Advanced Encryption Standard Hardware Accelerator

System-on-Chip Project

Bajdu Ștefania, Sonosy Omar

Université Grenoble Alpes
Institut Nationale Polytechnique
Ecole Supérieure en Systèmes Avancés et Réseaux

11th December 2024

Agenda

1. Project Ideea
2. Integrating Open Source AES Core
3. Developing our AES Core
4. FPGA Implementation
5. Software Implementation
6. Results and Comparison

Agenda

Project Ideea

- AES-128 Standard in ECB mode;
- Interrupts from PL to PS;
- Introducing PKCS5 padding;
- UART Communication;
- Encrypt / Decrypt up to 1024 bytes (configurable).

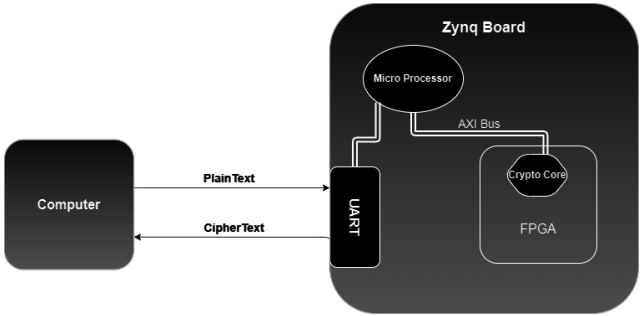


Figure 1: System Architecture

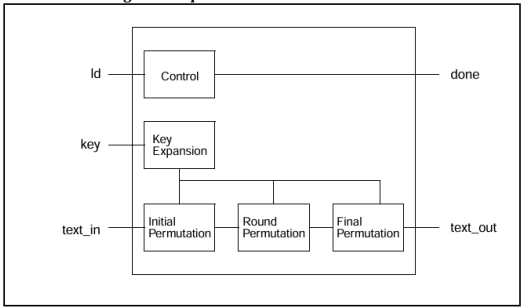
Agenda

Verilog AES Core

- Integrated an open source Verilog Core;
- Build and configure an IP;
- Interrupts the PS when encryption ends;
- Implement the C code for testing.

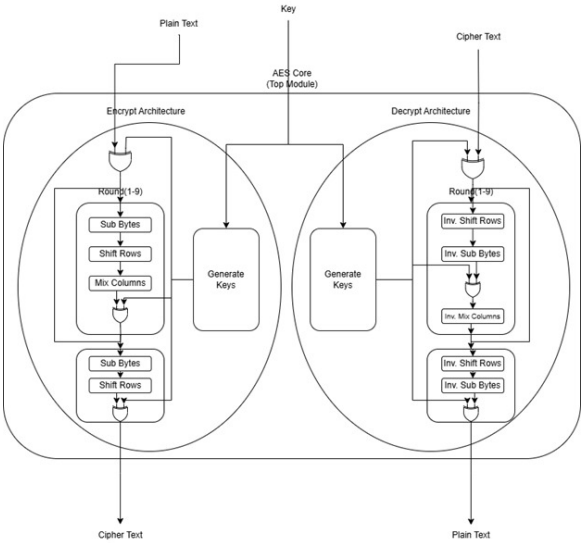
```
Start encryption.

Plaintext: 74 68 69 73 69 73 6D 79 70 6C 61 69 6E 74 78 78
Key: 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70
Ciphertext: 5 D0 E3 F0 CC A0 E3 BB 83 CB 6A 1C DB 8A 5B 7A
```

Figure 1: Cipher Core Architecture Overview



Agenda

Developing the Core



Validating our core in VHDL

- Encryption / Decryption : 11 clock cycles;
- Randomly generated 30.000 tests;
- Designed testbench and validated in Questasim.

```
# EXECUTION:: NOTE   : ---------- Test 1 Passed ----------
# EXECUTION:: Time: 330 ns,  Iteration: 0,  Instance: /testbench,  Process: test_process.
# EXECUTION:: NOTE   : ---------- Test 2 Passed ----------
# EXECUTION:: Time: 1030 ns,  Iteration: 0,  Instance: /testbench,  Process: test_process.
# EXECUTION:: NOTE   : ---------- Test 3 Passed ----------
# EXECUTION:: Time: 1330 ns,  Iteration: 0,  Instance: /testbench,  Process: test_process.
# EXECUTION:: NOTE   : ---------- Test 4 Passed ----------
# EXECUTION:: Time: 1630 ns,  Iteration: 0,  Instance: /testbench,  Process: test_process.
# EXECUTION:: NOTE   : ---------- Test 5 Passed ----------
# EXECUTION:: Time: 1930 ns,  Iteration: 0,  Instance: /testbench,  Process: test_process.
# EXECUTION:: NOTE   : ---------- Test 6 Passed ----------
# EXECUTION:: Time: 2230 ns,  Iteration: 0,  Instance: /testbench,  Process: test_process.
# EXECUTION:: NOTE   : ---------- Test 7 Passed ----------
# EXECUTION:: Time: 2530 ns,  Iteration: 0,  Instance: /testbench,  Process: test_process.
# EXECUTION:: NOTE   : ---------- Test 8 Passed ----------
# EXECUTION:: Time: 2830 ns,  Iteration: 0,  Instance: /testbench,  Process: test_process.
# EXECUTION:: NOTE   : ---------- Test 9 Passed ----------
# EXECUTION:: Time: 3130 ns,  Iteration: 0,  Instance: /testbench,  Process: test_process.
# EXECUTION:: NOTE   : ---------- Test 10 Passed ----------
# EXECUTION:: Time: 3430 ns,  Iteration: 0,  Instance: /testbench,  Process: test_process.
# EXECUTION:: NOTE   : ---------- Test 11 Passed ----------
```

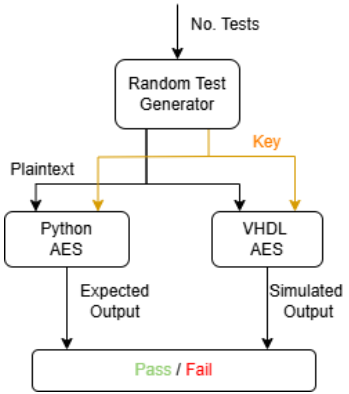


Figure 2: Test Architecture

Waveform

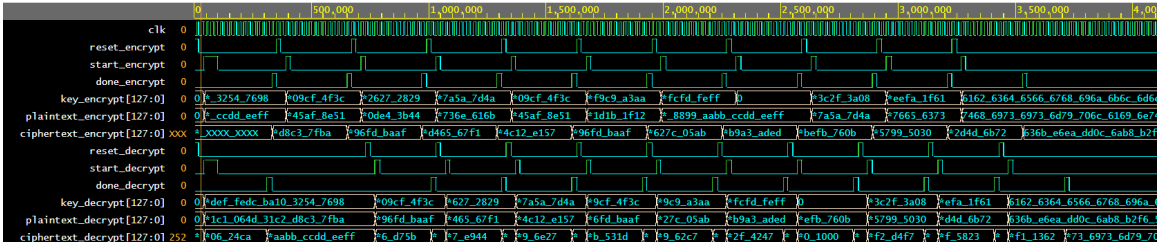
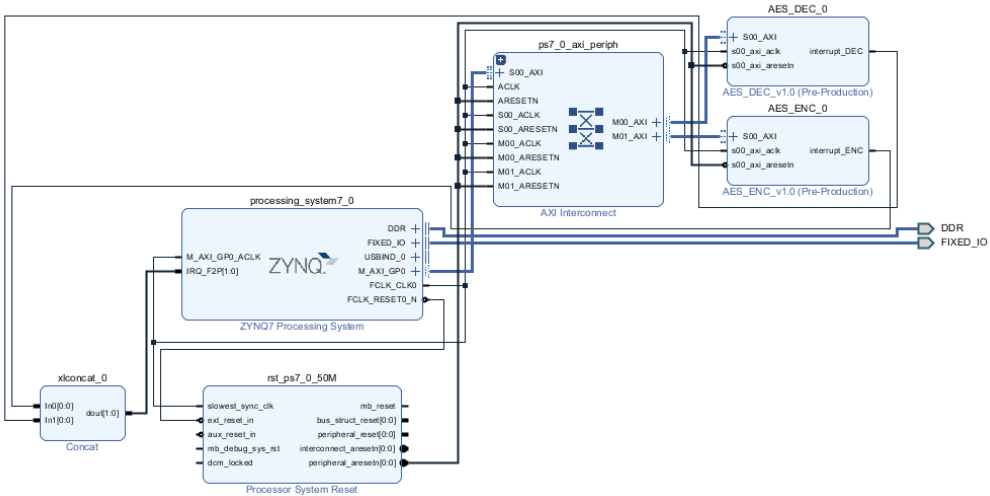


Figure 3: Test Waveform

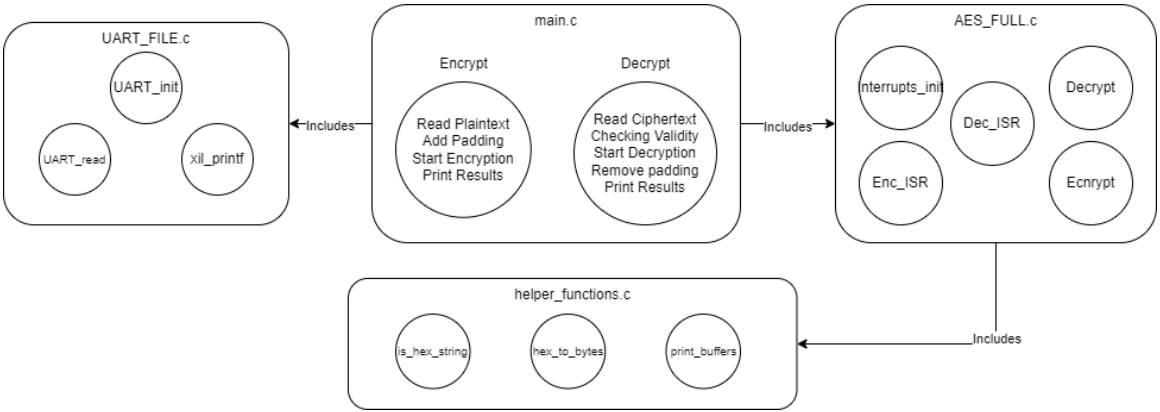
Agenda

Vivado Design



Agenda

Software Drivers



Agenda

Comparison

Code	Encryption	Decryption
C	51543087	51543437
VHDL	7.44	6.43

Table 1: Speed Comparison [ns]

```
Start encryption.
Plaintext: 74 68 69 73 69 73 6D 79 70 6C 61 69 6E 74 78 78
Key: 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70
Ciphertext: 5 D0 E3 F0 CC A0 E3 BB 83 CB 6A 1C DB 8A 5B 7A
Encryption in C takes 51543087.515936 ns.

Start decryption.
Plaintext: 5 D0 E3 F0 CC A0 E3 BB 83 CB 6A 1C DB 8A 5B 7A
Key: 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70
Ciphertext: 74 68 69 73 69 73 6D 79 70 6C 61 69 6E 74 78 78
Decryption in C takes 51543437.507925 ns.
```

Figure 4: C implementation

VHDL Execution Times

```
Initialize program.

Start encryption.

Plaintext: 74 68 69 73 69 73 6D 79 70 6C 61 69 6E 74 78 78
Key: 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70
Ciphertext: 5 D0 E3 F0 CC A0 E3 BB 83 CB 6A 1C DB 8A 5B 7A

Encryption takes 7.440000 ns.

Start decryption.

Plaintext: 5 D0 E3 F0 CC A0 E3 BB 83 CB 6A 1C DB 8A 5B 7A
Key: 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70
Ciphertext: 74 68 69 73 69 73 6D 79 70 6C 61 69 6E 74 78 78

Decryption takes 6.432000 ns.
```

Figure 5: VHDL results

Thank you for your attention!