**AES** **Add-on processor for RISC-V**

Project Report

Students:

|  |  |
| --- | --- |
| David Dan | 301914834 |
| Dolev Vaknin | 204280481 |

Supervisor:

Eric Herbelin

Table of Contents

[**List of figures** 4](#_Toc57387051)

[**List of tables** 6](#_Toc57387052)

[**Abstract** 7](#_Toc57387053)

[**List of abbreviations** 8](#_Toc57387054)

[**Introduction** 9](#_Toc57387055)

[RISC-V 9](#_Toc57387056)

[Rationale 9](#_Toc57387057)

[Specifications 9](#_Toc57387058)

[RI5CY 10](#_Toc57387059)

[PULP 11](#_Toc57387060)

[PULPino 11](#_Toc57387061)

[PULPenix 12](#_Toc57387062)

[AES 13](#_Toc57387063)

[AES ciphering process 13](#_Toc57387064)

[KeyExpansionUnit 15](#_Toc57387065)

[SubBytes 15](#_Toc57387066)

[ShiftRows 15](#_Toc57387067)

[MixColumns 15](#_Toc57387068)

[AddRoundKey 15](#_Toc57387069)

[**Possible solutions** 17](#_Toc57387070)

[Encryption from buffer 17](#_Toc57387071)

[Encryption command 17](#_Toc57387072)

[Encryption on the fly 18](#_Toc57387073)

[**Interface architecture** 19](#_Toc57387074)

[AES commands opcode 19](#_Toc57387075)

[AES Commands structure 20](#_Toc57387076)

[AES REG 20](#_Toc57387077)

[AES KEY 20](#_Toc57387078)

[AES MEM 20](#_Toc57387079)

[AES\_RUN 21](#_Toc57387080)

[**Design and Implementation** 22](#_Toc57387081)

[Flow 22](#_Toc57387082)

[AES register file 23](#_Toc57387083)

[Simulate the AES register file 23](#_Toc57387084)

[AES engine 24](#_Toc57387085)

[Simulate the AES engine 24](#_Toc57387086)

[AES write-back 26](#_Toc57387087)

[Simulate AES engine with register file and write-back module 27](#_Toc57387088)

[Integrate the AES flow with RISC-V core 28](#_Toc57387089)

[**Simulate and Debug** 29](#_Toc57387090)

[Syntax errors 29](#_Toc57387091)

[Connections problems 29](#_Toc57387092)

[Flow issues 30](#_Toc57387093)

[**Conformity check** 31](#_Toc57387094)

[**Performance** 33](#_Toc57387095)

[CoreMark 33](#_Toc57387096)

[Power 34](#_Toc57387097)

[Area 35](#_Toc57387098)

[Timing 36](#_Toc57387099)

[**Compiler** 37](#_Toc57387100)

[AES commands compilation options 37](#_Toc57387101)

[AES compiler 37](#_Toc57387102)

[**Methodology** 40](#_Toc57387103)

[**Summary** 41](#_Toc57387104)

[**Appendix A: Design changes** 42](#_Toc57387105)

[**Appendix B: User guide** 43](#_Toc57387106)

[Synthesis 44](#_Toc57387107)

[Simulation 46](#_Toc57387108)

[AES verification test 47](#_Toc57387109)

[Simvision 48](#_Toc57387110)

[Trace file 50](#_Toc57387111)

[**Bibliography** 51](#_Toc57387112)

**List of figures**

[Figure 1 - RI5CY CORE 10](#_Toc57387008)

[Figure 2 - PULPino Top Level 11](#_Toc57387009)

[Figure 3 - PULPenix Top Level 12](#_Toc57387010)

[Figure 4 - AES Algorithm diagram 14](#_Toc57387011)

[Figure 5 - AES SubBytes step 15](#_Toc57387012)

[Figure 6 - AES ShiftRows step 15](#_Toc57387013)

[Figure 7 - AES MixColumns step 15](#_Toc57387014)

[Figure 8 - AES AddRoundKey step 16](#_Toc57387015)

[Figure 9 - RI5CY CORE with AES flow 22](#_Toc57387016)

[Figure 10 - AES register file module diagram 23](#_Toc57387017)

[Figure 11 - AES register file simulation example 23](#_Toc57387018)

[Figure 12 - AES engine module diagram 24](#_Toc57387019)

[Figure 13 - AES engine simulation example 25](#_Toc57387020)

[Figure 14 - AES write back module diagram 26](#_Toc57387021)

[Figure 15 - AES write back simulation example 27](#_Toc57387022)

[Figure 16 - AES write back - wen bug 29](#_Toc57387023)

[Figure 17 - AES write back - wen fix 29](#_Toc57387024)

[Figure 18 – AES register file – data register override 30](#_Toc57387025)

[Figure 19 - AES register file – data register override fix 30](#_Toc57387026)

[Figure 31 - AES verification - success 32](#_Toc57387027)

[Figure 32 - AES verification - failure 32](#_Toc57387028)

[Figure 20 – GenPro PULPenix CoreMark 33](#_Toc57387029)

[Figure 21 - GenPro PULPenix AES CoreMark 33](#_Toc57387030)

[Figure 22 - GenPro PULPenix power report 34](#_Toc57387031)

[Figure 23 - GenPro PULPenix AES power report 34](#_Toc57387032)

[Figure 24 - GenPro PULPenix area report 35](#_Toc57387033)

[Figure 25 - GenPro PULPenix AES area report 35](#_Toc57387034)

[Figure 28 - GenPro PULPenix timing report 36](#_Toc57387035)

[Figure 29 - GenPro PULPenix AES timing report 36](#_Toc57387036)

[Figure 30 - specify clock window 45](#_Toc57387037)

[Figure 33 - open database window 48](#_Toc57387038)

[Figure 34 - signals select window 48](#_Toc57387039)

[Figure 35 - trace file example 50](#_Toc57387040)

**List of tables**

[Table 1 - R type commands structure 19](#_Toc57387041)

[Table 2 - RISCV base opcode map 19](#_Toc57387042)

[Table 3 - AES commands structure and opcode 19](#_Toc57387043)

[Table 4 - AES REG command structure 20](#_Toc57387044)

[Table 5 - AES KEY command structure 20](#_Toc57387045)

[Table 6 - AES MEM command structure 20](#_Toc57387046)

[Table 7 - AES RUN command structure 21](#_Toc57387047)

# **Abstract**

In our days, where we use sensors and processors anywhere and anytime, it’s getting very hard to keep the data we receive from those devices – safe.

There are a lot of ways to get data from devices that don’t belong to us, and that’s because, in most of the cases, the raw data sent from the sensors to a relatively far processor, and only after processing the information, the processor encrypts the processed data. Which means, there are a lot of chances to steal the information between collecting the raw data by the sensor, and encryption of that data by the processor.

The goal of this project is to design and implement an AES encryption (or any other safe encryption method) on the RISC-V processor, which will enable using the RISC-V for processing the information from as close to the sensor as can be and doing so safely.

In this project, we are using the RI5CY core embedded in the Pulpenix microcontroller.

# **List of abbreviations**

CPU – Central Processing Unit

ISA – Instruction Set Architecture

RISC – Reduced Instruction Set Computer

AES – Advanced Encryption Standard

SOC – System On Chip

PULP – Parallel Ultra-Low Power

RAM – Random Access Memory

AXI – Advanced eXtensible Interface

APB – Advanced Peripheral Bus

SPI - Serial Peripheral Interface

LSU – Load Store Unit

IF – Instruction Fetch

ID – Instruction Decode

EX – Execute

WB – Write Back

NIST – National Institute of Standards and Technology

RTL – Register Transfer Level

IoT – Internet of Things

SV – System Verilog

GNU – GNU’s Not Unix

GCC – GNU Compiler Collection

GUI – Graphical User Interface

DDC – Description and Design Constraints

**Introduction**

RISC-V

The RISC-V project started in 2010 at Berkeley USA.

Since 2015 RISC-V under the supervision of the non-profit RISC-V Foundation, with over 200 member organizations, from both academia and industry, including Samsung, Google, NVIDIA, Qualcomm, Berkeley Architecture Research, ETH Zurich, and many more.

Rationale

Most of the semiconductor companies (such as MIPS, ARM, etc.) charge royalties for the use of their designs and patents, due to the high cost of designing a CPU.

RISC-V was designed as an open-source ISA, that anybody can change and use for his personal or commercial uses, without paying royalties.

The original goals of RISC-V were [[[1]](#footnote-1)][[[2]](#footnote-2)]:

* ISA that supports a wide variety of practical uses
* Usable academically.
* Usable in any hardware or software design.

Specifications

The RISC-V ISA is designed for a wide range of uses. It is variable-width and extensible so that more encoding bits can always be added. It supports three word-widths: 32, 64, and 128 bits, and a variety of subsets. The definitions of each subset vary slightly for the three word-widths [[[3]](#footnote-3)].

RISC-V has 32 (or 16 in the embedded version) [integer](https://en.wikipedia.org/wiki/Integer) registers, and 32 separate floating-point registers when the floating-point extension is implemented.

RISC-V is implemented in a [load-store architecture](https://en.wikipedia.org/wiki/Load%E2%80%93store_architecture), which means that instructions address only registers, with load/store instructions to read/write from/to the memory.

RI5CY

RI5CY is a 4-stage in-order 32-bit RISC-V processer[[4]](#footnote-4) , with some added instructions not in the standard RISC-V ISA. The top-level diagram of the core:

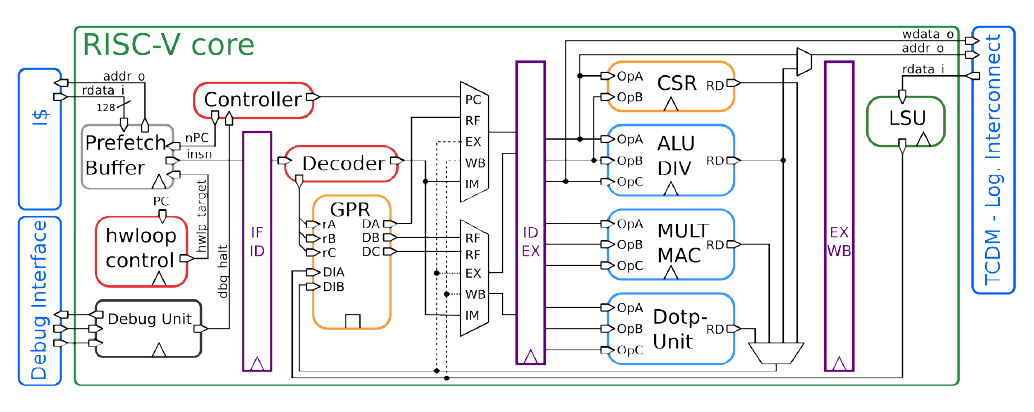


Figure 1 - RI5CY CORE

PULP

PULP is an open-source computing platform designed by ETH Zurich and the University of Bologna - started in 2013.

The processors embedded in the PULP range from single-core to multi-cluster (more than one processor).

The PULP architecture targets IoT applications requiring low-power, flexible processing of data streams generated by multiple sensors, such as accelerometers, low-resolution cameras, microphone arrays, vital signs monitors.

PULP consists of an advanced microcontroller architecture representing a significant step ahead in terms of completeness and complexity.

PULPino

PULPino is a single-core System-On-a-Chip (“SOC”) built for the RISC-V RI5CY and ZERO-RI5CY core. PULPino reuses most components from its bigger brother PULP. It uses separate single-port data and instruction RAMs. It includes a boot ROM that contains a boot loader that can load a program via SPI from an external flash device. The SOC uses an AXI as its main interconnect with a bridge to APB for simple peripherals. Both the AXI and the APB buses feature 32-bit wide data channels. For debugging purposes, the SOC includes an advanced debug unit that enables access to core registers, the two RAMs, and memory-mapped IO via JTAG. Both RAMs are connected to the AXI bus via bus adapters [[[5]](#footnote-5)].

PULPino top level:

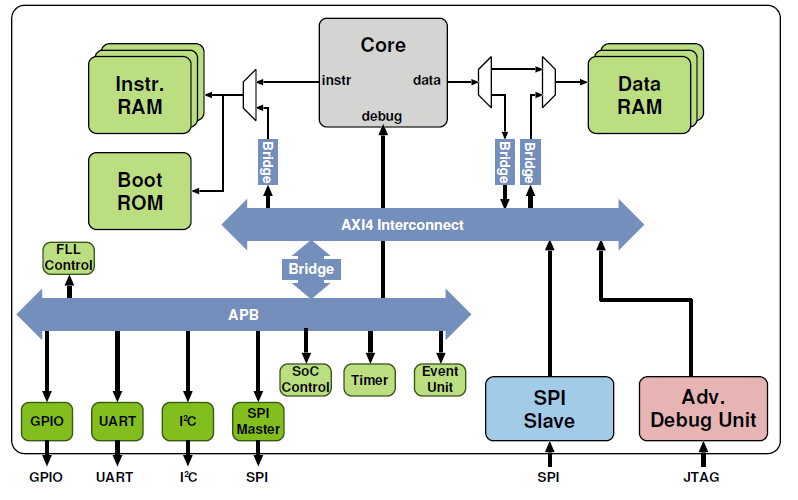


Figure 2 - PULPino Top Level

PULPenix

Developed in Bar-Ilan by Yehuda Kra, the PULPenix platform took the existing open-source implementation of the PULPino processor and added an interface and compiler system for the software, so bare-metal C programs could be compiled and run on the processor.

It also includes a set of scripts and tools to allow easy compilation and running of the program, debugging, making waveforms of the processor signals, and making a trace file of the assembly commands, including the simulation times and register values.

PULPenix top level:

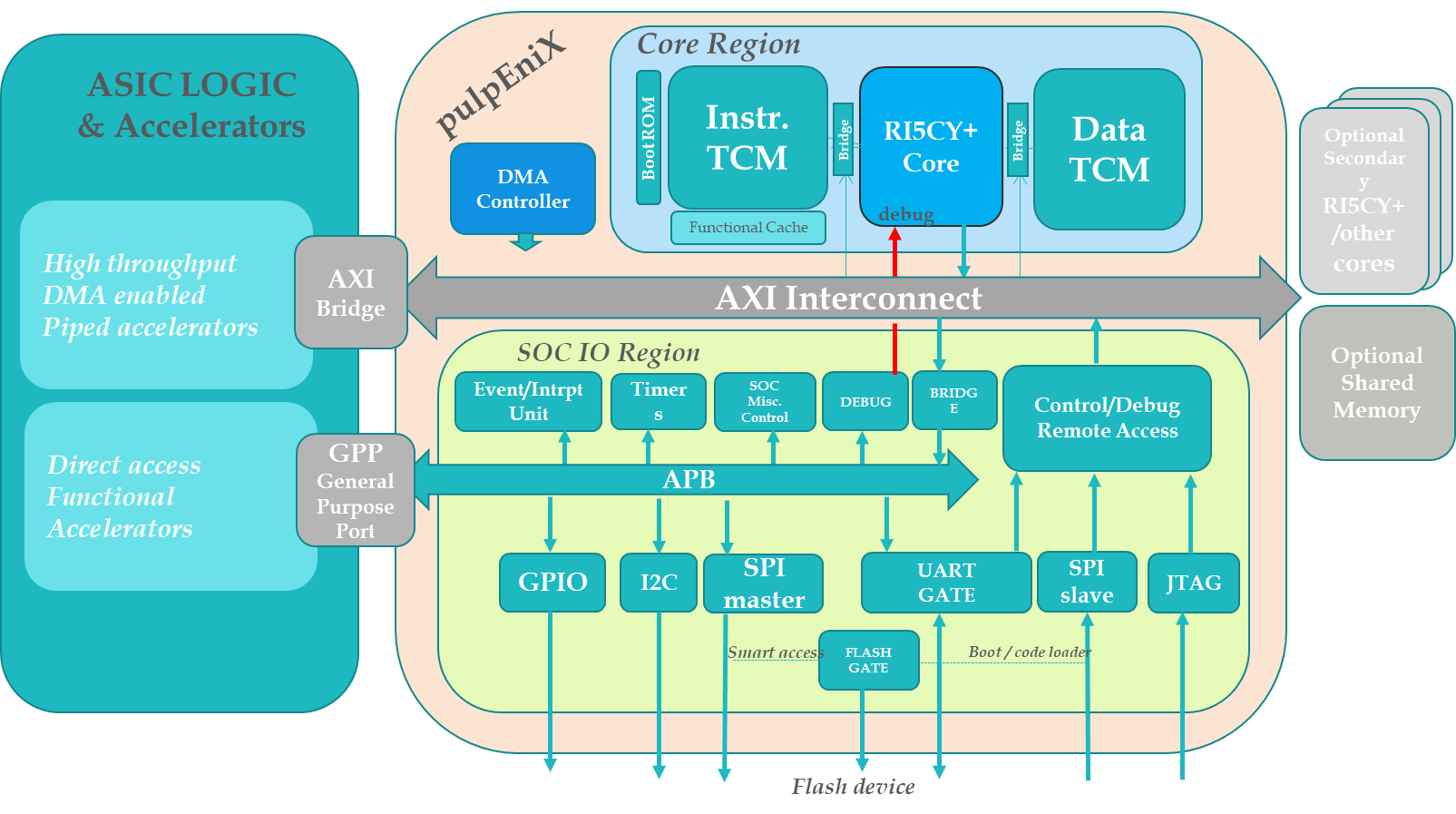


Figure 3 - PULPenix Top Level

AES

AES is a symmetric [block cipher](https://en.wikipedia.org/wiki/Block_cipher), adopted by the U.S. government and governments and organizations all around the world[[[6]](#footnote-6)].

The AES algorithm is a subset of the Rijndael block cipher, developed by [Vincent Rijmen](https://en.wikipedia.org/wiki/Vincent_Rijmen) and [Joan Daemen](https://en.wikipedia.org/wiki/Joan_Daemen), and chosen by NIST during the AES selection process in November 2001[[[7]](#footnote-7)].

Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192, and 256 bits[[[8]](#footnote-8)].

The AES algorithm is a [symmetric-key algorithm](https://en.wikipedia.org/wiki/Symmetric-key_algorithm), meaning the same key is used for both encryption and decryption of the data, which makes it easier to send and receive an encrypted text.

AES is a block cipher, meaning it encrypts blocks (128-bit blocks) of the text each time.

AES ciphering process

The AES consisting of 10, 12, or 14 rounds.

The first round is consisting of the steps: AddRoundKey, SubBytes, ShiftRows, MixColumns, AddRoundKey (in that order).

The next 8, 10, or 12 rounds consisting of the steps: SubBytes, ShiftRows, MixColumns, AddRoundKey.

The last round consisting the steps: SubBytes, ShiftRows, AddRoundKey.

AES diagram

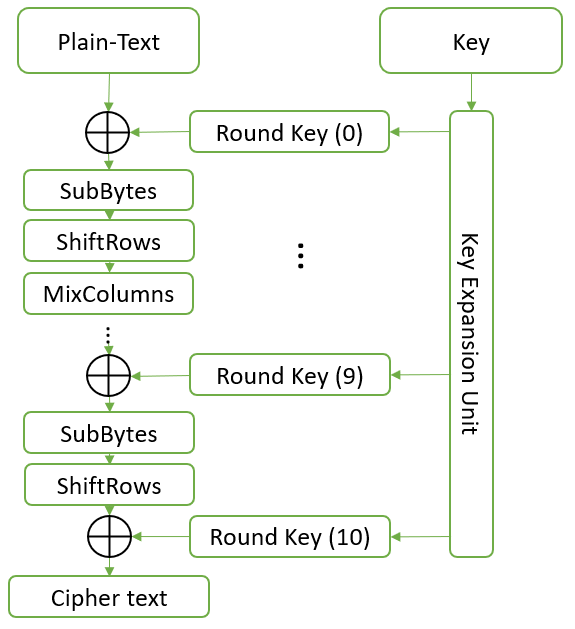


Figure 4 - AES Algorithm diagram

KeyExpansionUnit

round keys are derived from the cipher key using the [AES key schedule](https://en.wikipedia.org/wiki/AES_key_schedule). AES requires a separate 128-bit round key block for each round plus one more (before the first round, a total of 11 keys).

To supply 128\*11=1408bit of a key, the 128bit key is expanded using KeyExpansionUnit, which performs few manipulations on the original 128bit in order to expand it to 1408bit.

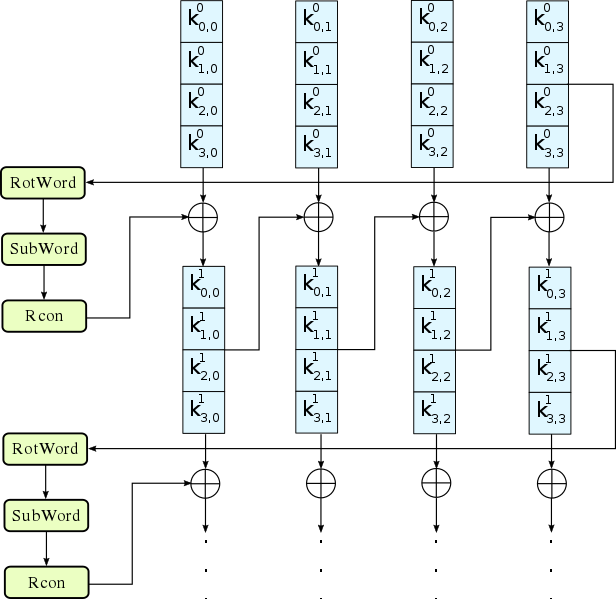


Figure - AES KeyExpansion unit

SubBytes

A non-linear substitution step where each byte is replaced with another according to a lookup table (AES S-box).

A picture containing crossword, clock, black, hanging

Description automatically generated

Figure 6 - AES SubBytes step

ShiftRows

A transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

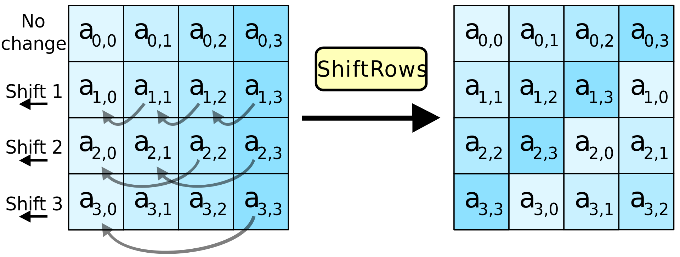


Figure 7 - AES ShiftRows step

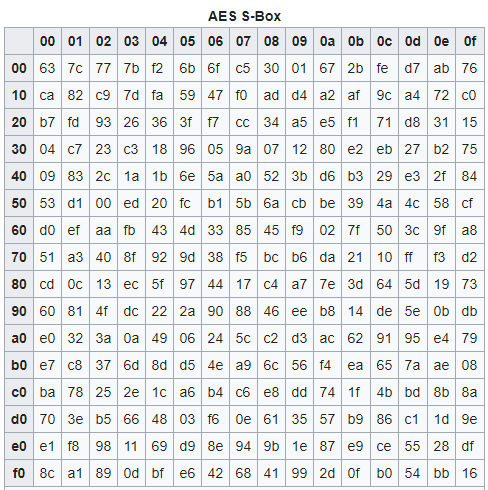


Figure - AES S-BOX

MixColumns

A linear mixing operation that operates on the columns of the state, combining the four bytes in each column.

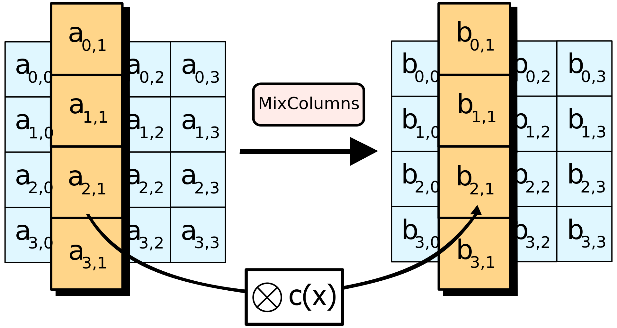


Figure 9 - AES MixColumns step

AddRoundKey

Each byte of the state is combined with a byte of the round key using [bitwise xor](https://en.wikipedia.org/wiki/Bitwise_xor).

A close up of a clock

Description automatically generated

Figure 10 - AES AddRoundKey step

# **Possible solutions**

There was 3 optional solution on the table:

1. Encryption from buffer

In this solution, the RISC-V core will hold 9 new AES registers, holding 4 data registers, 4 key registers, 1 write-back register. There will be special commands to write data to those registers, and running the AES command:

1. Storing 4 key registers in the AES register file.
2. Storing write-back register in the AES register file.
3. Storing 4 data registers in the AES register file.
4. Calling the AES command:

The command will cipher the AES data registers using the AES key registers, and store the ciphered 4 data registers to the memory (starting in the address given in step b.)

Advantages:

* + Relatively easy to implement.
  + Relatively secure – once the 4 registers hold the new data, the ciphering process can start.

Disadvantages:

* + Wasteful in terms of area - requires 9 new registers for the AES.
  + Need to encrypt 4 registers at every encryption process.

1. Encryption command

In this solution, the command will be the same as “Store”, but instead of writing the data directly to the memory, the data will be ciphered before:

* 1. Storing the key inside special 4 registers (hardware protected, nonvolatile).
  2. Calling the AES command (equivalent to “Store” command):

The command will load the 4 data registers from the memory (from the address given, but after alignment to 128-bit), decipher them, replace the correct (old) register with the new register, run the AES algorithm, and store the ciphered data back to the required address in the memory (read-modify-write).

Advantages:

* + Can store one register (instead of 4 at a time).

Disadvantages:

* + Not very secure – the data will wait in the core, un-ciphered, till finishing loading the 4 registers from the memory and deciphering them.
  + Hard to implement – there is a need for deciphering unit.
  + Wasteful in terms of time, power, and area - requires 4 loads from the memory and 4 stores to the memory.

1. Encryption on the fly

In this solution, we don’t use the AES algorithm, but using another cyphering method, that can cipher 32-bit block, so we could cipher data before writing it to the register, and storing ciphered data without loading data from the memory first (read-modify-write):

* 1. Storing key inside register (hardware protected, nonvolatile)
  2. Using encryption command, equivalent to “Store” command (or R type command):

The command will cipher the data and store it into the memory (or register).

Advantages:

* + Easy to implement.
  + The memory (including the registers) would hold only ciphered data.
  + Economical in terms of time and power (only one register is ciphered at any time, with a less complex ciphering algorithm.).

Disadvantages:

* + Not secure – due to the use of a less complex ciphering algorithm.

After discussing the advantages and disadvantages of the 3 solutions, we decided to implement solution number one, which is Encryption from a buffer.

# **Interface architecture**

To implement our solution to encryption command in RISC-V, we decided to use the following command structure (from R type commands):



Table 1 - R type commands structure

Where the opcode will be the same to all AES commands, while funct3 will distinguish between the AES commands, rd will be AES register (data or key), and rs1 will be RISCV register.

## AES commands opcode

The RISC-V opcode map:

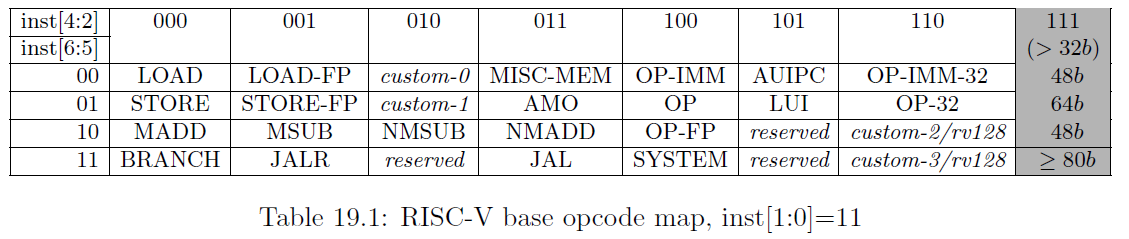


Table 2 - RISCV base opcode map , inst[1:0]=11

In the PULPenix RI5CY core, some of the opcodes in the table are not in use (not necessarily the “custom” opcodes).

We discovered that 0x3b opcode (OP-32 in the table) is not in use.

We decided to use 0x3b as AES commands opcode:

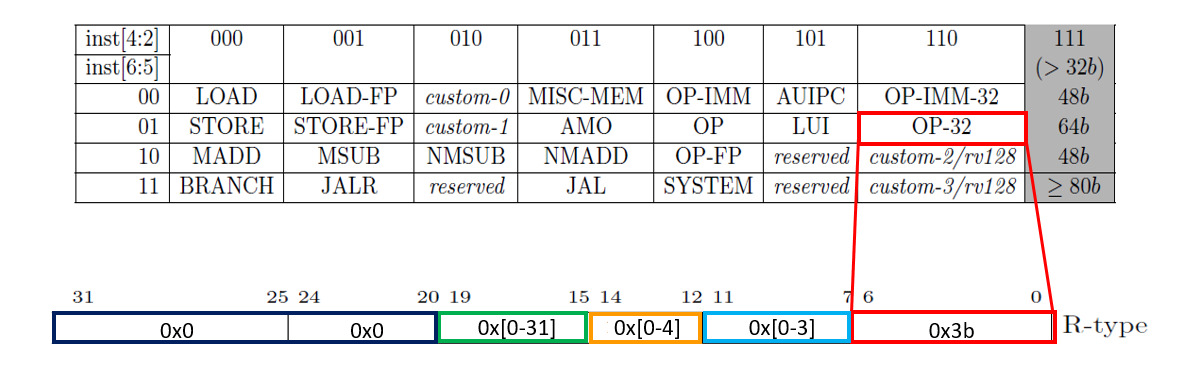


Table 3 - AES commands structure and opcode

Opcode

AES register (key or data)

AES function

RISCV register

Not in use

## AES Commands structure

To run the AES encryption command, first, the AES register file must hold the correct data, key, and write-back address.

Writing to the AES register file is done using the commands:

* AES REG

Writing data to AES data registers, it receives as parameters AES data register ( d[0:3] ) and RISC-V register.

Funct3 = 0

Command structure:



0x3b

0x[0-3]

0x00

0x[0-31]0

0x00

0x00

Table 4 - AES REG command structure

For example:

AES REG d0, t1

* AES KEY

Writing key to AES key registers, it receives as parameters AES key register ( k[0:3] ) and RISC-V register.

Funct3 = 1

Command structure:



0x3b

0x[0-3]

0x10

0x[0-31]0

0x00

0x00

Table 5 - AES KEY command structure

For example:

AES KEY k1, t3

* AES MEM

Writing an address to the AES WB register, which holds the write-back address. It receives as parameter RISCV register.

Funct3 = 2

Command structure:



0x3b

0x0

0x20

0x[0-31]0

0x00

0x00

Table 6 - AES MEM command structure

For example:

AES MEM t5

After storing the data, key, and write-back address in the AES register file, we can use the AES RUN command (with no parameters), to start the ciphering process:

* AES\_RUN

Funct3 = 4



0x3b

0x0

0x40

0x0

0x00

0x00

Table 7 - AES RUN command structure

For example:

AES RUN

At the end of the ciphering process, the AES WB module will write the ciphered data to the memory in 4 blocks of 32-bit, to the 4 memory blocks that start at the write-back address.

# **Design and Implementation**

## Flow

The flow of the AES implementation inside the RISCV- core is divided into three main modules:

* AES register file (“riscv\_aes\_registers”):

Contains 4 data registers, 4 key registers, and 1 write-back address register.

It receives AES instruction number, and instruction parameters (if any are given), and according to the instruction it manipulates the given parameters and sends the correct signals out.

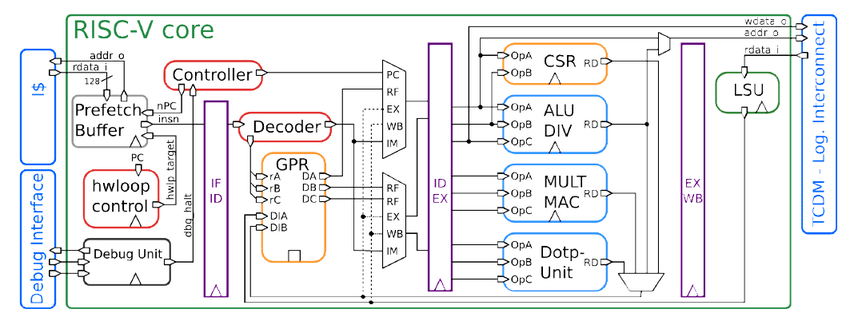
* AES Engine (“AES\_top”):

Contains the AES algorithm.

* AES WB (“riscv\_aes\_wb”):

Functions as a write-back module, it contains a state machine, which halts the RISC-V pipe each time it receives a new ciphered text.

It then writes to the write-back address one register (32-bit) of ciphered data at a time.



AES engine

AES reg file

AES WB

128-bit data

128-bit key

32-bit

128-bit data

128-bit ciphered

32-bit

Figure 11 - RI5CY CORE with AES flow

## AES register file

We designed the AES register file to hold 4 data registers, 4 key registers, and a write-back register.

The register file sends the above registers to the AES engine.

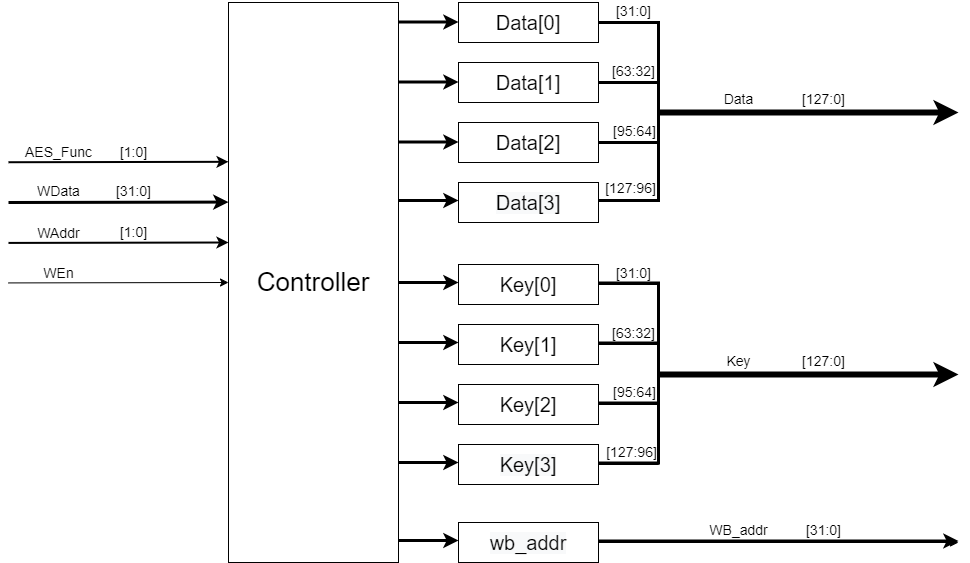


Figure 12 - AES register file module diagram

### Simulate the AES register file

In the simulation below, we loaded the 128’h deadbeefdeafbabe0000000000000000 into the data registers inside the AES register file:

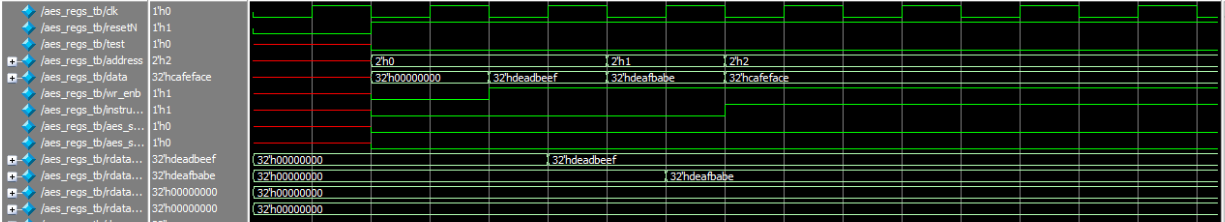
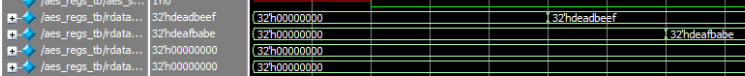


Figure 13 - AES register file simulation example

## AES engine

The second phase of the project was to implement 10 rounds, 128-bit, AES algorithm in SV.

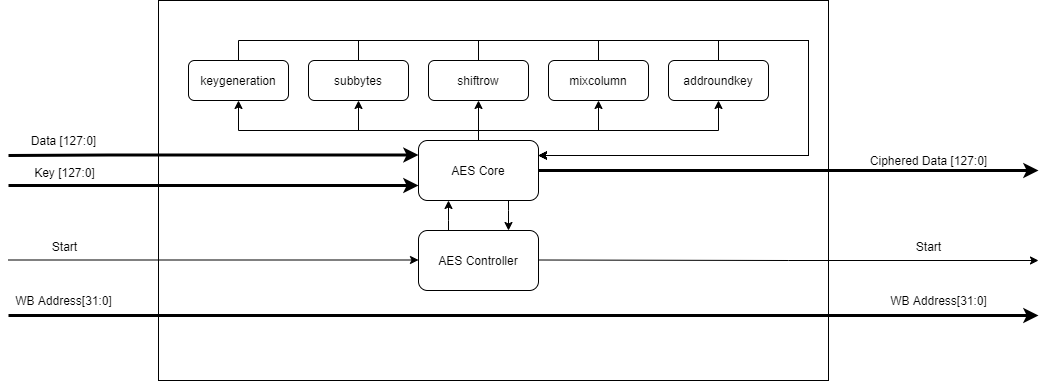


Figure 14 - AES engine module diagram

We found a basic implementation of the above algorithm in Git-Hub, we used it as a basic starting point to the RISCV AES implementation.

The top-level is running the 10 rounds of AES cipher one after another.

The rounds are managed by the controller, which sends to the core signals that indicate which module should work at any given cycle.

The core module calls the following modules in each round (in that order):

addroundkey

keygeneration

subbytes

shiftrow

mixcolumn

Each of the modules represents each one of the AES processing steps that occur in every round (except the last round, which runs only the first three steps).

### Simulate the AES engine

In the simulation below (in Mentor Graphics’s ModelSim PE), we loaded the 128’h deadbeefdeafbabe0000000000000000 into the data registers, and 128’h 0000000000000000cafeface00000000 into the key registers, and set the start signal to 1.

We can see in the waveform, that in the cycle after setting the start signal to 1, the start signal in the output raised, and the cyphered data bits updated to the correct cyphered data: 128’h 2da8a1cf3772e5a2a49c22d1fd03b8a8 (verified by AES algorithm implemented in python):

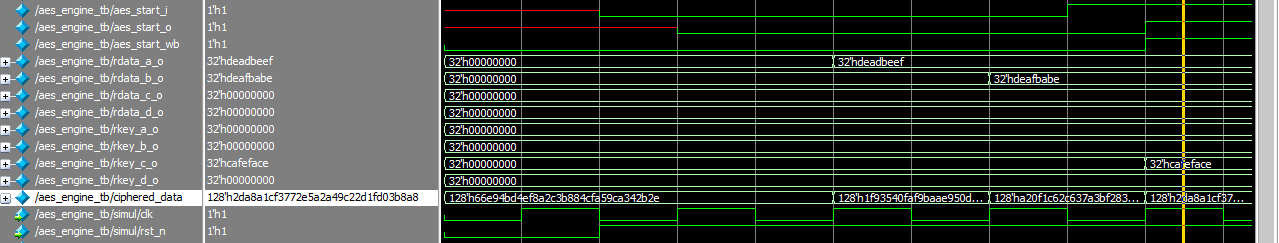
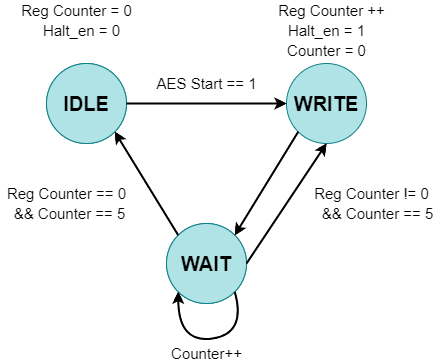


Figure 15 - AES engine simulation example

## AES write-back

We designed the write-back as a state-machine:

****

The state-machine starts in the “IDLE” state and waits in this state till the “AES Start” signal from the AES engine raises.

Once the “AES Start” signal raises, it switches to the “WRITE” state, and in this state the “halt\_en” signal raises (which halts the pipeline), parsing the data to 32-bits, and start to write the data to the memory (6 clock cycles every write).

After finishing with the memory writing, the state-machine switches to the “FINISH” state, which resets the “halt\_en” signal, and return the machine to the “IDLE” state.

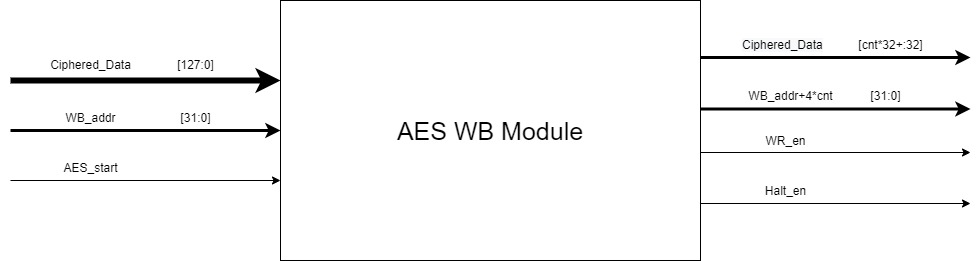


Figure 16 - AES write back module diagram

### Simulate AES engine with register file and write-back module

After implementing the AES register file and write-back module, we integrate it with the AES engine and simulate it.

In the simulation below, we loaded the same data and key as the last simulation, but this time to the register file (instead of directly to the AES engine) and received the same ciphered data.

The ciphered data was parsed by the write-back module into 4 32-bit registers (in RED), and each one of the registers was sent out with an address, while the address is raised by 4 (in Orange) with each register (the registers are stored in adjacent locations in the memory):

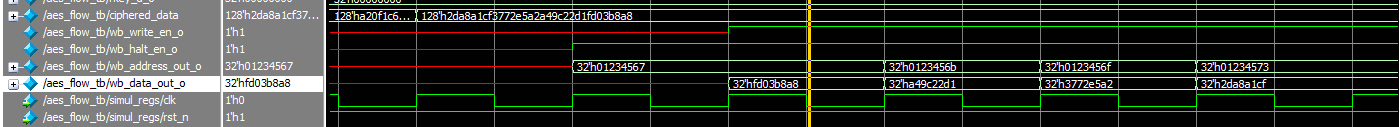


Figure 17 - AES write back simulation example

## Integrate the AES flow with RISC-V core

After implementing and simulating the AES flow, we integrated the AES flow with the RISC-V core, and from this step, we switched from working with Mentor Graphics’s “ModelSim PE”, to working with Cadence and Synopsys tools, that provided to us by VLSI lab.

During the integration, we decided to put the AES modules (register file, engine, and write-back) in the CORE module of the RISC-V, which gives us the ability to take signals from the original RISC-V modules relatively easy, and add the AES flow as parallel as we can to the RISC-V flow (keep the RISC-V performance).

In addition to adding the AES modules, we had to update modules in the ID, EX, and WB stages.

There were a few different changes to be done:

* Decoding of AES commands:

Since we added new commands to the RISC-V, we had to add those commands to the Decoder module, to parse the new commands properly.

* Signals in the ID stage:

To receive data from the main register file (according to the AES commands), we had to update signals in the ID stage.

* Signals in the EX stage:

Halting the pipe during the write-back of ciphered data to the memory was done by sending signals to the EX stage.

* Write-back signals and data:

To write the ciphered data in the memory, we had to halt the pipe, supply the data and addresses to be written, and raise a writing signal to the LSU.

# **Simulate and Debug**

When we first started to run the full AES flow on the RISC-V, we had a lot of problems:

* Syntax errors

Mismatched signal names - fixed easily by renaming the incorrect signal.

* Connections problems

After synthesis, we saw in the RTL schematic view that one of the outputs of the write-back module is disconnected:

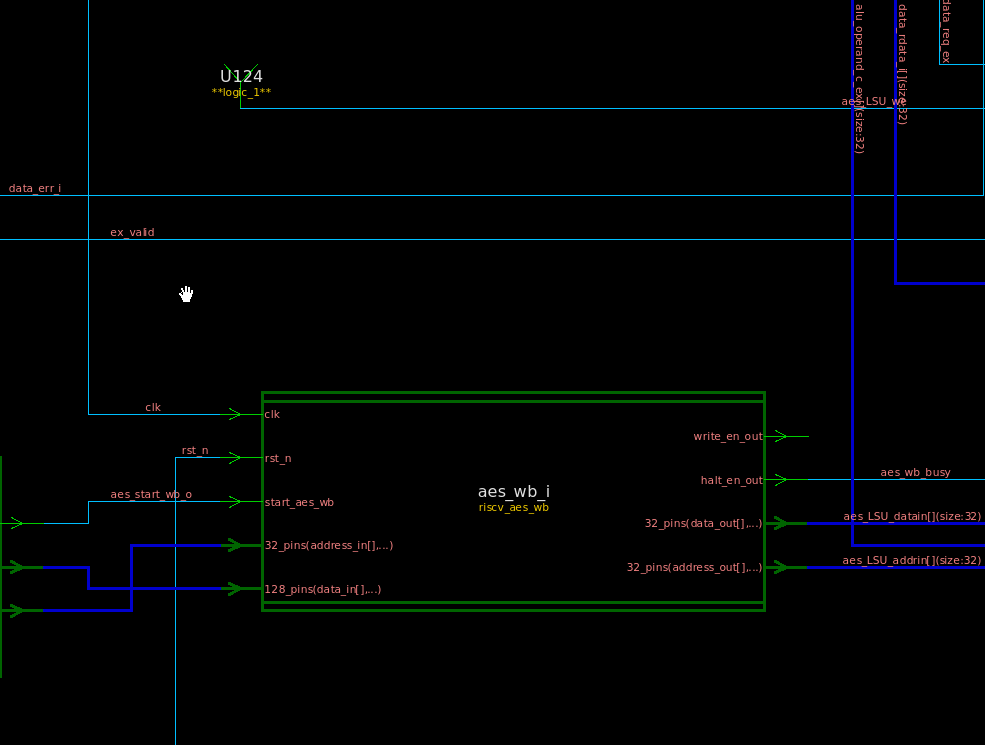


Figure 18 - AES write back - wen bug

After looking for the problem in the AES write-back module and the LSU, the cause of this issue was defining the write\_en\_out signal only once (to logic 1) in the AES write-back module, which caused the dc\_shell to replace the connection with logic 1 signal during synthesis. After adding resets to this signal, the problem was solved:

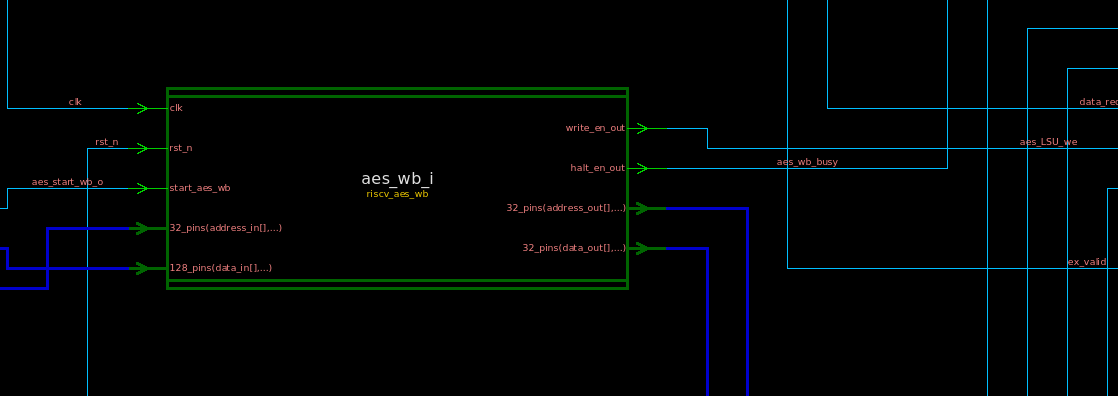


Figure 19 - AES write back - wen fix

* Flow issues

When we started testing the AES flow, we had an issue with writing to the first AES data register in the register file, which caused the value we written to the register being overwritten with 0:

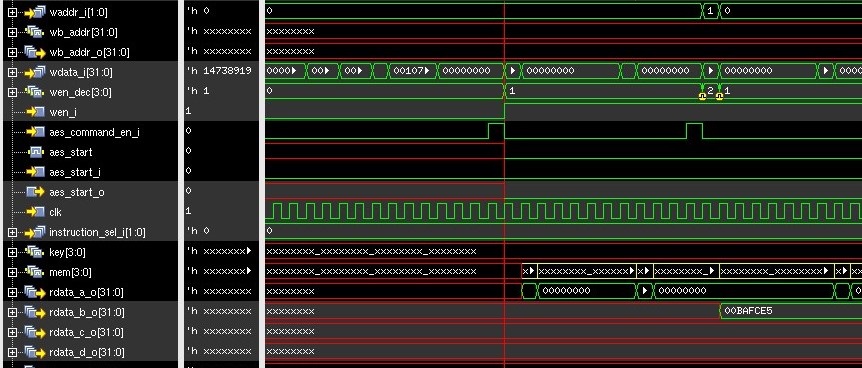


Figure 20 – AES register file – data register override

We can see in the waveform that data is being stored in the first AES register, and in the next cycle, the data is replaced with zeros (in RED).

The cause of this bug was the wen\_i signal, which changes to logic 1 (in BLUE) once we started writing to the AES register file, and didn’t go back to logic 0.

We found the source of this bug in the ID stage main module, due to updating the above signal only when we have the AES command, thus resulting in wen\_i stuck on logic 1 after AES writing command.

We fixed the issue by updating the wen\_i signal on every clock cycle:

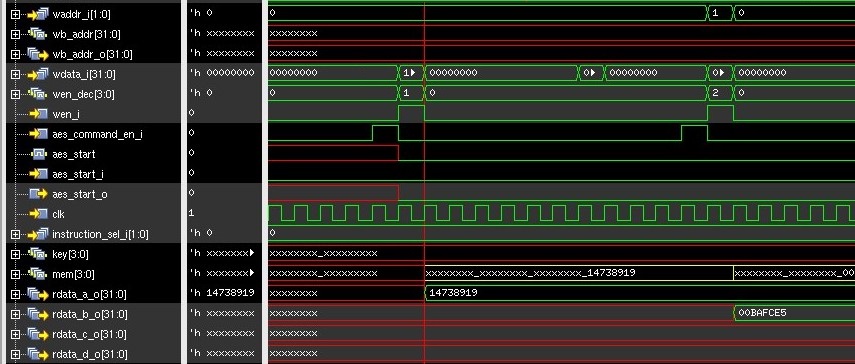
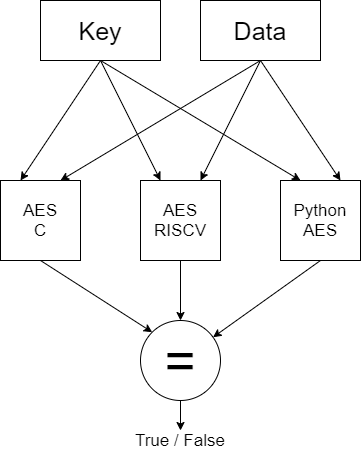


Figure 21 - AES register file – data register override fix

# **Conformity check**

To check that our design is not only compiled and runs, but also encrypt the data properly, we designed a verification script, which works as follows:



The script generates 128bit random key and 128bit random data, and then send the data to 3 implementations of AES:

* AES C – AES algorithm implemented in C, and compiled to run on our RISCV core.
* AES RISCV – AES algorithm implemented in SV inside the RISCV core.
* Python AES – AES algorithm implemented in Python, and runs on the Linux operating system.

After receiving the results from the 3 implementations, we compare them to see if all the 3 encrypted texts are identical (in BLUE):

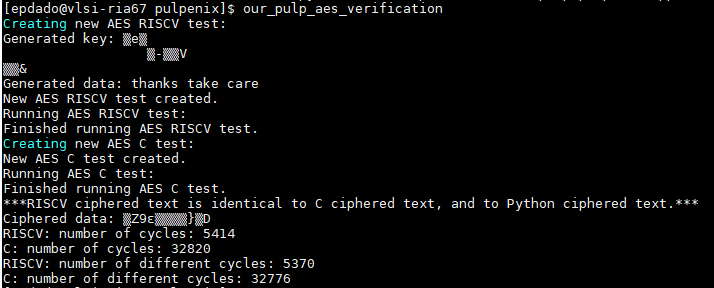


Figure 22 - AES verification - success

The number of cycles is also printed (in RED), specifying the number of different cycles between the AES RISCV test and the AES C test.

If one of the three is different from the other, an error message is printed specifying the results of the different implementations (in RED):

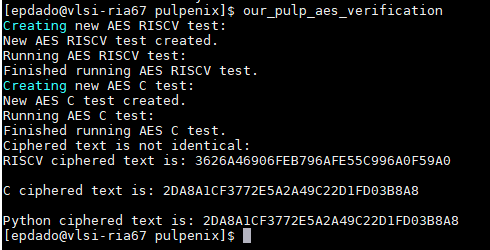


Figure 23 - AES verification - failure

# **Performance**

## CoreMark

|  |  |
| --- | --- |
| GenPro PULPenix | GenPro PULPenix AES |
| Figure 24 – GenPro PULPenix CoreMark | Figure 25 - GenPro PULPenix AES CoreMark |
|  |  |

CoreMark is a benchmark program, a program that runs several chosen algorithms, that test different aspects of hardware performance.

The benchmark program gives, as a result, the number of clock cycles took the CPU to run the program, to compare to other CPUs.

As seen above, both the original RISCV and our RISCV AES ran for 369594 cycles.

CoreMark score is calculated as follows:

thus, the CoreMark score of both the original RISCV and our RISCV AES is:

|  |  |
| --- | --- |
| GenPro PULPenix | GenPro PULPenix AES |
| Figure 26 - GenPro PULPenix power report | Figure 27 - GenPro PULPenix AES power report |
|  |  |

## Power

Our solution effect on the power in percents:

## Area

|  |  |
| --- | --- |
| GenPro PULPenix | GenPro PULPenix AES |
| Figure 28 - GenPro PULPenix area report | Figure 29 - GenPro PULPenix AES area report |
|  |  |

We can see that the AES flow is taking a quite big area – the RISCV with AES is 1.5 times bigger than RISCV without AES.

Our solution effect on the area in percents:

## Timing

|  |  |
| --- | --- |
| GenPro PULPenix | GenPro PULPenix AES |
| Figure 30 - GenPro PULPenix timing report | Figure 31 - GenPro PULPenix AES timing report |
|  |  |

As seen above, our solution had not affected the critical path delay in the RISCV processor, and the processor can work with a clock without a problem.

# **Compiler**

To use the RI5CY core inside the PULPenix controller, we had to write “apps” in C or assembly, which later being compiled by GNU’s compiler into hexadecimal words, and those words are being written to the instruction memory of the RI5CY core.

During the project, we added 4 new commands to the core.

To use those commands, we need to manually parse them into hexadecimal words, since the new commands are not supported by GNU’s compiler.

The manual parsing of the AES commands takes a lot of time when you work a lot with the new commands.

Also, debugging is getting harder, since it’s hard to get the values we chose after parsing the command into hexadecimal word.

AES commands compilation options

We had 3 options regarding the compilation of AES commands:

* Manually parse the AES commands – keep parse the commands manually, hoping there won’t be a lot of changes.
* Update the GCC – getting inside the GCC source files, and insert our commands into the parsing process.
* Create a pre-compile step – create a script that compiles the AES commands before running the GNU’s compiler.

We decided to create a pre-compile step.

AES compiler

Our pre-compile step is written in Python, it receives <file\_name>.c file, and clone the file with a new file named <file\_name>\_pre\_compile.c.

After cloning the file, the script parses only the AES commands inside the file, and store the file with the compiled AES commands in <file\_name>.c.

The script will print a message if it ends successfully:

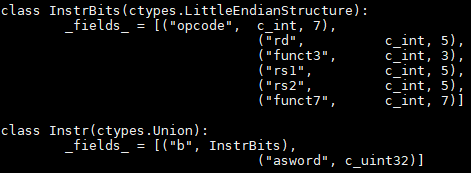


Example of AES command compilation:

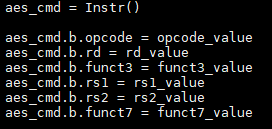
|  |  |
| --- | --- |
| Before AES compile: | After AES compile: |
|  |  |

In our script we used several Python packages and data structures, that helped us create a clean and easy to maintain code:

* ctypes – the ctypes package allows us to create a class that is built out of several fields, each with a different length in bits, enabling us to create our desired command structure, and place the required values in the correct fields very easily.



Example to an assignment of values to an instance of ctypes class:



The class name is “Instr”, the instance of “Instr” is named aes\_cmd, and when we access to aes\_cmd.b we get the fields available in the class, and can change their value.

* Python dictionaries – we use Python dictionaries instead of using constant values such as opcodes of commands, actual Index of the register, etc.

|  |  |
| --- | --- |
|  |  |

Example of usage of aes\_funct3\_dict:



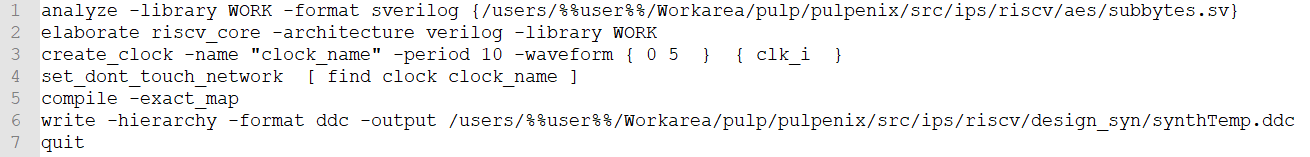
After checking if the current command is “aes\_run”, we assign the funct3 field of the command to be the value stored in the funct3 dictionary under the “aes\_run” key.

# **Methodology**

During the project, we decided we want to create an easier and faster way to synthesize the project.

After some research, we found a dc\_shell command that allows running a script on the dc\_shell without opening the GUI.

Example of a script to run on the dc\_shell:



1st line - “analyze” step, in the script above there is only one file to analyze (as an example).

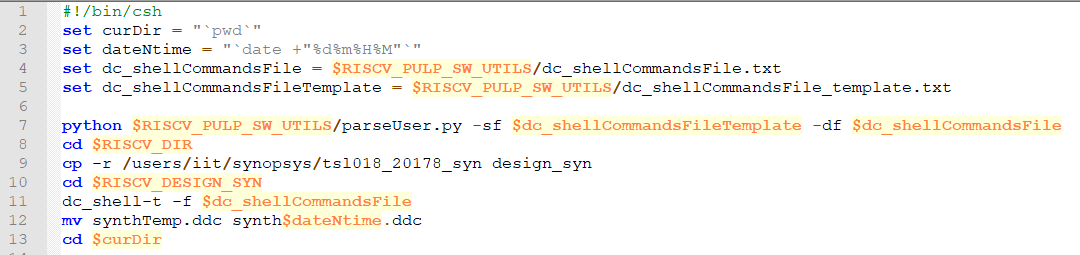
2nd line - “elaborate” step, we can see in the script above that the “riscv\_core” has been chosen as the top module, and the library to the synthesis is WORK.

3rd and 4th lines - create a clock, in the above script the clock is .

5th line - compiling the project.

6th line - saves the synthesis architecture file in the temporary name (which we change in the next step).

The top script of the synthesis:



The script updates the dc\_Shell script with the current user name (in the full path of the design files), and then changes the directory to the design\_syn directory and sends the updated script to run on dc\_shell.

At the end of the process, a new .ddc file is created, with the current time as its name (.ddc file contains a gate-level description and design constraints of the chip) in the design\_syn directory.

# **Summary**

The main goal of this project was to implement an AES engine inside the RISCV core, in order to shorten the time of encryption of data in the processor, and allow encryption of data before storing the data to the memory, thus gaining a more secure processor.

During the project, we successfully implemented a full AES flow, which includes an AES register file that holds all the data the AES engine needs, an AES engine that encrypts the data, and an AES write-back module which writes the encrypted data to the memory.

To make the AES commands easily available to the user, we implemented a pre-compiler, which converts the AES commands to a hexadecimal word before running the GNU’s compiler (GCC).

Also, the secondary goal was to make the PULPenix setup and synthesis more automatic and user friendly.

To make the setup easier, we added a full synthesis script to the project, thus allowing the user to run synthesis in a single command (without opening the GUI).

Also, we added some new scripts and added environment variables to the setup script, thus allowing the user to navigate more easily in the project.

# **Appendix A: Design changes**

During our work on the project we added the following files (under pulp/pulpenix/src/ips/riscv/) :

* aes/aes\_sbox.sv
* aes/AddRndKey\_top.sv
* aes/matrix\_mult.sv
* aes/KeySchedule\_top.sv
* aes/subBytes\_top.sv
* aes/shiftRows\_top.sv
* aes/MixCol\_top.sv
* aes/AEScntx.sv
* aes/AESCore.sv
* aes/AES\_top.sv
* riscv\_aes\_wb.sv
* riscv\_aes\_registers.sv

Also, we changed some of the PULPenix original files:

* riscv\_defines.sv
* riscv\_decoder.sv
* riscv\_ex\_stage.sv
* riscv\_load\_store\_unit.sv
* riscv\_id\_stage.sv
* riscv\_core.sv

# **Appendix B: User guide**

In order to use the PULPenix AES, a few steps must be done:

1. Clone the project from Github to /%user%/Workarea/pulp/ (the exact path is important to the project’s scripts).
2. Add GCC for RISCV to pulp directory:
   1. Run in the command line:

>mkdir toolchain

>cd toolchain

* 1. Download and un-tar [GCC for RISCV](https://github.com/gnu-mcu-eclipse/riscv-none-gcc/releases/download/v7.2.0-2-20180110/gnu-mcu-eclipse-riscv-none-gcc-7.2.0-2-20180111-2230-centos64.tgz) into the “toolchain” directory.
  2. Run from inside “toolchain” directory:

>mv gnu-mcu-eclipse/riscv-none-gcc/7.2.0-2-20180111-2230 gnu-mcu-eclipse/

>rm -r gnu-mcu-eclipse/riscv-none-gcc

1. There are some shortcut scripts and environment settings that necessary in order to work efficiently with PULPenix.

Running PULPenix setup:

>source <path\_to\_pulp>/pulp/pulpenix/misc/genpro\_pulpenix\_setup.sh

Consider adding the above line to your .cshrc (in order it to run on startup).

Then you will have the PULPenix commands and scripts available, you can see those at:

<path\_to\_pulp>/pulp/pulpenix/misc/scripts

<path\_to\_pulp>/pulp/pulpenix/apps/sw\_utils

## Synthesis

To run the synthesis and create a “fresh” copy of PULPenix, you can use the “shortcut” script:

> our\_pulp\_synthesis

The technology in use is Tower , with clock () with a duty cycle.

If an error message occurs, you’ll need to do a full manual synthesis via dc\_shell:

1. Go to RISCV folder by typing:

>cd $RISCV\_DIR

1. Copy the library files using the command:

>cp -r /users/iit/synopsys/tsl018\_20178\_syn design\_syn

1. Type in your terminal the following commands:

>cd $RISCV\_DESIGN\_SYN

>dc\_shell

>start\_gui

1. In the GUI that opened, go to the upper left corner and click:

File -> Analyze -> Add

and add:

riscv\_defines

riscv\_config

apu\_macros

apu\_core\_package

If the last step gives you errors, it’s probably because of the files themselves including each other, so try adding them one by one in that order.

1. Click:

File -> Analyse -> Add

And add everything under the “riscv” folder, except the files mentioned above, the “riscv\_tracer” files, and “riscv\_register\_file\_latch”.

1. Click:

File -> Analyse -> Add

and add everything under the “aes” folder.

1. Click:

File - > Elaborate

Choose the library to be WORK and the top-level module to be “riscv\_core”

1. Specify a clock:

In the hierarchy pane, click on the hierarchy drop-down menu and filter by “pins/ports”, and click on your clock-signal (clk\_i).

In the upper bar of the GUI, click:

attributes->specify clock.

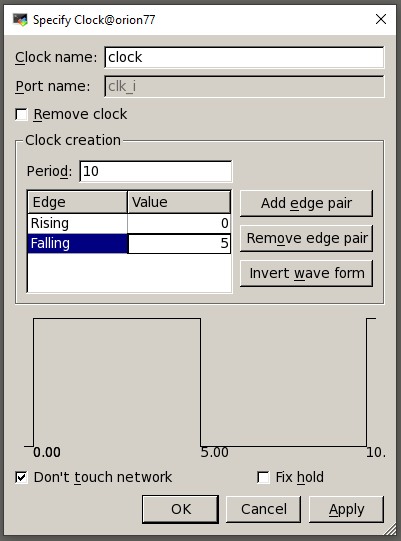


Figure 32 - specify clock window

We specified the clock to be – 10 [ns] (frequency of 100 [MHz]), and symmetrical.

1. In the upper bar click:

Design -> Compile Design

1. After compilation click:

File->Save As <name>, then click: Open

To open:

File -> Read <name>

1. In the logical hierarchy pane, right-click on the top-level module and select Schematic View. Then, you’ll be able to watch the synthesized file at the gate level.

## Simulation

In order to run a simulation, a few steps must be done:

1. Create a folder under pulp/pulpenix/apps with your program (source code, .c files)
2. Compile your program:

cd $MY\_PULP\_APPS/<progname>

our\_pulp\_compile <progname>

This step converts the AES commands to .word commands (by using AES compiler, converts into the hexadecimal base), creates .s files (assembly files), .elf files (Executable Linkable Format), and .slm files (memory initialization files) out of your source files.

If the compilation fails, check your code for errors and run again.

1. Get your app:

> cd $MY\_PULP\_IRUN

> pulp\_get\_app <progname>

this step copies your .slm files to the irun folder.

1. Run:

You have three main options for running your program:

* 1. running with wave form:

> pulp\_irun\_probe

The waves file will be created in $MY\_PULP\_IRUN/waves.shm folder.

* 1. running with trace:

> pulp\_irun\_trace

The trace file will be named “trace\_core\_00\_0.log” inside $MY\_PULP\_IRUN folder.

* 1. running with trace and probe:

> pulp\_irun\_probe\_trace

There is a shortcut script that runs steps 2,3 and 4.c:

> our\_pulp\_run <progname>

The waves file will be saved as:

$MY\_PULP\_APPS/waves/<name>.shm

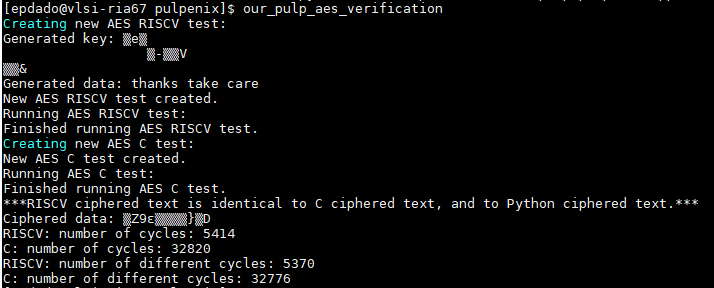
The trace file will be saved as:

$MY\_PULP\_IRUN/trace\_core\_00\_0.log

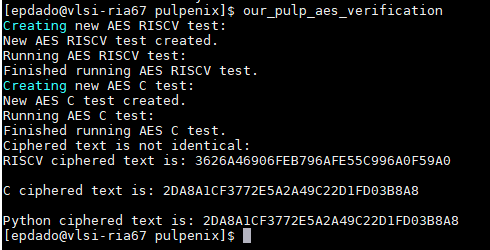
AES verification test

You can also run the AES verification test. running the test:

> our\_pulp\_aes\_verification

The results of the test will be printed on the screen, in case of success: 

In case of failure (see more at [Conformity check](#_Conformity_check)):



## Simvision

To see the waveform of the simulation, open Simvision:

> simvision &

In simvision:

File -> Open Database

in the browse tab, there will be a folder called waves.shm, select it, and then click `open & dismiss`.

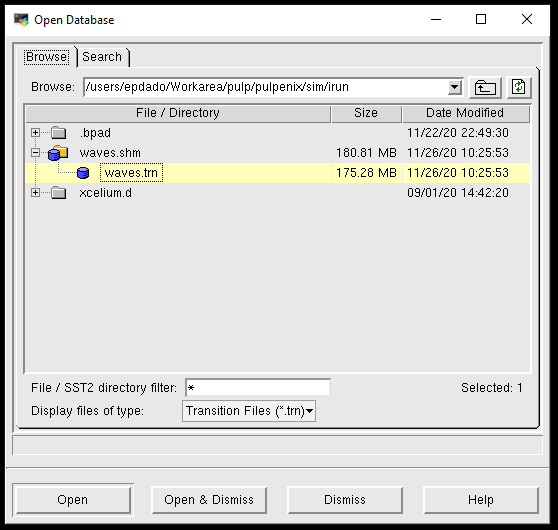


Figure 33 - open database window

You’ll find the RISC-V design under tb/top\_i/core\_region\_i/CORE/RISCV\_CORE:

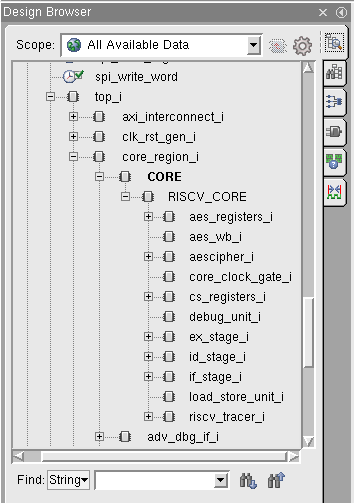


Figure 34 - signals select window

Now you can add signals of your choice to the waveform, and travel across the simulation timeline.

You can save a command script, which will save all your actions on the Simvision session (signals, markers, position on the timeline, etc.) since you opened it:

File -> save command scrip

Choose a name and location

OK

Running a command script:

File -> source command script

Choose your script

Open

## Trace file

Inside the trace file, you can see each assembly command that runs on the CPU and its:

* Cycle - cycle number in the simulation.
* Time - Time in the simulation.
* PC - Program Counter, the address in which the command is stored inside the instruction memory.
* Instr – hex decoding of the assembly instruction.
* Mnemonic – the assembly instruction, and the values of the registers after the current instruction.

The time column can help in finding the required commands in the waveform.

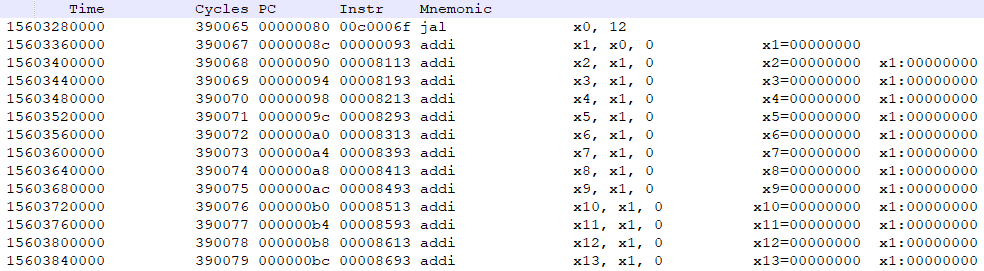
Example for trace file:

Figure 35 - trace file example

The first lines

# Bibliography

[Book].

"Announcing the ADVANCED ENCRYPTION STANDARD (AES)" [Journal] // Federal Information Processing Standards Publication 197 United States National Institute of Standards and Technology (NIST). - November 26, 2001..

Advanced Encryption Standard [Online] // Wikipedia, the free encyclopedia.

**Andreas Traber Michael Gautschi, and Pasquale Davide Schiavone** RI5CY User-Manual [Book]. - 6, Apr 2019.

**Andrew Waterman Krste Asanovic** The RISC-V Instruction Set Manual Volume I: User-Level ISA [Journal]. - 2017.

**datasheet Pulpino** [Online].

**gowgos5** aes-verilog [Online] // GitHub. - https://github.com/gowgos5/aes-verilog.

**Waterman Andrew Asanović Krste** "The RISC-V Instruction Set Manual, Volume I: Base User-Level ISA version 2.2" [Book].

**Waterman Azndrew Asanović Krste:** "The RISC-V Instruction Set Manual, Volume I: Base User-Level ISA version 2.2" [Book].

**Westlund Harold B.** "NIST reports measurable success of Advanced Encryption Standard". [Journal] // Journal of Research of the National Institute of Standards and Technology.. - 2007-11-03.

1. Waterman A (Placeholder1)ndrew, [Asanović Krste](https://en.wikipedia.org/wiki/Krste_Asanovi%C4%87): ["The RISC-V Instruction Set Manual, Volume I: Base User-Level ISA version 2.2"](https://riscv.org/technical/specifications/) [↑](#footnote-ref-1)
2. [Asanović, Krste](https://en.wikipedia.org/wiki/Krste_Asanovi%C4%87). ["Instruction Sets Should be Free"](https://www2.eecs.berkeley.edu/Pubs/TechRpts/2014/EECS-2014-146.pdf) [↑](#footnote-ref-2)
3. Waterman, Andrew; [Asanović, Krste](https://en.wikipedia.org/wiki/Krste_Asanovi%C4%87). ["The RISC-V Instruction Set Manual, Volume I: Base User-Level ISA version 2.2"](https://riscv.org/technical/specifications/) [↑](#footnote-ref-3)
4. Andreas Traber, Michael Gautschi, and Pasquale Davide Schiavone, RI5CY User-Manual, 6, Apr 2019 [↑](#footnote-ref-4)
5. Pulpino datasheet [↑](#footnote-ref-5)
6. Westlund, Harold B. (2002). "NIST reports measurable success of Advanced Encryption Standard". Journal of Research of the National Institute of Standards and Technology. Archived from the original on 2007-11-03. [↑](#footnote-ref-6)
7. "Announcing the ADVANCED ENCRYPTION STANDARD (AES)" (PDF). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. [↑](#footnote-ref-7)
8. 8 Advanced Encryption Standard, From Wikipedia, the free encyclopedia. [↑](#footnote-ref-8)