



# RISC-V ISA

Labor Architecture des ordinateurs

## Contenu

1 Objectifs .....	2
2 Instructions .....	3
2.1 Constantes (Immediate) .....	4
2.2 Calculs de base .....	4
2.3 Accès mémoire .....	4
2.4 Algorithmes .....	4
3 Programmation impérative .....	6
3.1 Branching .....	6
3.1.1 If / else .....	6
3.1.2 Switch case .....	6
3.2 Loops .....	6
3.2.1 While / Do While .....	6
3.2.2 For .....	6
3.3 Fonctions .....	7
3.4 Algorithmes .....	8
3.4.1 Fibonacci par récursivité .....	8
3.4.2 Nombre au carré .....	8
4 Assembler / Disassembler .....	9
4.1 Program Ripes .....	9
4.1.1 Installation Ripes .....	9
4.1.2 Setup Ripes .....	10
4.2 Analyse 1: Gestion de la mémoire dans Ripes .....	10
4.3 Analyse 2: Fonction main .....	11
4.4 HEIRV-32 .....	13
4.4.1 Utilisation <b>HEIRV32-asm</b> .....	14
4.4.1.1 Ligne de commande (CLI) .....	14
4.4.1.2 Avec l'interface graphique (GUI) .....	16
4.4.2 Analyse 3: Assembly & Disassembly .....	17
4.5 Reverse Engineering .....	18
Bibliographie .....	23



# 1 | Objectifs

Ce laboratoire est divisé en plusieurs blocs réalisés sur plusieurs semaines. Le but est de se familiariser avec le langage assembleur du RISC-V.

- La partie Chapitre 2 du laboratoire porte sur les instructions individuelles.
- La partie Chapitre 3 du laboratoire nous amène à la programmation impérative, respectivement aux boucles et aux fonctions.
- La dernière partie Chapitre 4 du laboratoire est consacrée au travail sur le compilateur : l'assemblage et le désassemblage d'un programme (passage d'un langage haut-niveau à du code machine et inversement).

Dans cette première partie du laboratoire, nous allons travailler avec l'interpréteur RISC-V sur le site <https://course.hevs.io/car/riscv-interpreter/>, voir illustration Fig. 1. Celui-ci permet aux registres d'écrire en mémoire et d'exécuter le code étape par étape. Ces outils en ligne vous aideront à résoudre et à contrôler les tâches.

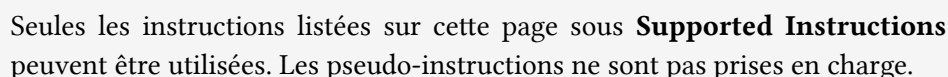


Fig. 1. – Interpréteur RISC-V en ligne



- Le type **int** est considéré de taille 32 bits signé.
- Le type **unsigned int** est considéré de taille 32 bits non-signé.
- Si il est suivi d'un nombre (ex: **int16\_t**), cela signifie que la variable est sur x bits (ici 16). Si précédé d'un **u**, il est non-signé.

3 / 23



## 2.1 Constantes (Immediate)

Écrire le code assembleur RV32i pour les instructions suivantes :

a)

```
int a = 10;
int b = 0;
a = a + 4;
b = a - 12;

int i = 0;
int x = 2032;
int y = -78;
```

b)

```
int a = 0xABCDE123;
int b = 0xFEEDA987;
```

## 2.2 Calculs de base

Écrire le code assembleur RV32i pour les instructions suivantes :

a)

```
int b = 1;
int c = 2;
int d = 5;
a = b + c - d;
```

b)

```
int b = -1;
int c = 2;
int d = -78;
a = b + c - d;
```

c)

```
int b = -12;
int c = 2023;
int d = 22;
a = b + c - d;
```

## 2.3 Accès mémoire

Écrire le code assembleur RV32i pour les instructions suivantes :

a)

```
# We have an array of int, i.e., multiple
ints one after the other in memory such
as [int0][int1][int2] ...
# The notation mem[x] means getting the
x th element of that array

int a = mem[4];

int b = mem[5];
```

b)

```
mem[5] = 42;
```

## 2.4 Algorithmes

Écrire le code assembleur RV32i pour les algorithmes suivants, en utilisant uniquement les instructions de base sans *loops*, *conditionals* ainsi que *branches* :

1. Dans un système, il peut être nécessaire d'attendre sans rien faire, sans modifier l'état actuel du système (pas d'accès mémoire, pas de modification des registres). Cette opération est communément appelée **NOP** (NO Operation).



1. Proposez une instruction pour ce faire.
2. Testez qu'aucun registre ni valeur mémoire n'est effectivement modifié.
2. Calculer les 10 premiers nombres de Fibonacci. Enregistrer chaque nombre dans un registre différent.



## 3 | Programmation impérative

### 3.1 Branching

#### 3.1.1 If / else

```
int a = 1, b = 2, c;  
  
if(a == b) {  
    c = 1;  
}  
else {  
    c = 0;  
}
```

#### 3.1.2 Switch case

```
int a, b;  
  
switch(b) {  
    case 0:  
        a = 17;  
        break;  
    default:  
        a = 99;  
}
```

### 3.2 Loops

#### 3.2.1 While / Do While

```
// A  
int a = 10;  
  
do{a = a - 1;}  
while(a != 0);  
  
// B  
int a = 10;  
  
while(a >= 0)  
{a = a - 1;}
```

#### 3.2.2 For

a)

```
unsigned int a = 0, i;  
  
for(i = 0; i < mem[0]; i = i + 1) {  
    a = a + 2;  
}
```

b)

```
// An array of 10 bytes  
uint8_t myArray[10] = ...  
// ...  
  
// Let say myArray[0] is at the address  
// saved in register s0.  
// Arrays are contiguous in memory:  
myArray = [el0][el1][el2]...[elN]  
  
int i;  
  
for(i = 0; i < 10; i = i + 1) {  
    myArray[i] = myArray[i] - 5;  
}
```



### 3.3 Fonctions

Bien qu'un programmeur seul puisse agencer son code comme il l'entend, certaines conventions ont été établies pour permettre l'interopérabilité de plusieurs sources de code entre elles.

La fonction en appelant une autre est nommée **caller** et la fonction appelée nommée **callee**. Elles doivent être synchronisées sur la façon dont sont passés les arguments, quels registres doivent être conservés ...

Les notions suivantes sont les règles essentielles:

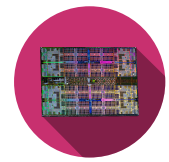
- Les registres **a0** à **a7** permettent de passer des arguments. Si plus sont nécessaires, ils sont passés sur le stack.
- Le résultat est placé dans le registre **a0**.
- Le **caller** enregistre l'adresse de retour (PC + 4) générée par l'instruction **jal** dans le registre **ra**.
- Le **callee** ne doit pas réécrire l'adresse de retour, le stack ou encore les registres sauves sXX. Si elles sont utilisées, l'espace doit être réservé sur le stack et ces informations doivent être stockées puis restaurées.

a)

```
doNothing();  
  
...  
  
void doNothing() {  
    return;  
}
```

b)

```
int a = 1, b;  
b = callA(a);  
  
...  
  
// Functions can be  
// optimized at will  
  
int callA(int v1) {  
    v1 = v1 * 2;  
    return callB(v1);  
}  
  
int callB(int v1) {  
    v1 = v1 + 12;  
    return v1;  
}
```



## 3.4 Algorithmes

### 3.4.1 Fibonacci par récursivité

La notion de récursivité implique qu'une fonction se rappelle elle-même pour calculer un résultat, de la même manière qu'elle appellerait une autre fonction.

Le but est de calculer la suite de fibonacci d'un nombre entier non-signé selon l'algorithme suivant:

```
unsigned int fibonacci(unsigned int n){
    if(n == 0){
        return 0;
    } else if(n == 1) {
        return 1;
    } else {
        return (fibonacci(n-1) + fibonacci(n-2));
    }
}
```

- Implémenter la fonction donnée avec RV32I
- Tester et valider la fonction
- Quelles sont les valeurs  $n$  supportées ?

Il est possible d'accélérer grandement le calcul en utilisant la [mémoïsation](#). Le principe est de réserver de la place mémoire et de stocker les résultats déjà connus pour chaque  $n$  calculé et de réutiliser cette valeur directement.

- Implémenter la fonction donnée. RV32IM est conseillé ici.
- Tester et valider la fonction
- Comparer les algorithmes

### 3.4.2 Nombre au carré

Un nombre mis au carré n'est autre que la multiplication dudit nombre par lui-même. Mais ici, nous ne travaillons qu'avec le set d'instruction RV32I:

- Proposer une fonction capable de calculer  $n * n$  par une boucle d'additions.
- Tester avec  $n = 5, 10$  et  $20$ .
- Généraliser la fonction pour pouvoir lui fournir deux paramètres en calculant  $i * j$ .
- Tester avec  $i = 5, j = 100$ . Tester avec  $i = 100, j = 5$ . Que constatez-vous ?
- Optimiser la fonction pour que l'ordre des opérandes n'influe pas sur le temps de calcul.

Cet algorithme est de complexité  $O(n)$ . Il est possible de le réduire à une complexité de  $O(\log_2(n))$  en utilisant intelligemment les additions et shifts. Ce dernier s'appelle **fast multiplication**:

- Proposer une fonction optimisée.





## 4 | Assembler / Disassembler

### 4.1 Program Ripes

Dans ce laboratoire, vous pouvez continuer à utiliser l'interpréteur en ligne - Fig. 1. En outre, le programme **Ripes** est également disponible, voir l'illustration Fig. 2.

Il supporte tout le set RV32I, les labels ainsi que les pseudo-instructions.

Vous devez d'abord le télécharger et le configurer. Ou si vous utilisez la [version en ligne \(https://ripes.me/\)](https://ripes.me/), il vous suffit de la configurer. Mais vous perdez la possibilité d'écrire du code C.

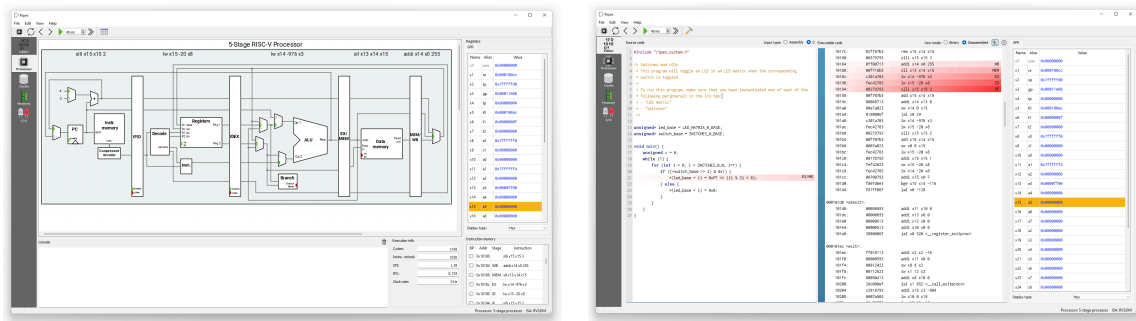


Fig. 2. – Interface graphique de développement de Ripes



Sur les PCs de laboratoire, Ripes et le compilateur **gcc** énoncés ci-après sont trouvables sous **C:/eda/RiscV**.

#### 4.1.1 Installation Ripes

1. Téléchargez la dernière version du programme pour votre plateforme en suivant le lien : <https://github.com/mortbopet/Ripes/releases>.
2. Téléchargez la version suivante de la chaîne d'outils RISC-V -GNU pour votre plateforme en suivant le lien : <https://github.com/sifive/freedom-tools/releases/tag/v2020.04.0-Toolchain.Only>
3. Décompressez les deux et copiez le dossier RISC-V -GNU-Toolchain dans le dossier Ripes.
4. Lancez Ripes et configurez les paramètres du compilateur dans : **Edit** → **Settings**. Pour cela, vous devez sélectionner le fichier **/riscv64-unknown-elf-gcc-8.3.0.exe**.

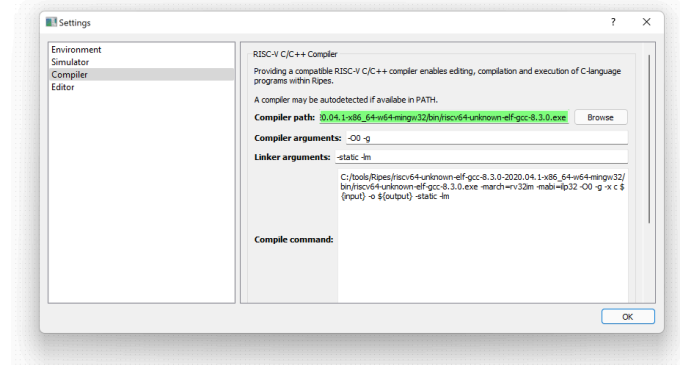


Fig. 3. – Paramètres de la chaîne d'outils de Ripes

#### 4.1.2 Setup Ripes

1. Dans les paramètres du processeur, sélectionnez le processeur monocycle RISC-V → 32-bit → sans extensions ISA.

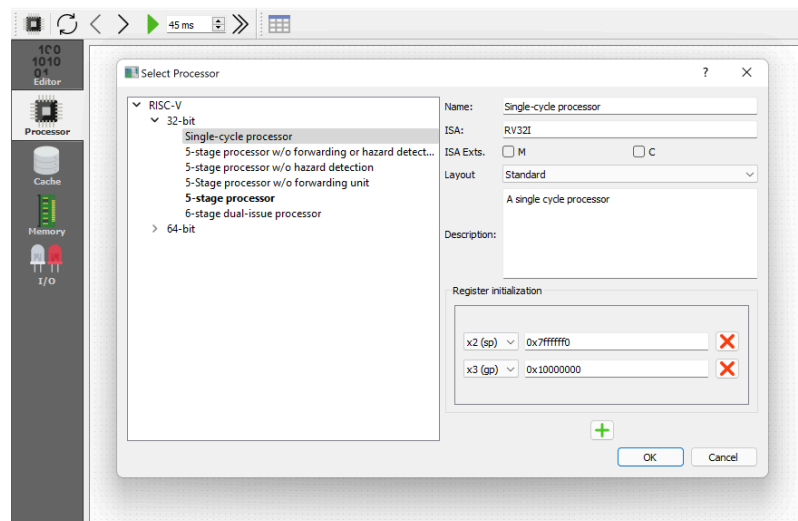


Fig. 4. – Paramètres du processeur de Ripes

## 4.2 Analyse 1: Gestion de la mémoire dans Ripes

Ripes permet de sélectionner plusieurs processeurs (voir figure Fig. 4). Malgré que le processeur single-cycle arbore deux puces de mémoire différentes pour les instructions et les données :

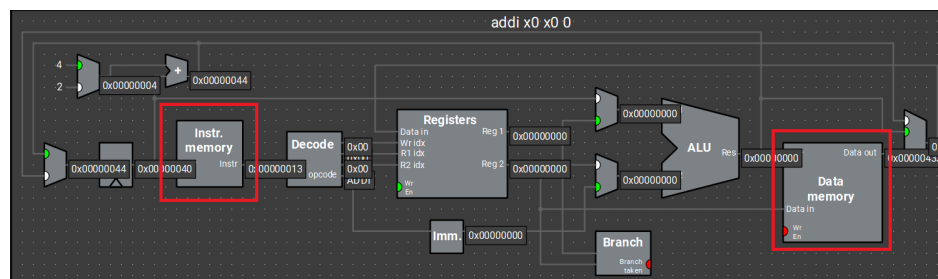


Fig. 5. – Mémoires processeur single-cycle



La mémoire est considérée comme commune, de même que généralement sur une puce physique. Cela veut dire qu'il est possible de **réécrire votre propre code par inadvertance**.



Pour illustrer cela, exécutez le code suivant et regardez comment les instructions sont écrasées dans la mémoire d'instructions.

```
# s0 counts the number of times we really loop
addi s0, zero, 0
addi s1, zero, 0 # place in memory
# t0 is the number of times we SHOULD be looping
addi t0, zero, 10

store_loop:
    sw s0, 0(s1)      # store current loop counter in memory
    addi s1, s1, 4     # increment memory place
    addi s0, s0, 1     # increment how many times we have looped
    addi t0, t0, -1    # decrement loop counter
    blt t0, zero, end
    jal zero, store_loop

end:
    nop
```

La boucle est censée enregistrer 0 à l'adresse 0, 1 à l'adresse 4, 2 à l'adresse 8 ... Mais lors de la quatrième itération de la loop, l'instruction `sw s0, 0(s1)` est exécutée telle que `sw 3, 0(0x0C)`, ce qui remplace cette même instruction par `0x00000003`, correspondant à une instruction `lb x0, 0(x0)`:

0x00000020	4276088943	111	240	223	254
0x0000001c	181347	99	196	2	0
0x00000018	4294083219	147	130	242	255
0x00000014	1311763	19	4	20	0
0x00000010	4490387	147	132	68	0
0x0000000c	3	3	0	0	0
0x00000008	2	2	0	0	0
0x00000004	1	1	0	0	0
0x00000000	0	0	0	0	0

Fig. 6. – Réécriture mémoire

Le code a donc été modifié et ne correspond plus au but initial. Pour éviter de tels problèmes, il faut travailler avec la mémoire au travers du **stack pointer**, comme lors d'appels de fonctions :

- Réservez de la place en mémoire en décrémentant **sp** du nombre de bytes nécessaires (pour l'exemple, nous aurions  $10 * 4$  bytes)
- Travaillez avec la mémoire réservée **UNIQUEMENT**



### 4.3 Analyse 2: Fonction main

Dans le programme Ripes Chapitre 4.1, nous avons compilé les 2 codes C suivants. Cherchez dans le code généré les commandes d'assemblages correspondantes. Que signifient les différentes instructions dans **main**: ?

a)

```
void main() {  
    int a = 0;  
}
```

b)

```
void main() {  
    while(1) {  
        int a = 0;  
    }  
}
```

```
addi sp sp -32 # stack for 8 items  
sw s0 28 sp    # saves s0 in stack[0]  
as it will use it and is a callee saved  
register  
addi s0 sp 32  # s0 points to stack[-1]  
sw x0 -20 s0   # stack[4] = 0  
addi x0 x0 0   # nop  
lw s0 28 sp    # s0 = stack[0]  
addi sp sp 32  # unstack 8 items  
jalr x0 x1 0   # return
```

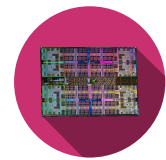
```
addi sp sp -32 # stack for 8 items  
sw s0 28 sp    # saves s0 in stack[0]  
as it will use it and is a callee saved  
register  
addi s0 sp 32  # s0 points to stack[-1]  
sw x0 -20 s0   # stack[4] = 0  
jal x0 -4      # jal to code
```



Que contiennent les deux codes assembleur. Pourquoi sont-ils différents ?



Utilisez Ripes pour réaliser et tester vos laboratoire mais aussi votre série d'exercices. Il est capable de réagir comme un vrai processeur, vous montrant des comportements auxquels on peut ne pas s'attendre (ex. avec la réécriture de son propre programme en gérant mal les instructions L-S - Chapitre 4.2).



## 4.4 HEIRV-32

L'assembleur et désassembleur RISC-V utilisé dans ce labo peut être trouvé dans le repo sous **isa/heirv32-asm/** pour Windows (**HEIRV32-ASM\_1.2.0\_windows\_x86\_64.exe**) & Linux amd64 (**HEIRV32-ASM\_1.2.0\_linux\_x86\_64**) et macOS arm64 (**HEIRV32-ASM\_1.2.0\_macos\_aarch64**). Cet outil vous permet de transformer le code assembleur d'un processeur RV32i ou HEIRV32 en code binaire (Assembly) ainsi que de retransformer le code binaire en code assembleur (Disassembly).

- Assembly  $\Rightarrow$  Fichier assembleur **\*.s** ou **\*.asm**  $\Rightarrow$  Fichier binaire **\*.bin**
- Désassemblage  $\Rightarrow$  Fichier binaire **\*.bin**  $\Rightarrow$  Fichier assembleur **\*.asm**.



L'outil peut être utilisé soit en ligne de commande, soit en tant qu'interface graphique.

```
$cd isa/heirv32-asm
$./HEIRV32-ASM_1.2.0_macos_aarch64

usage: HEIRV32-ASM
  Assembler/Disassembler to support HEIRV32 ISA,
  See help below for usage : it auto-detects if the file is binary like (=> will
  disassemble) or contains ASM instructions (=> will assemble).
  If no switches are given, will open a GUI to select the file and run with '-t = 'phb''
  argument.

Usage:
heirv32 -f <ASMfile> [-t="phb"] [-i="HEIRV32" | "RV32I"]
heirv32 -s <string> [(-t="hb" -of <outputPathName>)] [-i="HEIRV32" | "RV32I"]
heirv32 -g [-t="phb"] [-i="HEIRV32" | "RV32I"]
heirv32 -i <ISA>
heirv32 -h | --help
heirv32 [-g -t="phb" -i="HEIRV32"]

Options:
-h --help      Show this screen.
-f             Input ASM file.
-s             Input string.
-g             Open GUI to select file to convert.
-i             ISA to use ('HEIRV32' or 'RV32I' supported), default 'HEIRV32'. Can be
used alone to log the ISA specs.

-t             Output type ('p' - print, 'h' - BRAM file, 'b' - bin File), default 'p'.
-of            Output file path whe convertin an input string ('-s'), if 'h' and/or 'b'
are used for '-t'
```



#### 4.4.1 Utilisation HEIRV32-asm

Assemblage ou désassemblage automatique en fonction des fichiers d'entrée.

##### 4.4.1.1 Ligne de commande (CLI)

**Assembleur ⇒ Binaire**

```
$HEIRV32-ASM_1.2.0_macos_aarch64 -f ./tasassembly.s -t p

Generating file with output type p

File: ./tests/tasassembly.s
Conversion ongoing
* Using the ASSEMBLER
* Found a value in code : 1500 at address 88 - do not let code try to run it !
* Found a value in code : 1 at address 92 - do not let code try to run it !
* Found a value in code : 255 at address 96 - do not let code try to run it !
** Found data / instructions: 25

----- p : Printing instructions list and write to file -----
* Output file: _syn.txt
0x0000: addi x2 x0 5      => 0b00000000'01010000'00000001'00010011 => 0x00500113
0x0004: addi x3 x0 12     => 0b00000000'11000000'00000001'10010011 => 0x00c00193
0x0008: addi x7 x3 -9     => 0b11111111'01110001'10000011'10010011 => 0xff718393
0x000c: or   x4 x7 x2     => 0b00000000'00100011'11100010'00110011 => 0x0023e233
0x0010: and  x5 x3 x4     => 0b00000000'01000001'11110010'10110011 => 0x0041f2b3
0x0014: add  x5 x5 x4     => 0b00000000'01000010'10000010'10110011 => 0x004282b3
0x0018: beq  x5 x7 end    => 0b00000010'01110010'10001000'01100011 => 0x02728863
0x001c: slt  x4 x3 x4     => 0b00000000'01000001'10100010'00110011 => 0x0041a233
0x0020: beq  x4 x0 around => 0b00000000'00000010'00000100'01100011 => 0x00020463
0x0024: addi x5 x0 0      => 0b00000000'00000000'00000010'10010011 => 0x00000293
0x0028: slt  x4 x7 x2     => 0b00000000'00100011'10100010'00110011 => 0x0023a233
0x002c: add  x7 x4 x5     => 0b00000000'01010010'00000011'10110011 => 0x005203b3
0x0030: sub  x7 x7 x2     => 0b01000000'00100011'10000011'10110011 => 0x402383b3
0x0034: sw   x7 84(x3)    => 0b00000100'01110001'10101010'00100011 => 0x0471aa23
0x0038: lw   x2 88(x0)    => 0b00000101'10000000'00100001'00000011 => 0x05802103
0x003c: add  x9 x2 x5     => 0b00000000'01010001'00000100'10110011 => 0x005104b3
0x0040: jal  x3 end       => 0b00000000'10000000'00000001'11101111 => 0x008001ef
0x0044: addi x2 x0 1      => 0b00000000'00010000'00000001'00010011 => 0x00100113
0x0048: add  x2 x2 x9     => 0b00000000'10010001'00000001'00110011 => 0x00910133
0x004c: sw   x2 0x20(x3)  => 0b00000010'00100001'10100000'00100011 => 0x0221a023
0x0050: beq  x2 x2 main   => 0b11111010'00100001'00001000'11100011 => 0xfa2108e3
0x0054: jal  x3 main     => 0b11111010'11011111'11110001'11101111 => 0xfadff1ef
0x0058: 1500             => 0b00000000'00000000'00000101'11011100 => 0x000005dc
0x005c: 0b1              => 0b00000000'00000000'00000000'00000001 => 0x00000001
0x0060: 0xff             => 0b00000000'00000000'00000000'11111111 => 0x000000ff
```

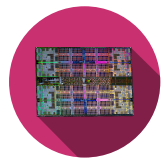
**Binaire ⇒ Assembleur**

```
$HEIRV32-ASM_1.2.0_macos_aarch64 -f ./tasassembly.txt -t p

Generating file with output type p

File: ./tests/tasassembly.txt
Conversion ongoing
* Using the DISASSEMBLER
```

HEI-Vs / ZaS, AmA / 2024 / v1.2



#### 4.4.1.2 Avec l'interface graphique (GUI)

Pour cela, il suffit d'exécuter le fichier et de suivre les 3 étapes suivantes dans l'interface :

1. Choix du processeur
  - **RV32I** - Processeur RISC-V complet
  - **HEIRV32** - Processeur du projet à la fin du semestre.
3. Appuyer sur le bouton **Next**.
2. Choix du fichier d'entrée - soit **\*.s**, **\*.asm** ou **\*.bin**.

Ensuite, vous trouverez la sortie dans le même dossier et dans le terminal la sortie du programme.

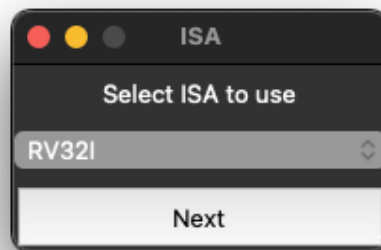


Fig. 7. – GUI du programme HEIRV32-ASM

```
base ~/work/repo/edu/car/labo/car-labs-stud/isa/heirv32-asm git:(main)±4
./HEIRV32-ASM_1.2.0_macos_aarch64

Converting file: /Users/zas/work/repo/edu/car/labo/car-labs-stud/isa/ex4.3_helperFunctions.asm
Cleaning up code
** Cleanup done
Conversion ongoing
* Using the ASSEMBLER with ISA RV32I
** Big li found -> ['li', 'x30', '0xf0000004'] - converting ...
*** Modifying existing code: lui x30, 983040
*** Inserting new code: addi x30, x30, 4
** Big li found -> ['li', 'x31', '0xf0000000'] - converting ...
*** Modifying existing code: lui x31, 983040
*** Inserting new code: addi x31, x31, 0
** Checking li with values: ['li', 't0', '8']
*** Not adding extra instr
** Checking li with values: ['li', 't2', '0x00ffffff']
*** Is an extra instr
** beq x0, t0, leds_end
*** Front jump of 48 (0x30) to label leds_end with i = 30, instr_num = 16, lbls_between = 3
** Checking li with values: ['li', 't0', '8']
*** Not adding extra instr
** Checking li with values: ['li', 't2', '0x00ffffff']
*** Is an extra instr
** beq t1, x0, isoff
*** Front jump of 16 (0x10) to label isoff with i = 22, instr_num = 18, lbls_between = 1
** Big li found -> ['li', 't2', '0x00ffffff'] - converting ...
*** Modifying existing code: lui x7, 4096
*** Inserting new code: addi x7, x7, 4095
** Checking li with values: ['li', 't0', '8']
*** Not adding extra instr
** j leds_loop_end
*** Front jump of 8 (0x8) to label leds_loop_end with i = 25, instr_num = 22, lbls_between = 1
** Checking li with values: ['li', 't0', '8']
*** Not adding extra instr

* Found data / instructions: 24
```

Fig. 8. – Sortie du programme heirv32-asm





#### 4.4.2 Analyse 3: Assembly & Disassembly

1. Enregistrez le code suivant sous un fichier **.s** ou **.asm** :

```
myLabel:
    li    x20 0b1111111111
    add   x20 x20 x20
    add   x20 x20 x20
    add   x20 x20 x20
    addi  x3 x0 0
begin:
    mv    x1 x0
a:
    slt   x2 x1 x20
    beq   x2 x0 subing
    addi  x1 x1 1
    beq   x0 x0 a
subing:
    addi  x3 x3 -1
    beq   x3 x0 test
label_wo_beq:
    addi  x30 x0 0xCC
    jal   ra begin
test:
    addi  x30 x0 0b00110011
    jal   begin
l6: # This is very important
# But won't always save you
    jal   ra myLabel
```

2. Compilez-le à l'aide de HEIRV32-ASM avec les sorties **print** et **bin** activées :

```
./dist/HEIRV32-ASM_1.1.3_xxx -i RV32I -f ./my/file/disassembly-01.s -t pb
```

Un fichier **.txt** est créé, qui est une version hexadécimale lisible par les humains du fichier **.bin** généré.

3. Maintenant, décompilez-le fichier **.txt** de la même manière pour recréer un fichier assembleur :

```
./dist/HEIRV32-ASM_1.1.3_xxx -i RV32I -f ./my/file/assembled-01.txt -t pb
```

Cela devrait créer un fichier **\_disassembly.s**.

4. Qu'est-ce qui change entre les deux codes ? Donnez au moins 3 points.
5. A quoi peut servir l'instruction **jal ra myLabel** dans ce contexte ?



## 4.5 Reverse Engineering

Vous travaillez sur un projet en binôme sur un processeur RISC-V quelque peu modifié.

En effet, pour se simplifier la vie et communiquer avec le monde extérieur, ce dernier peut lire l'état de 4 boutons reliés au processeur en lisant l'adresse mémoire **0xf0000000**, et allumer 8 leds en écrivant aux adresses mémoire **0xf0000004** (led 0) à **0xf0000020** (led 7):

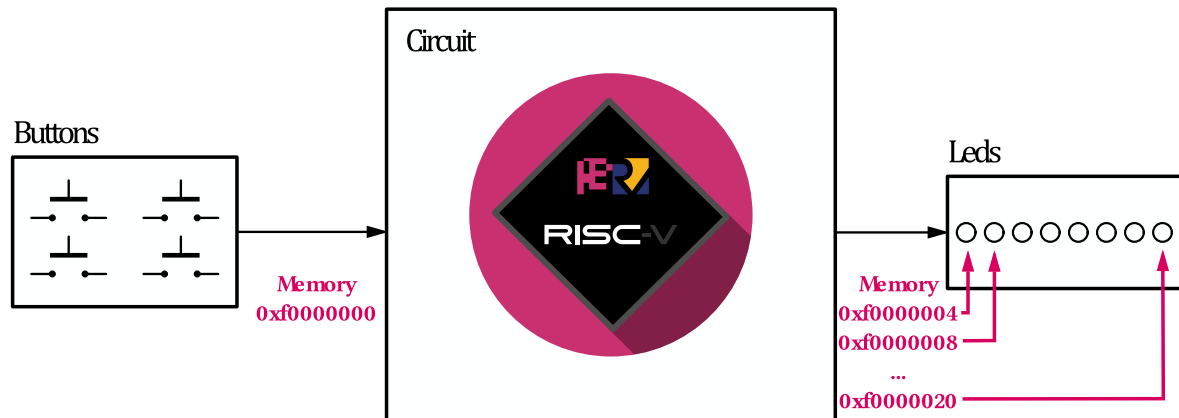


Fig. 9. – Processeur RISC-V modifié

Le premier laboratoire consistait à faire clignoter les leds selon les boutons appuyés:

- Aucun bouton: les 8 leds sont allumées selon le pattern 0xAA
- Le bouton 0 est à < 1 >: les 8 leds clignotent à une fréquence raisonnable (le clignotement est visible)

Pour simplifier l'accès au bouton et aux leds, le code suivant vous était donné:



```
setup:
    # led is sw xx, offBy4(x30) with xx loaded as 0x00rrggbb
    li x30, 0xf0000004 # base address for leds
    li x31, 0xf0000000 # base address for buttons, one register

    # DO NOT MODIFY x30 (t5) and X31 (t6) !!!
    # MUST BE THE FIRST THING IN YOUR PROGRAM, BEFORE MAIN

get_btns: # return buttons value in a0
    lw a0, 0(x31)
    jr ra

set_leds: # pass a 8 bits which if bit(n) = '1', led(n) is on
    li t0, 8 # loop the leds
    mv t3, x30 # mem position
    addi t3, t3, 28 # leds display is reversed, so stock reverted

    leds_loop:
        beq x0, t0, leds_end
        andi t1, a0, 1
        # if 1, lights corresponding led
        beq t1, x0, isoff

    ison:
        li t2, 0x00ff00ff
        j leds_loop_end

    isoff:
        mv t2, x0

    leds_loop_end:
        sw t2, 0(t3) # save led value
        srli a0, a0, 1 # shift right leds value
        addi t0, t0, -1 # decrement loop
        addi t3, t3, -4 # add memory pos
        j leds_loop

    leds_end:
        jr ra
```

Malheureusement, votre collègue est absent aujourd'hui et ne vous a pas laissé une copie du code déjà écrit (*pensez à apprendre [Git](#) !*). En plus, il y'avait quelques bugs:

- Aucun bouton: les leds s'allument selon le pattern 0x2A
- Le bouton 0 est à < 1 >: seules 7 leds clignotent, et à une fréquence qui semble bien trop élevée
- Un des autres bouton est appuyé: même comportement que si le bouton 0 était appuyé

*Un problème matériel peut être exclu.*

Vous vous souvenez que le dernier code écrit avait été flashé sur votre board RISC-V et, vu que le chip n'avait pas été protégé contre la relecture, vous arrivez à l'extraire par accès au bus JTAG, ce qui vous a donné:



```
f0000f37
004f0f13
f0000fb7
000f8f93
00000413
040000ef
02a00463
00900663
fff48493
ff1ff06f
06400493
00800663
00000413
0140006f
0bf00413
00c0006f
02a00413
00000493
00040513
010000ef
fc5ff06f
000fa503
00008067
00800293
000f0e13
01ce0e13
02500863
00157313
00030863
010003b7
fff38393
0080006f
00000393
007e2023
00155513
fff28293
ffce0e13
fd5ff06f
00008067
```

1. Décompilez votre code
2. Identifiez et séparez le code donné du reste
3. Comprenez l'utilisation des fonctions données



Pour simuler le système, sous Ripes, ouvrez l'onglet I/O:

- Double-cliquez sur Switches, sélectionnez le widget créé et configurez-le tel que:

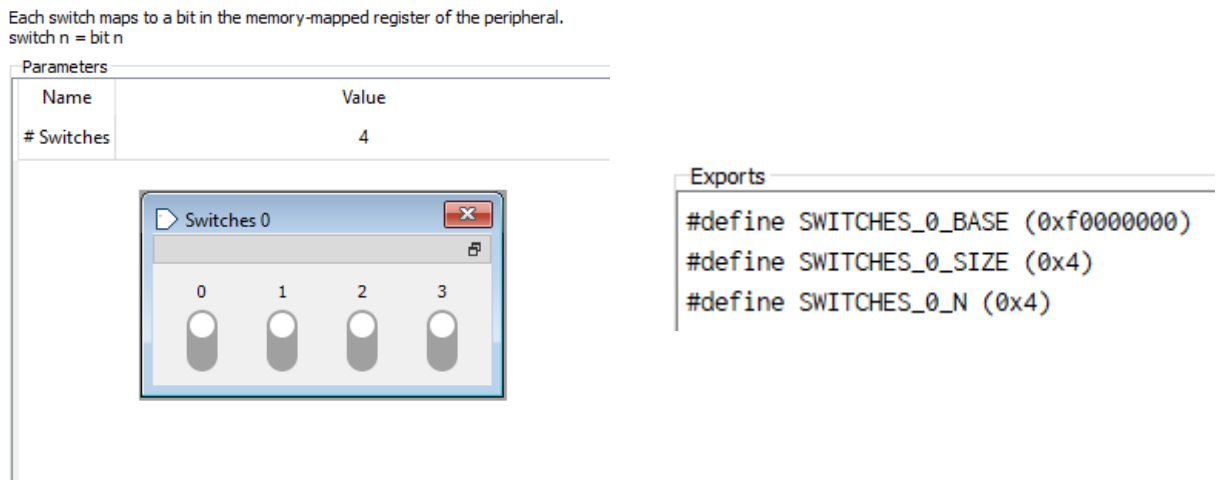


Fig. 10. – Ripes - configuration des interrupteurs

Contrôlez que **Exports** contienne les mêmes informations que sur l'image donnée après réglage du module.

- Double-cliquez sur LED Matrix, sélectionnez le widget créé et configurez-le tel que:

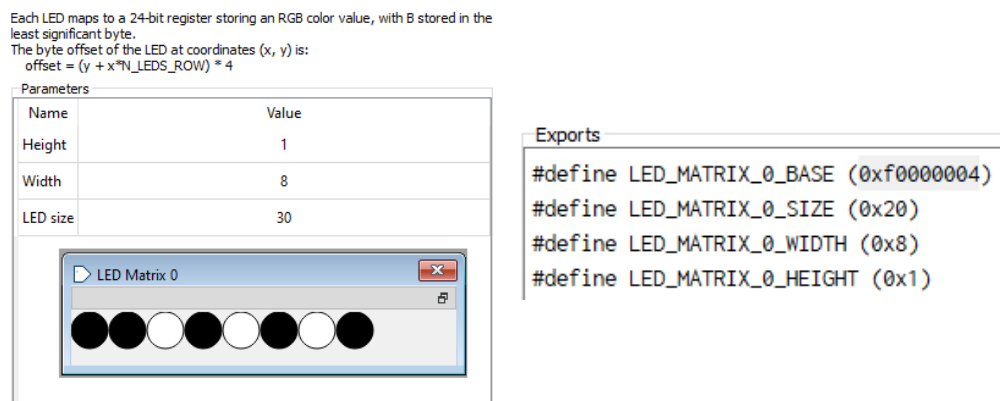


Fig. 11. – Ripes - configuration des leds

Contrôlez que **Exports** contienne les mêmes informations que sur l'image donnée après réglage du module.



Ajoutez d'abord les switches puis les leds pour obtenir la bonne adresse de base des modules.



1. Chargez votre code assembleur décompilé dans **Editor**
2. Appuyez sur F8 (ou l'icône >>) et constatez que le circuit fonctionne selon les problèmes énoncés en interagissant sous **I/O** avec les interrupteurs.
3. Fixez les problèmes cités (4 problèmes)
4. Testez votre circuit sur Ripes

*La clock ne pouvant être réglée de manière précise, la fréquence de clignotement des leds se fait sans calcul. Corriger le code pour obtenir environ 2 Hz.*



Ce que vous venez d'accomplir s'apparente à du hardware hacking : un code est dumpé (copié), analysé, modifié, puis réinjecté dans un système pour l'adapter à son envie. Bien sûr, il n'est pas toujours si simple de copier et réinjecter un code. Des méthodes parfois exotiques ont vu le jour (voir le [Kamikaze Hack de la Xbox 360](#)).



# Bibliographie