption tag, respectively, “Loop verification succeeded.” is printed on Nios II Command Shell as shown in Figure 15.

```
++++++ AES256GCM Demo Menu ++++++
0. KeyIn Setting
1. IvIn Setting
2. Show Data Memory
3. Fill AAD Memory
4. Fill DataIn Memory
5. Encrypt Data
6. Decrypt Data
7. Bypass Data
8. Clone Memory
9. Loop verification
Choice: 9

+++ Loop verification +++

KeyIn= 0x00112233445566778899AABBCCDDEEFF00112233445566778899AABBCCDDEEFF
 IvIn= 0x1001200F0011000F20003400
Length of encrypt-AAD  : 62 byte
Length of encrypt-Data : 56 byte

               Original Data                         Encrypted Data
Addr#  .0.....3 .4.....7 .8.....B .C.....F  .0.....3 .4.....7 .8.....B .C.....F
0000:  00010203 04050607 08090A0B 0C0D0E0F  00010203 04050607 08090A0B 0C0D0E0F
0001:  10111213 14151617 18191A1B 1C1D1E1F  10111213 14151617 18191A1B 1C1D1E1F
0002:  20212223 24252627 28292A2B 2C2D2E2F  20212223 24252627 28292A2B 2C2D2E2F
0003:  30313233 34353637 38393A3B 3C3D0000  30313233 34353637 38393A3B 3C3D0000
0004:  00000001 00020003 00040005 00060007  DDF0CA11 4C764E96 86BE4884 96BDCDBF
0005:  00080009 000A000B 000C000D 000E000F  7042B8F5 E7992D9D 7E05B475 BCFAE8A0
0006:  00100011 00120013 00140015 00160017  404C4651 0009B5EC FC8DE8D5 4A474C9C
0007:  00180019 001A001B 00000000 00000000  A8C9D384 D9D9AF2E 00000000 00000000

Encrypted Tag : 404544F835F7E98DF1376D210D48FF2A

              Encrypted Data                         Decrypted Data
Addr#  .0.....3 .4.....7 .8.....B .C.....F  .0.....3 .4.....7 .8.....B .C.....F
0000:  00010203 04050607 08090A0B 0C0D0E0F  00010203 04050607 08090A0B 0C0D0E0F
0001:  10111213 14151617 18191A1B 1C1D1E1F  10111213 14151617 18191A1B 1C1D1E1F
0002:  20212223 24252627 28292A2B 2C2D2E2F  20212223 24252627 28292A2B 2C2D2E2F
0003:  30313233 34353637 38393A3B 3C3D0000  30313233 34353637 38393A3B 3C3D0000
0004:  DDF0CA11 4C764E96 86BE4884 96BDCDBF  00000001 00020003 00040005 00060007
0005:  7042B8F5 E7992D9D 7E05B475 BCFAE8A0  00080009 000A000B 000C000D 000E000F
0006:  404C4651 0009B5EC FC8DE8D5 4A474C9C  00100011 00120013 00140015 00160017
0007:  A8C9D384 D9D9AF2E 00000000 00000000  00180019 001A001B 00000000 00000000

Decrypted Tag : 404544F835F7E98DF1376D210D48FF2A
Loop verification succeeded.
```

Figure 15 Nios II Command Shell after loop verification is succeeded

5 Revision History

Revision	Date (D-M-Y)	Description
2.01	1-Nov-24	- Revise wording. - Correct missing cross-reference.
2.00	14-Oct-24	Update KeyIn Setting command
1.03	20-Jan-23	- Add Bypass feature. - Improve performance.
1.02	27-Oct-22	Update description for new design
1.00	17-Jun-22	Initial version release

