ChaCha20Poly1305-IP Demo Instruction

ChaCha20Poly1305-IP Demo Instruction

Rev1.00 31-Jul-2026

This document describes the instruction to demonstrate the operation of ChaCha20Poly1305-IP Arria10 SoC Board. In the demonstration, ChaCha20Poly1305-IP is used to encrypt/decrypt data between two memories in FPGA and provide authentication tag. User can fill memory with Additional Authenticated Data (AAD) and Input Data, set encryption/decryption key and Initialization Vector (IV), and control test operation via serial console.

1 Environment Setup

To operate ChaCha20Poly1305-IP demo, please prepare the following test environment.

1) FPGA 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 command shell, installed on PC.
5) Demo configuration file (To download this file, please visit our web site at www.design-gateway.com).

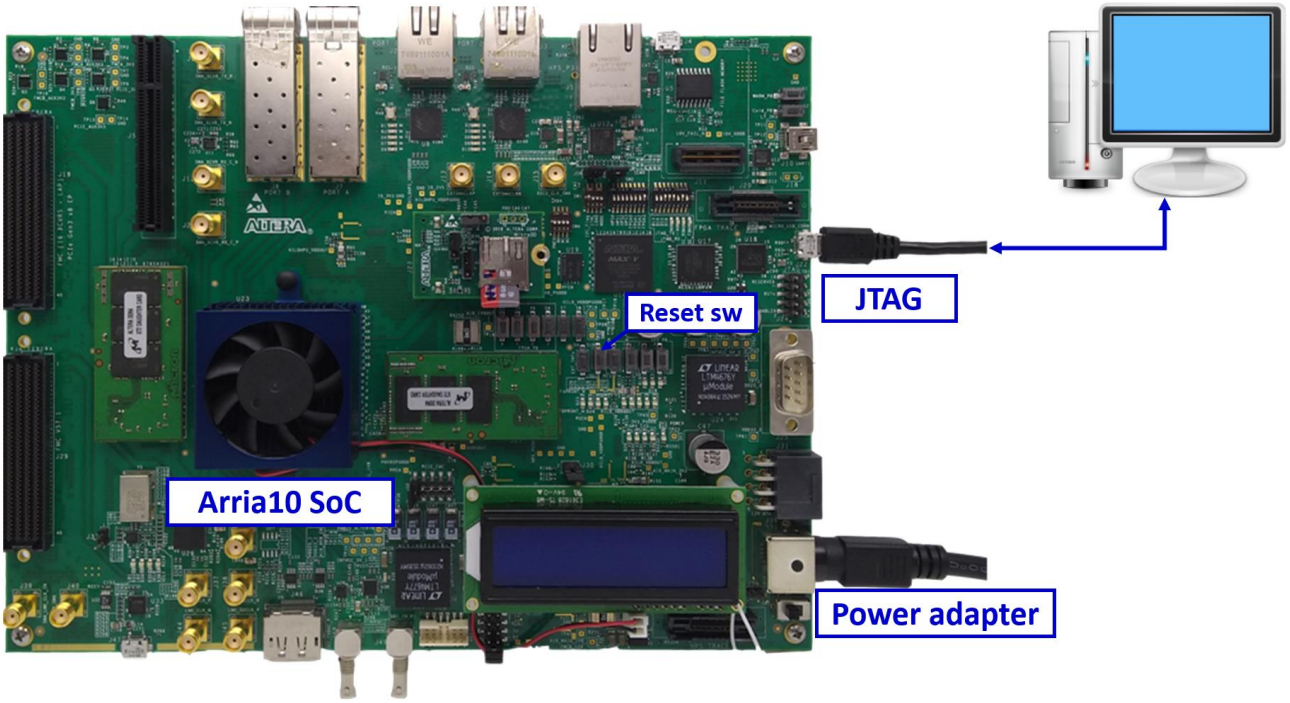

Figure 1 ChaCha20Poly1305-IP demo environment on Arria10 SoC board

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]
   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%.

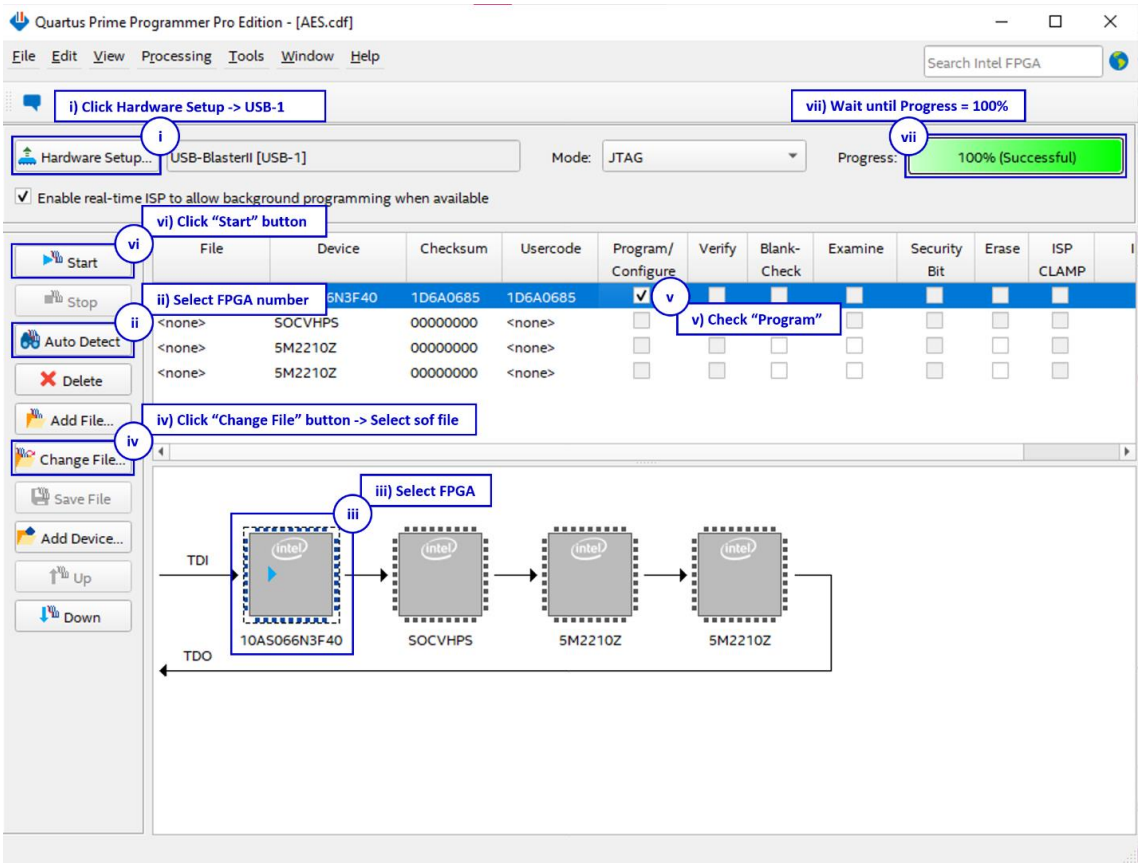

Figure 2 Program device

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

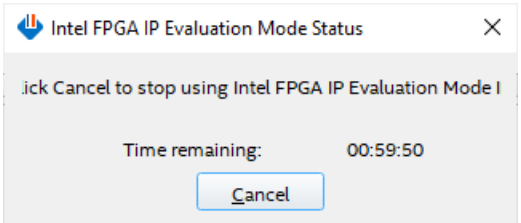

Figure 3 Intel FPGA IP evaluation mode status

3 Nios Command Shell

User can fill RAMs with AAD, IV, Input Data, and encryption/decryption key via Nios II Command Shell. The current parameters are shown together with the available options in the main menu as shown in Figure 4. The details of each menu are described in topic 4.

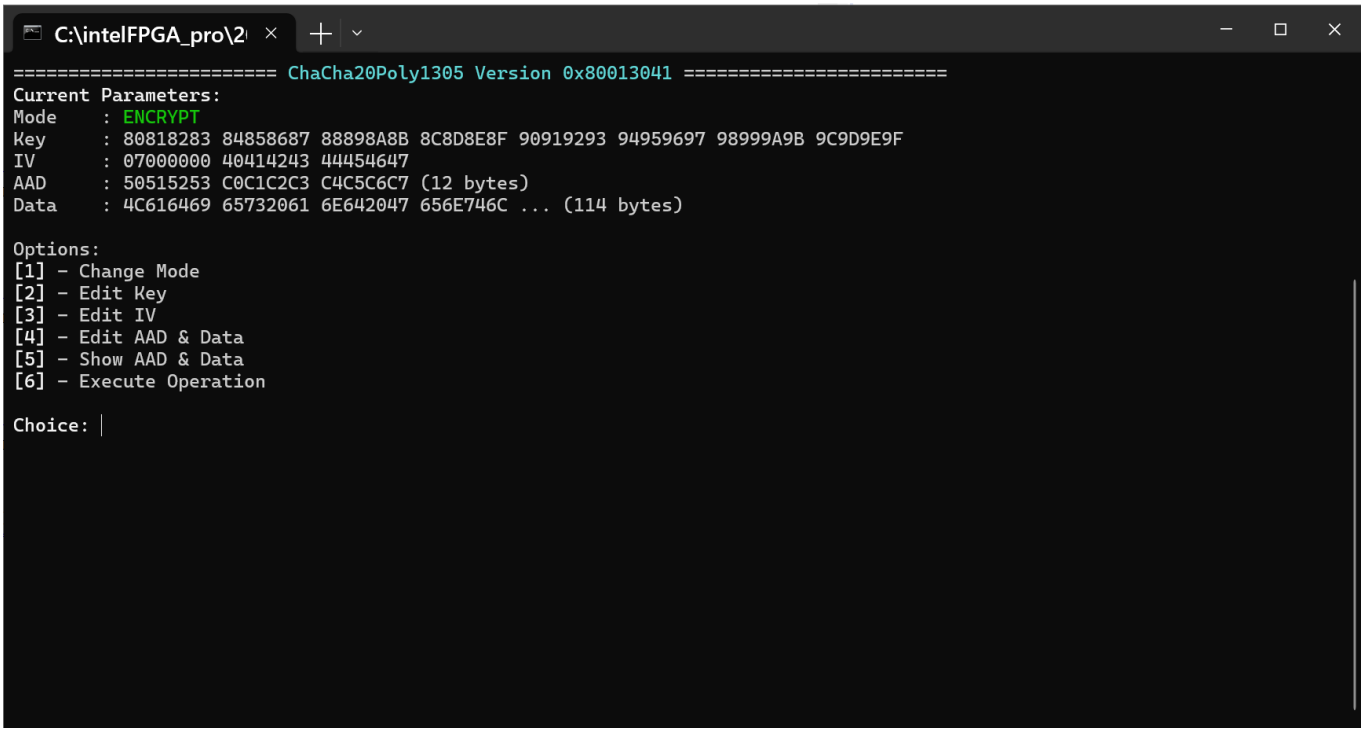

Figure 4 Main menu on Nios II Command Shell

4 Command Details and Test Results

4.1 Change Mode

Select “Change Mode” from the main menu to switch the ChaCha20Poly1305-IP operation mode. The available options are shown in Figure 5.

1) ENCRYPT: Encrypts Input Data stored in memory.
2) DECRYPT: Decrypts Input Data stored in memory.
3) BYPASS: Bypasses Input Data stored in memory without encryption or decryption.
4) SPEED TEST: Evaluates the computational efficiency of the ChaCha20Poly1305-IP when processing large volumes of data.

```
======================== ChaCha20Poly1305 Version 0x80013041 ========================
Current Parameters:
Mode    : ENCRYPT
Key     : 80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
IV      : 07000000 40414243 44454647
AAD     : 50515253 C0C1C2C3 C4C5C6C7 (12 bytes)
Data    : 4C616469 65732061 6E642047 656E746C ... (114 bytes)

Options:
[1] - Change Mode
[2] - Edit Key
[3] - Edit IV
[4] - Edit AAD & Data
[5] - Show AAD & Data
[6] - Execute Operation

Choice: 1

Select mode:
[1] - ENCRYPT
[2] - DECRYPT
[3] - BYPASS
[4] - SPEEDTEST
[0] - Back

Choice:
```

Figure 5 Change mode menu

4.2 Edit Key

The steps to edit key are as follows

1) Select “Edit Key”.
2) Enter up to 256-bit key value in hexadecimal format as shown in Figure 6.
3) After pressing Enter, the new key value will be updated and displayed in the main menu.

```
======================== ChaCha20Poly1305 Version 0x80013041 ========================
Current Parameters:
Mode    : ENCRYPT
Key     : 80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
IV      : 07000000 40414243 44454647
AAD     : 50515253 C0C1C2C3 C4C5C6C7 (12 bytes)
Data    : 4C616469 65732061 6E642047 656E746C ... (114 bytes)

Options:
[1] - Change Mode
[2] - Edit Key
[3] - Edit IV
[4] - Edit AAD & Data
[5] - Show AAD & Data
[6] - Execute Operation

Choice: 2

Enter new Key (enter to set, 'q' to exit): 0x1234567890abcdef
```

Figure 6 Key setting example

4.3 Edit IV

The steps to edit IV are as follows

1) Select “Edit IV”.
2) Enter up to 96-bit IV value in hexadecimal format as shown in Figure 7.
3) After pressing Enter, the new IV value will be updated and displayed in the main menu.

```
======================== ChaCha20Poly1305 Version 0x80013041 ========================
Current Parameters:
Mode    : ENCRYPT
Key     : 12345678 90ABCDEF 00000000 00000000 00000000 00000000 00000000 00000000
IV      : 00000000 00000000 00000000
AAD     : 50515253 C0C1C2C3 C4C5C6C7 (12 bytes)
Data    : 4C616469 65732061 6E642047 656E746C ... (114 bytes)

Options:
[1] - Change Mode
[2] - Edit Key
[3] - Edit IV
[4] - Edit AAD & Data
[5] - Show AAD & Data
[6] - Execute Operation

Choice: 3

Enter new IV (enter to set, 'q' to exit): 0xababcdcdefef1234
```

Figure 7 IV setting example

4.4 Edit AAD & Data

Select “Edit AAD & Data” to update AAD and Data in memory. Users must update both AAD and Data in this menu. Editing differs by mode:

Speed Test Mode:

1) Enter AAD size (bytes) and press Enter.
2) Enter Data size (bytes) as shown in Figure 8 and press Enter.
3) After both inputs, the new sizes are updated and shown in the main menu.

Other Modes:

1) Enter AAD value in hexadecimal and press Enter.
2) Enter Data value in hexadecimal as shown in Figure 9 and press Enter.
3) After both inputs, the new values and sizes are updated and shown in the main menu.

Notes:

- Combined AAD + Data size cannot exceed 16 KB.
- In Decrypt mode, Data is treated as Ciphertext; in Encrypt mode, it is Plaintext.
- In Speed Test Mode, the entered AAD size and Data size can be any value; the IP rounds each size up to the nearest 16-byte alignment.

```
======================== ChaCha20Poly1305 Version 0x80013041 ========================
Current Parameters:
Mode     : SPEEDTEST
Key      : 12345678 90000000 00000000 00000000 00000000 00000000 00000000 00000000
IV       : ABCDEF12 34560000 00000000
AAD      : (Forced 0) (0 bytes)
Data     : (Forced 0) (16 bytes)

Options:
[1] - Change Mode
[2] - Edit Key
[3] - Edit IV
[4] - Edit AAD & Data
[5] - Show AAD & Data
[6] - Execute Operation

Choice: 4

Enter AAD size in bytes (aligned to 16B, 'q' to skip): 9999999999
AAD size aligned and updated to 10000000000 bytes.

Enter Data size in bytes (aligned to 16B, 'q' to skip): 9999999999
```

Figure 8 AAD & Data setting example in Speed Test mode


```
======================== ChaCha20Poly1305 Version 0x80013041 ========================
Current Parameters:
Mode    : ENCRYPT
Key     : 12345678 90ABCDEF 00000000 00000000 00000000 00000000 00000000 00000000
IV      : ABABCDCD EFEF1234 00000000
AAD     : 50515253 C0C1C2C3 C4C5C6C7 (12 bytes)
Data    : 4C616469 65732061 6E642047 656E746C ... (114 bytes)

Options:
[1] - Change Mode
[2] - Edit Key
[3] - Edit IV
[4] - Edit AAD & Data
[5] - Show AAD & Data
[6] - Execute Operation

Choice: 4

Enter new AAD Value (enter to set, 'q' to exit): 0xababcdcdefef123456
AAD updated successfully (9 bytes).

Enter new Data (enter to set, 'q' to exit): 0xababcdcdefefab135790
```

Figure 9 AAD & Data setting example in other modes

4.5 Show AAD & Data

The steps to show AAD & Data in memory are as follows:

1) Select “Show AAD & Data”
2) Enter the number of bytes to display (or press Enter to display all).
3) The AAD and Data values are shown in table form as shown in Figure 10.
4) After pressing Enter, the console will return to the main menu.

```
======================== ChaCha20Poly1305 Version 0x80013041 ========================
Current Parameters:
Mode     : ENCRYPT
Key      : 80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
IV       : 07000000 40414243 44454647
AAD      : 50515253 C0C1C2C3 C4C5C6C7 (12 bytes)
Data     : 4C616469 65732061 6E642047 656E746C ... (114 bytes)

Options:
[1] - Change Mode
[2] - Edit Key
[3] - Edit IV
[4] - Edit AAD & Data
[5] - Show AAD & Data
[6] - Execute Operation

Choice: 5

Enter number of AAD & Data want to show in bytes (enter = all, 'q' to exit):

          Input Data
          0 1 2 3  4 5 6 7  8 9 A B  C D E F
00000000: 50515253 C0C1C2C3 C4C5C6C7 00000000
00000010: 4C616469 65732061 6E642047 656E746C
00000020: 656D656E 206F6620 74686520 636C6173
00000030: 73206F66 20273939 3A204966 20492063
00000040: 6F756C64 206F6666 65722079 6F75206F
00000050: 6E6C7920 6F6E6520 74697020 666F7220
00000060: 74686520 66757475 72652C20 73756E73
00000070: 63726565 6E20776F 756C6420 62652069
00000080: 742E
================================================================================
Press any key to continue...
```

Figure 10 Show AAD & Data example

4.6 Execute Operation

Select “Execute Operation” to start the operation in the currently selected mode.

4.6.1 Encrypt

In Encrypt mode, the IP uses the current key and IV to encrypt the Input Data in memory. The Output Data (Ciphertext) and 128-bit authentication tag are displayed as shown in Figure 11.

```
======================== ChaCha20Poly1305 Version 0x80013041 ========================
Current Parameters:
Mode    : ENCRYPT
Key     : 80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
IV      : 07000000 40414243 44454647
AAD     : 50515253 C0C1C2C3 C4C5C6C7 (12 bytes)
Data    : 4C616469 65732061 6E642047 656E746C ... (114 bytes)

Options:
[1] - Change Mode
[2] - Edit Key
[3] - Edit IV
[4] - Edit AAD & Data
[5] - Show AAD & Data
[6] - Execute Operation

Choice: 6
Operation started...
Operation Complete!

          Input Data                          Output Data
          0 1 2 3  4 5 6 7  8 9 A B  C D E F    0 1 2 3  4 5 6 7  8 9 A B  C D E F
00000000: 50515253 C0C1C2C3 C4C5C6C7 00000000   50515253 C0C1C2C3 C4C5C6C7 00000000
00000010: 4C616469 65732061 6E642047 656E746C   D31A8D34 648E60DB 7B86AFBC 53EF7EC2
00000020: 656D656E 206F6620 74686520 636C6173   A4ADED51 296E08FE A9E2B5A7 36EE62D6
00000030: 73206F66 20273939 3A204966 20492063   3DBEA45E 8CA96712 82FAFB69 DA92728B
00000040: 6F756C64 206F6666 65722079 6F75206F   1A71DE0A 9E060B29 05D6A5B6 7ECD3B36
00000050: 6E6C7920 6F6E6520 74697020 666F7220   92DDBD7F 2D778B8C 9803AEE3 28091B58
00000060: 74686520 66757475 72652C20 73756E73   FAB324E4 FAD67594 5585808B 4831D7BC
00000070: 63726565 6E20776F 756C6420 62652069   3FF4DEF0 8E4B7A9D E576D265 86CEC64B
00000080: 742E                                  6116

Generated Tag: 1AE10B59 4F09E26A 7E902ECB D0600691

Took 4us (134 Mbps)
================================================================================
Press any key to continue...
```

Figure 11 Encryption mode result

4.6.2 Decrypt

In Decrypt mode, the IP uses the current key and IV to decrypt the Input Data in memory. The Output Data (recovered Plaintext) and the 128-bit authentication tag are displayed as shown in Figure 12.

```
======================== ChaCha20Poly1305 Version 0x80013041 ========================
Current Parameters:
Mode    : DECRYPT
Key     : 80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
IV      : 07000000 40414243 44454647
AAD     : 50515253 C0C1C2C3 C4C5C6C7 (12 bytes)
Data    : 4C616469 65732061 6E642047 656E746C ... (114 bytes)

Options:
[1] - Change Mode
[2] - Edit Key
[3] - Edit IV
[4] - Edit AAD & Data
[5] - Show AAD & Data
[6] - Execute Operation

Choice: 6
Operation started...
Operation Complete!

          Input Data                                Output Data
          0 1 2 3  4 5 6 7  8 9 A B  C D E F       0 1 2 3  4 5 6 7  8 9 A B  C D E F
00000000: 50515253 C0C1C2C3 C4C5C6C7 00000000      50515253 C0C1C2C3 C4C5C6C7 00000000
00000010: 4C616469 65732061 6E642047 656E746C      D31A8D34 648E60DB 7B86AFBC 53EF7EC2
00000020: 656D656E 206F6620 74686520 636C6173      A4ADED51 296E08FE A9E2B5A7 36EE62D6
00000030: 73206F66 20273939 3A204966 20492063      3DBEA45E 8CA96712 82FAFB69 DA92728B
00000040: 6F756C64 206F6666 65722079 6F75206F      1A71DE0A 9E060B29 05D6A5B6 7ECD3B36
00000050: 6E6C7920 6F6E6520 74697020 666F7220      92DDBD7F 2D778B8C 9803AEE3 28091B58
00000060: 74686520 66757475 72652C20 73756E73      FAB324E4 FAD67594 5585808B 4831D7BC
00000070: 63726565 6E20776F 756C6420 62652069      3FF4DEF0 8E4B7A9D E576D265 86CEC64B
00000080: 742E                                     6116

Generated Tag: 661E9434 67EDB196 3BFE9015 190609F0

Took 4us (134 Mbps)
================================================================================
Press any key to continue...
```

Figure 12 Decryption mode result

4.6.3 Bypass

In Bypass mode, the IP simply passes the Input Data from memory to output memory without any encryption or decryption. Both Input Data and Output Data are displayed as shown in Figure 13.

```
======================== ChaCha20Poly1305 Version 0x80013041 ========================
Current Parameters:
Mode    : BYPASS
Key     : 80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
IV      : 07000000 40414243 44454647
AAD     : 50515253 C0C1C2C3 C4C5C6C7 (12 bytes)
Data    : 4C616469 65732061 6E642047 656E746C ... (114 bytes)

Options:
[1] - Change Mode
[2] - Edit Key
[3] - Edit IV
[4] - Edit AAD & Data
[5] - Show AAD & Data
[6] - Execute Operation

Choice: 6
Operation started...
Operation Complete!

          Input Data                          Output Data
          0 1 2 3  4 5 6 7  8 9 A B  C D E F    0 1 2 3  4 5 6 7  8 9 A B  C D E F
00000000: 50515253 C0C1C2C3 C4C5C6C7 00000000   50515253 C0C1C2C3 C4C5C6C7 00000000
00000010: 4C616469 65732061 6E642047 656E746C   4C616469 65732061 6E642047 656E746C
00000020: 656D656E 206F6620 74686520 636C6173   656D656E 206F6620 74686520 636C6173
00000030: 73206F66 20273939 3A204966 20492063   73206F66 20273939 3A204966 20492063
00000040: 6F756C64 206F6666 65722079 6F75206F   6F756C64 206F6666 65722079 6F75206F
00000050: 6E6C7920 6F6E6520 74697020 666F7220   6E6C7920 6F6E6520 74697020 666F7220
00000060: 74686520 66757475 72652C20 73756E73   74686520 66757475 72652C20 73756E73
00000070: 63726565 6E20776F 756C6420 62652069   63726565 6E20776F 756C6420 62652069
00000080: 742E                                  742E


Took 4us (134 Mbps)
================================================================================
Press any key to continue...
```

Figure 13 Bypass mode result

4.6.4 Speed Test

In Speed Test mode, the IP ignores the actual AAD and Data values. Only the entered sizes, together with the current key and IV, are used to run the encryption process. The console shows the execution time and calculated throughput, as shown in Figure 14.

```
======================== ChaCha20Poly1305 Version 0x80013041 ========================
Current Parameters:
Mode    : SPEEDTEST
Key     : 80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
IV      : 07000000 40414243 44454647
AAD     : (Forced 0) (1000000 bytes)
Data    : (Forced 0) (100000000 bytes)

Options:
[1] - Change Mode
[2] - Edit Key
[3] - Edit IV
[4] - Edit AAD & Data
[5] - Show AAD & Data
[6] - Execute Operation

Choice: 6
Operation started...
Operation Complete!

Generated Tag: 7459D7DA CD8070DE C94110BD A9390630

Took 11433us (11433 Mbps)
================================================================================
Press any key to continue...
```

Figure 14 Speed Test mode result

5 Revision History

Revision	Date (D-M-Y)	Description
1.00	31-Jul-26	Initial version release

