Accelerator hardware de criptare și decriptare implementat pe FPGA.

Absolvent:
Tudusciuc Cristian-Rafael

Coordonator științific: ș.l. dr.ing. Monor Mircea-Călin

Cuprins

1 Domeniul și tema propusă

2 Proiectarea aplicției

3 Implementarea aplicației

4 Rezultate experimentale

5 Concluzii

1 Domeniul și tema propusă

Domeniul și tema propusă

Tema propusa: Dezvoltarea și implementarea unui dispozitiv pe FPGA pentru criptare și decriptare, superior soluțiilor software in cadrul aplicațiilor embedded.

Domeniul:

Proiectare digitală
(digital design)

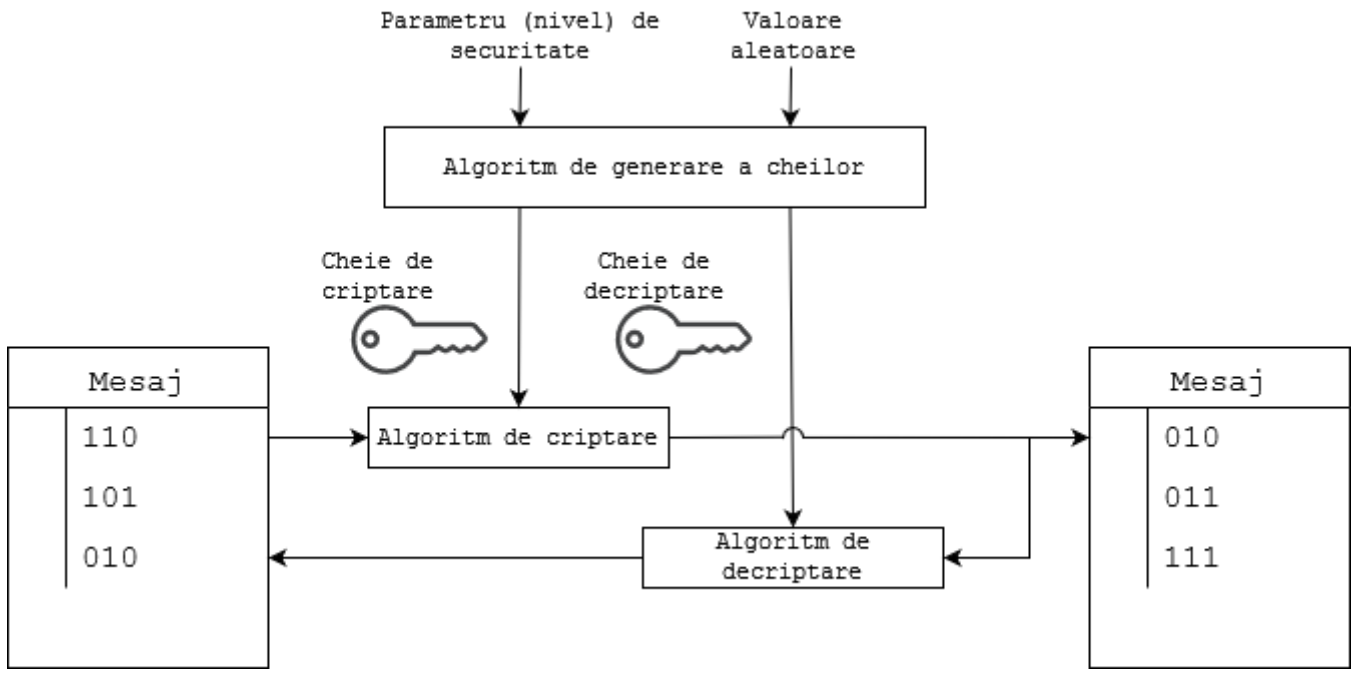
Mediu de verificare
(design verification)

Criptografie
light-weight

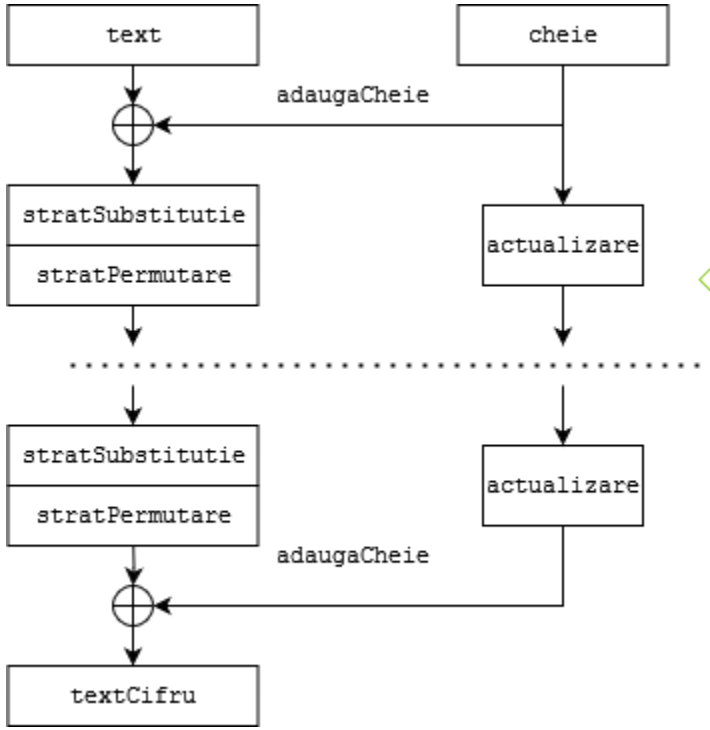
2 Proiectarea aplicției

Proiectarea aplicției

Arhitectura sistemului criptografic

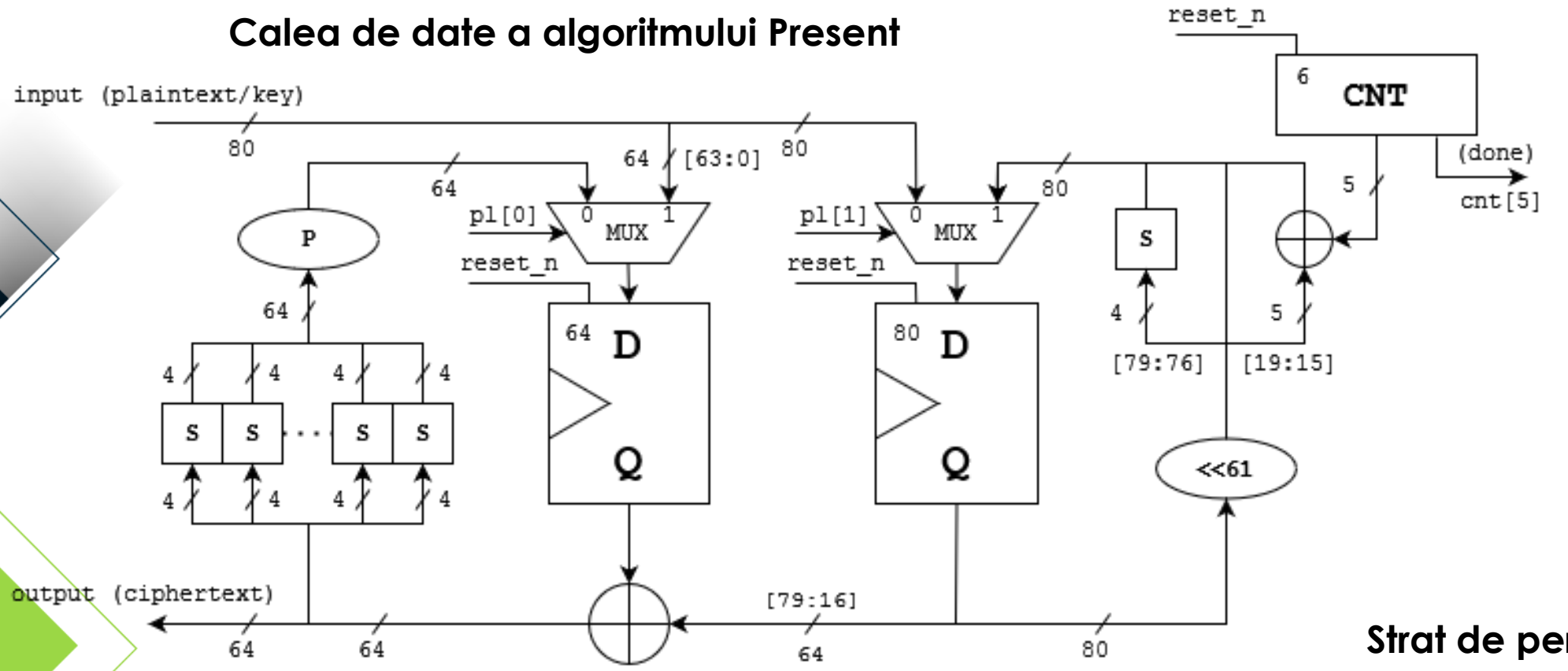


Descrierea algoritmului Present



Proiectarea aplicției

Calea de date a algoritmului Present



Funcția de substituție

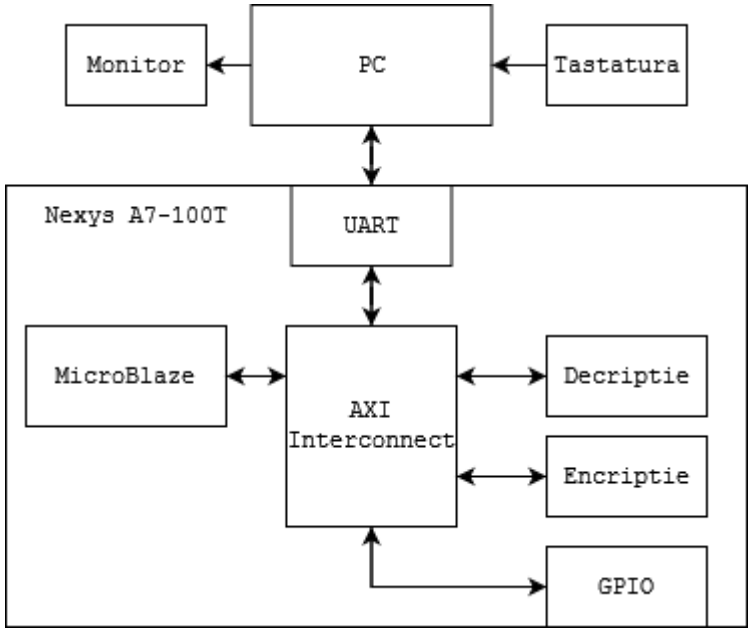
x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Strat de permutare

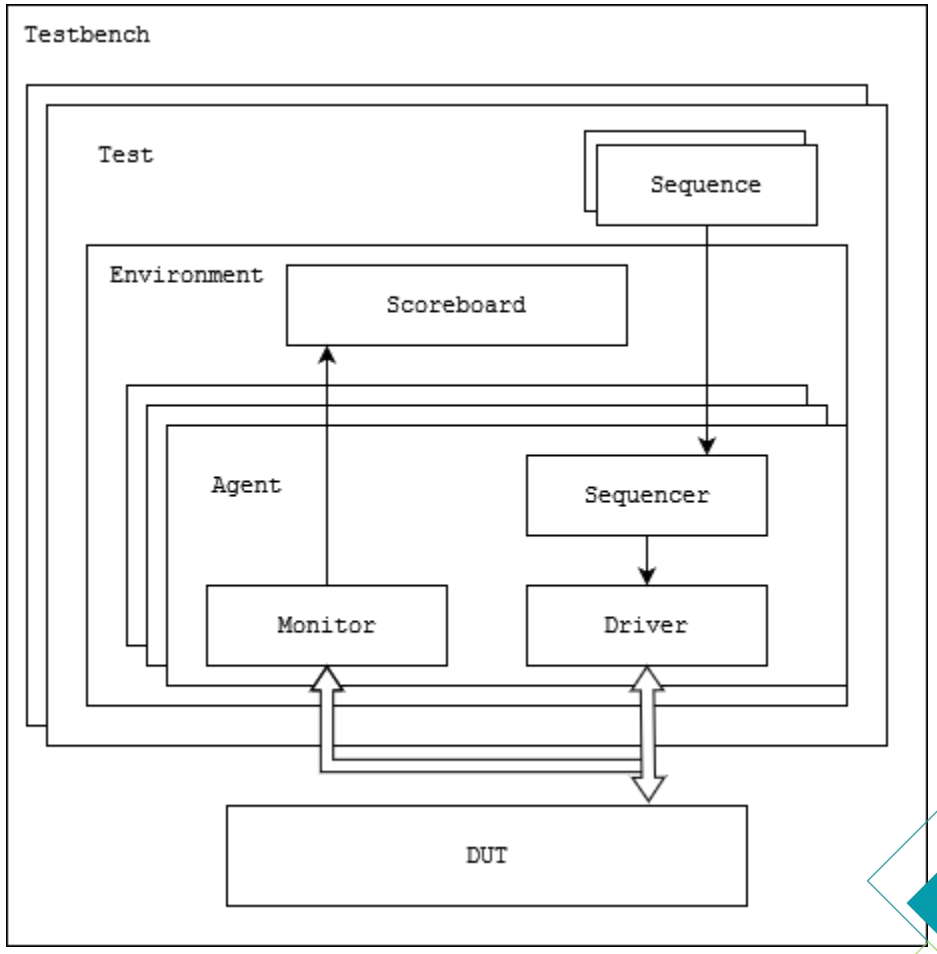
i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Proiectarea aplicției

Arhitectura înregului ansamblu



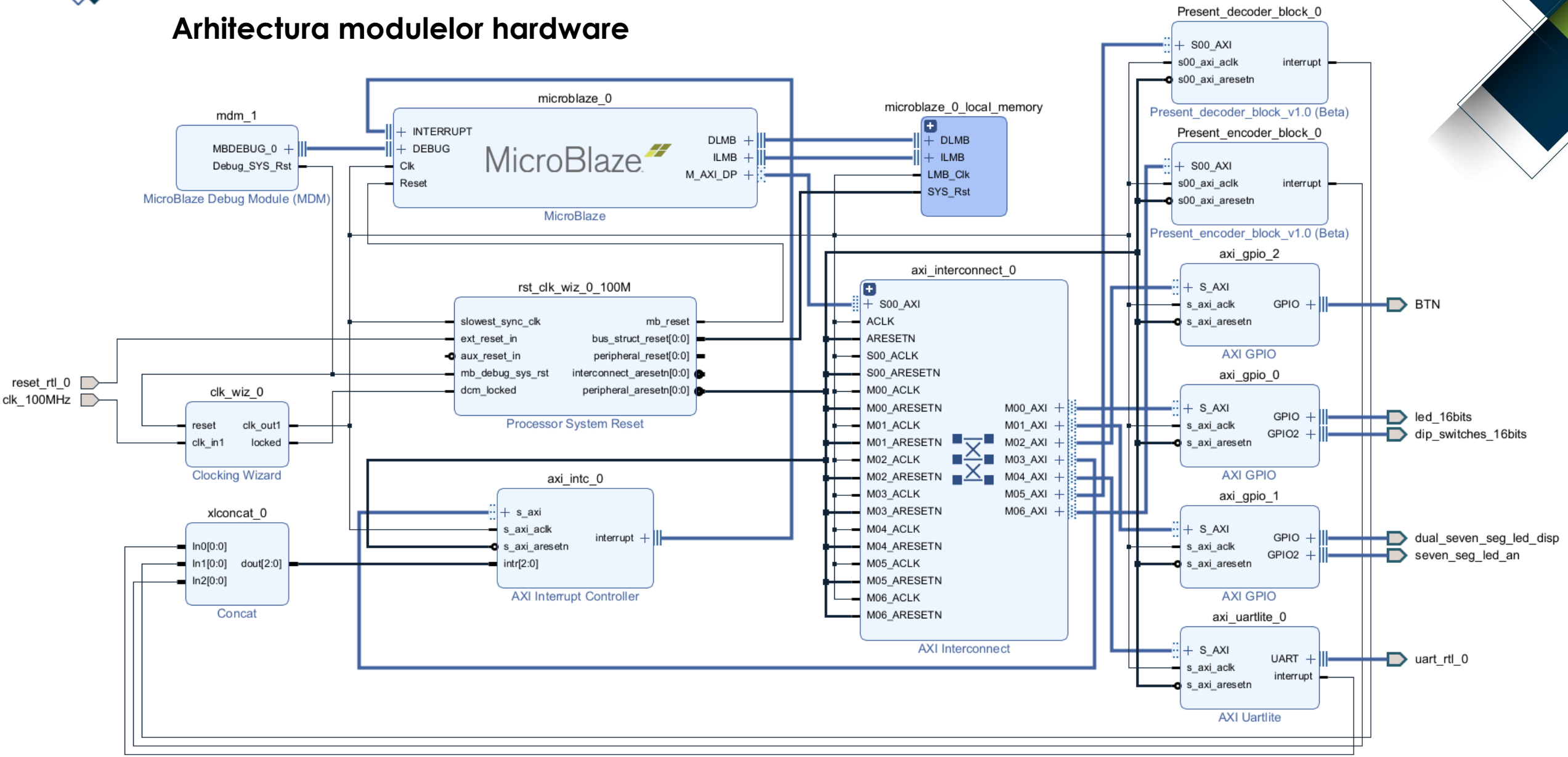
Arhitectura mediului de verificare prin UVM
a modulelor de criptare/decriptare



3 Implementarea aplicției

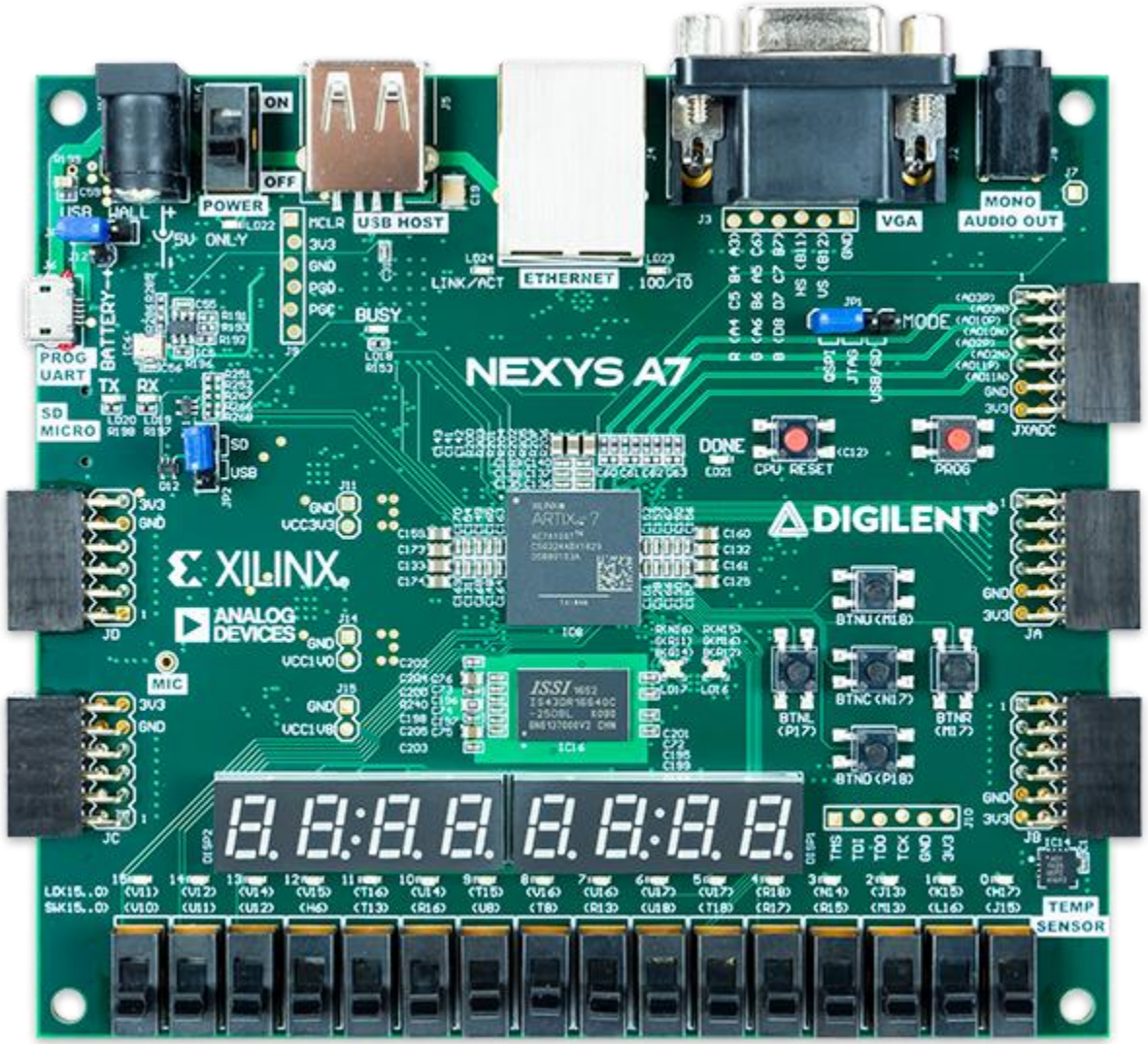
Implementarea aplicției

Arhitectura modulelor hardware

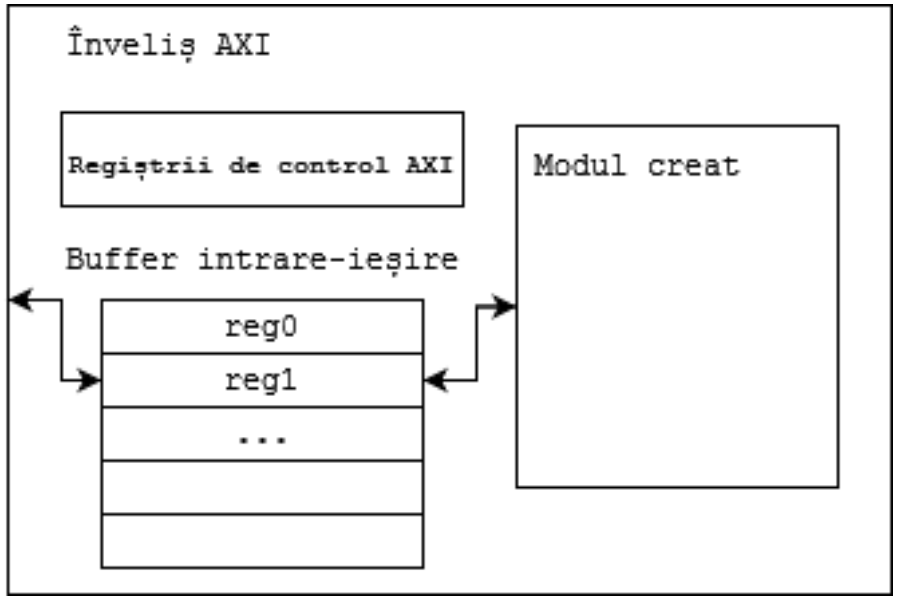


Implementarea aplicției

Platforma hardware folosită

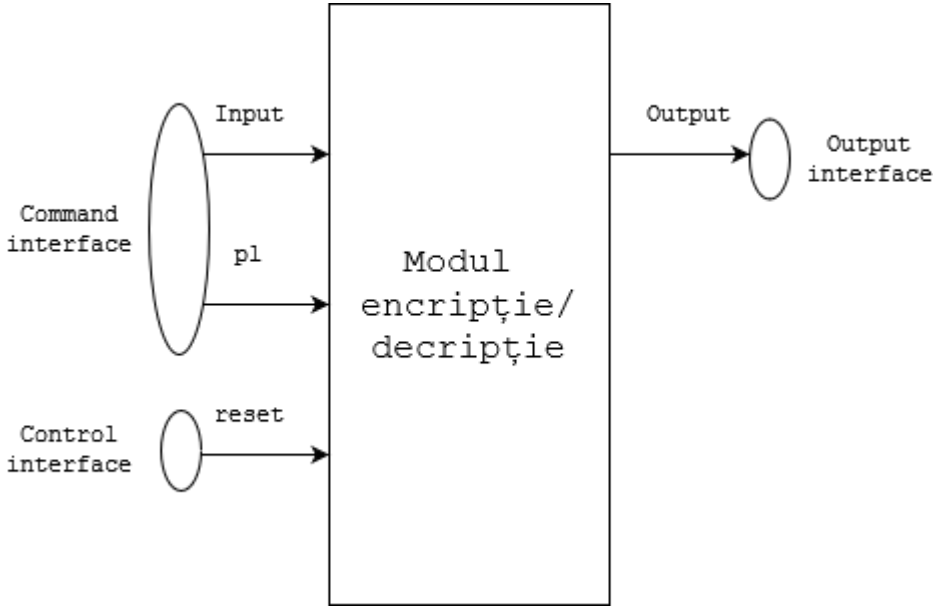


Împachetare AXI

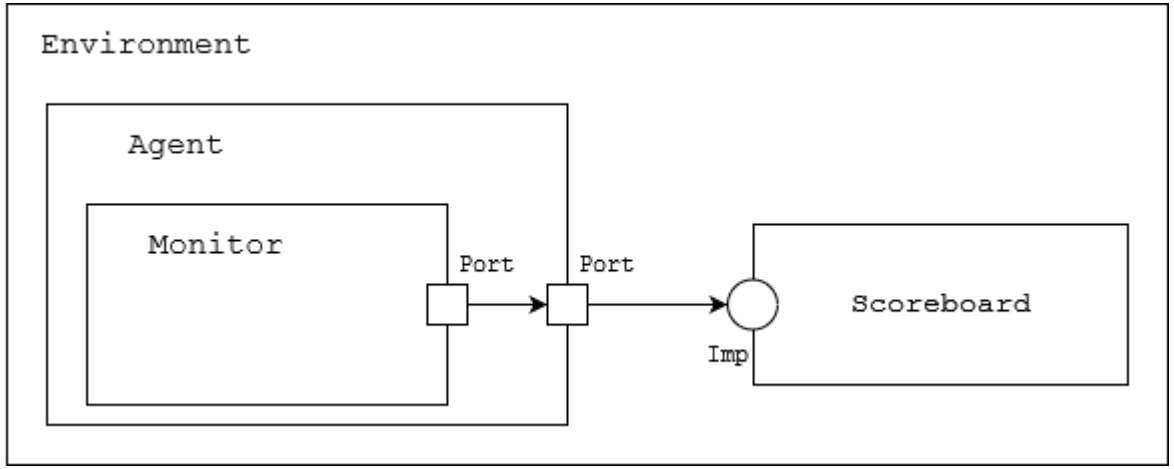


Implementarea aplicției

Împărțirea pe interfețe

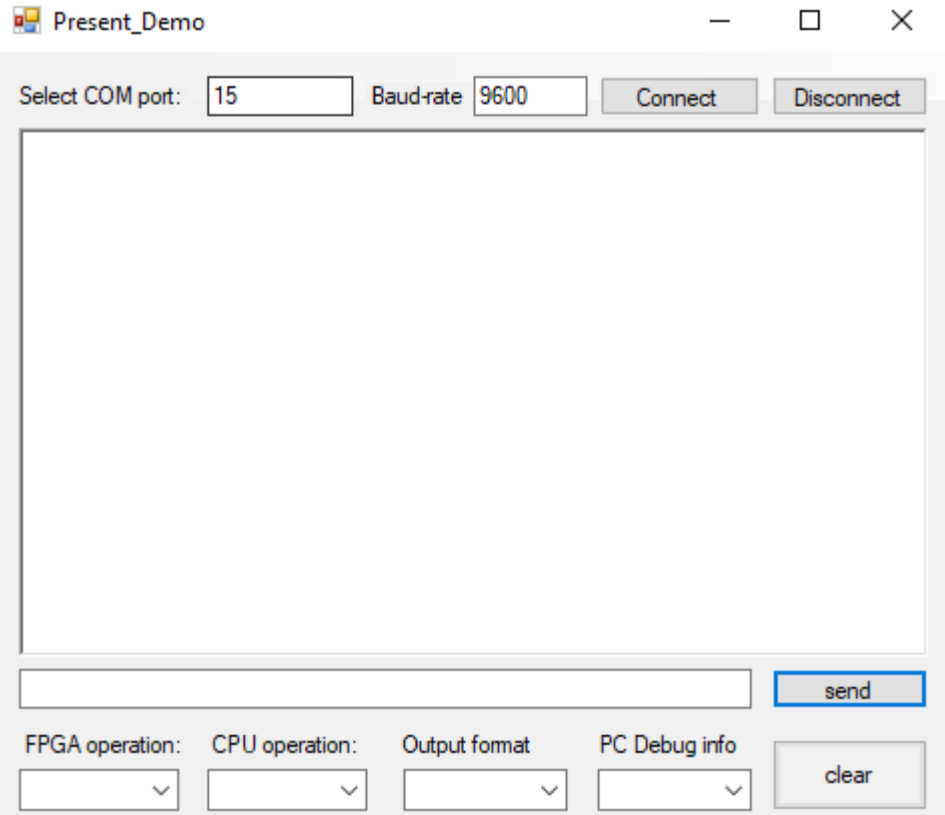


Comunicare Monitor-Scoreboard



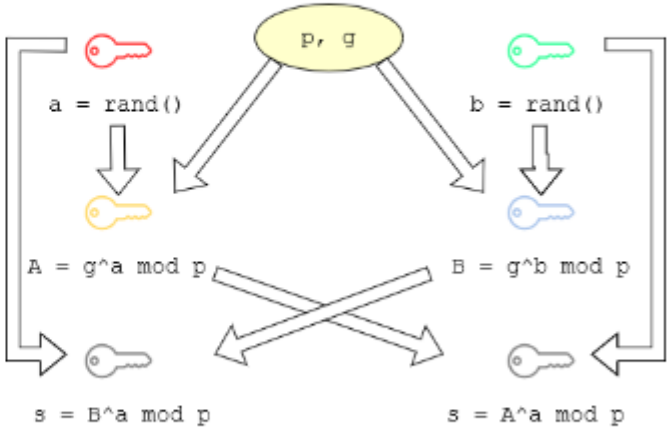
Implementarea aplicției

Interfața grafică



Funcție pentru stabilirea cheii

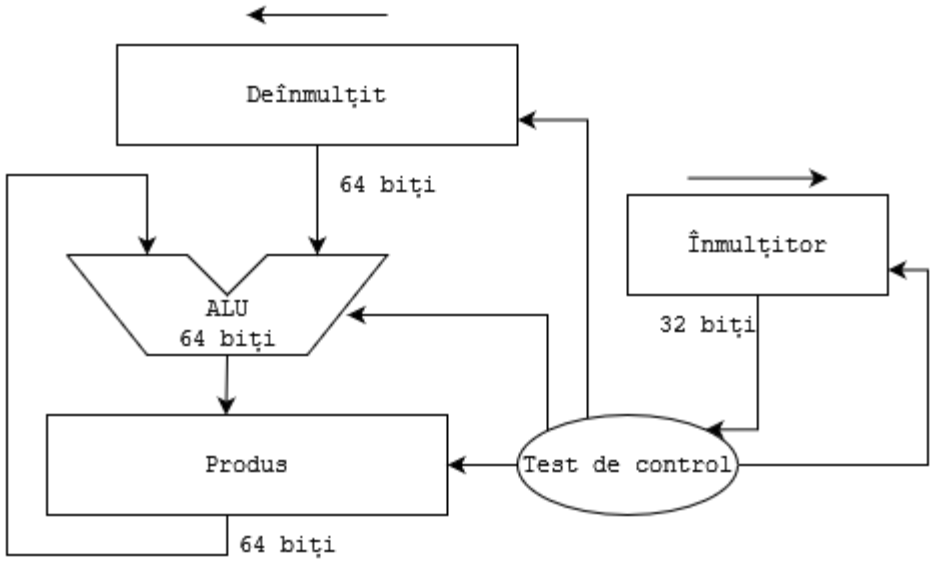
```c
void key_agreement(){
    uint8_t size = word_80 * 2;
    uint32_t a[size];
    set_rand(a, size);
    uint32_t g[size];
    uint32_t p[size];
    set_zero(g, size);
    set_zero(p, size);
    g[0] = 2;
    p[2] = 0x10000;
    p[0] = 0xd;

    pow_mod(g, a, p, size);
    send_hex(g,"A", size/2);

    recive_B(g, size/2);
    pow_mod(g, a, p, size);

    set_key(g);
}
```



Implementarea aplicției

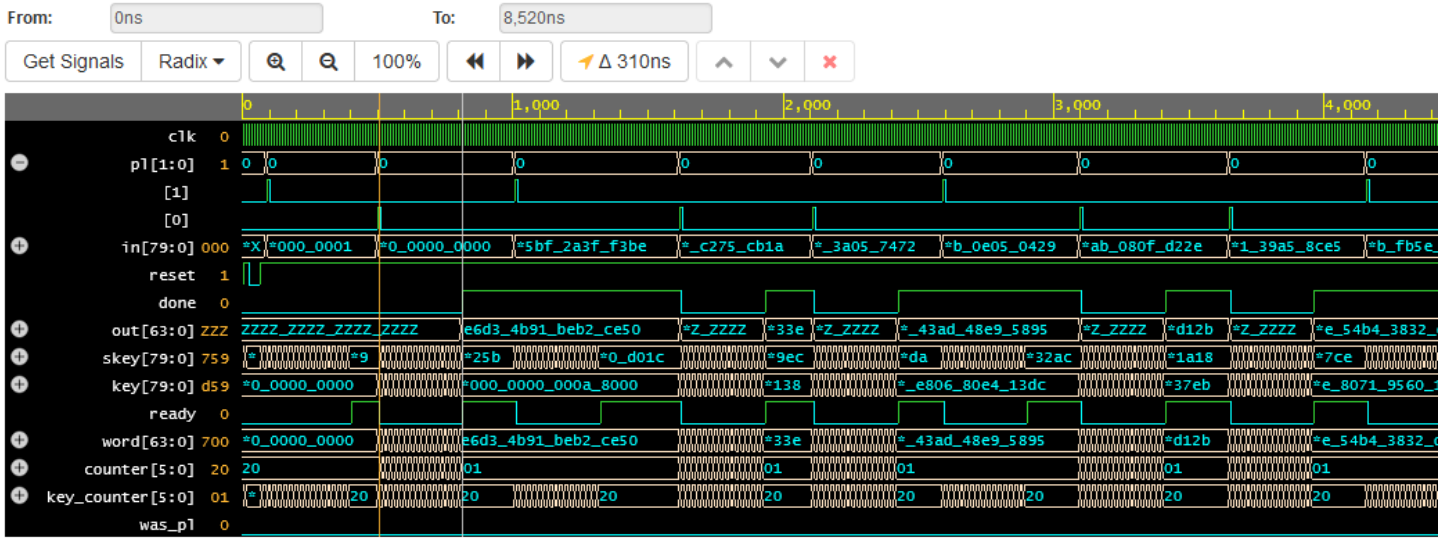
Modul de operare cu numere mari

```
1   void multiply(uint32_t* a, uint32_t* b, uint8_t size) {
2       uint32_t* ml = (uint32_t*)malloc(size * sizeof(uint32_t));
3       uint32_t* mr = (uint32_t*)malloc(size * sizeof(uint32_t));
4       cpy(ml, a, size);
5       cpy(mr, b, size);
6       set_zero(a, size);
7       while (!is_zero(mr, size)) {
8           // print(mr, "mr");
9           if (mr[0] & 1) { addition(a, ml, size); }
10          shift_left(ml, size);
11          shift_right(mr, size);
12      }
13      free(ml);
14      free(mr);
15  }
```

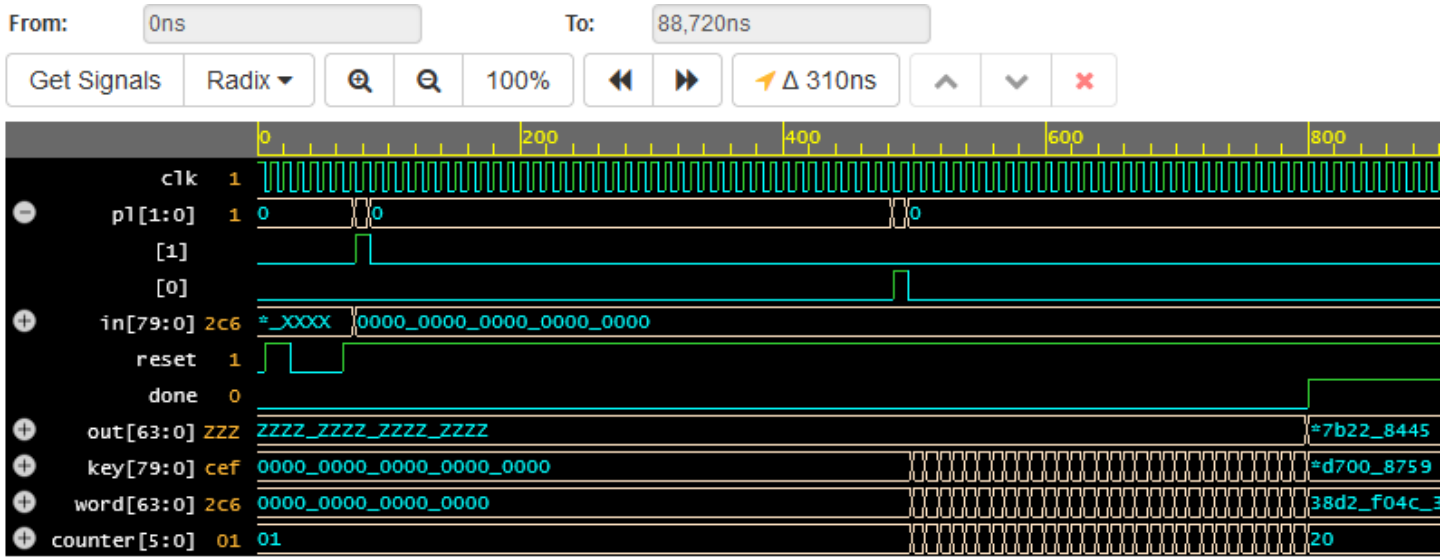


4 Rezultate experimentale

Rezultate experimentale



Verificarea modulului de decriptare



Verificarea modulului de criptare

Rezultate experimentale

Rezultatele testelor pentru decriptare

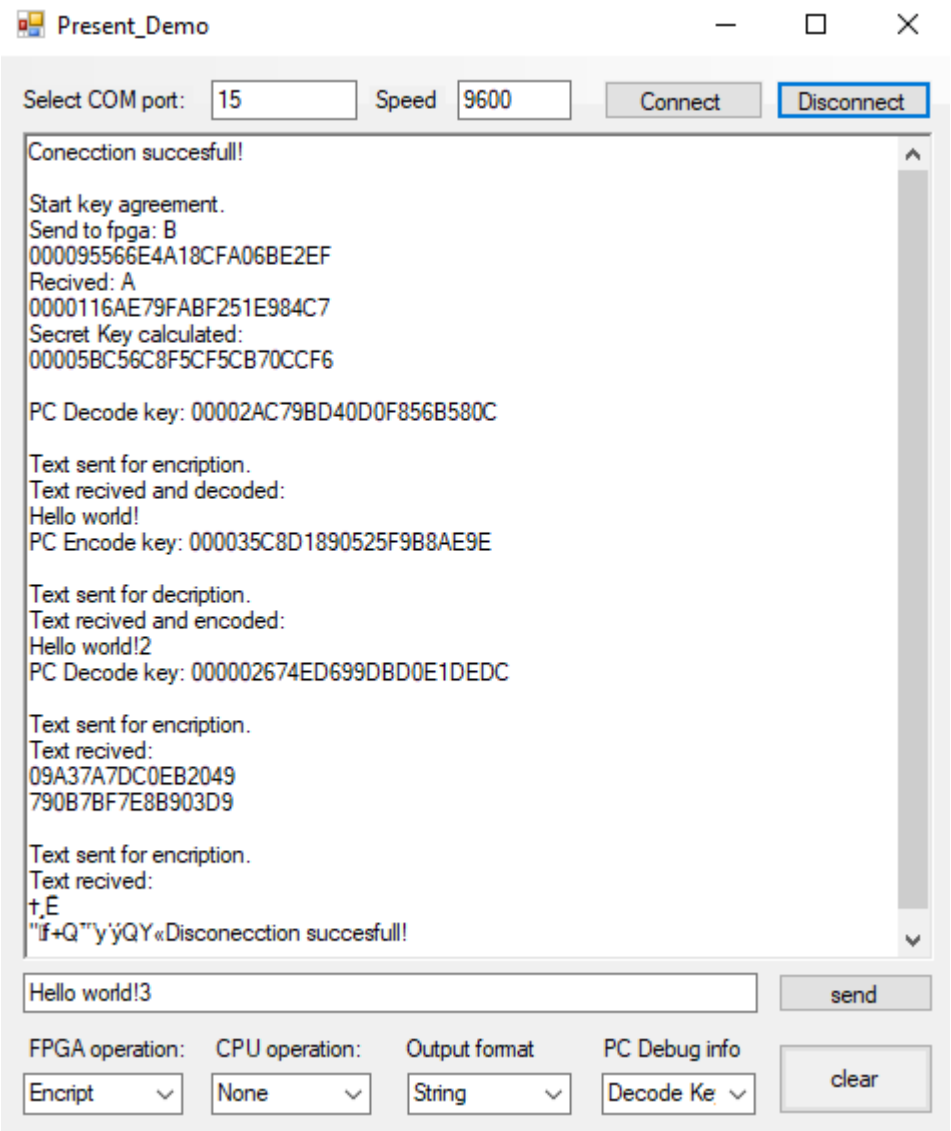
```
UVM_INFO test_lib.sv(46) @ 46720: uvm_test_top [simple_test] ** UVM TEST PASSED **
UVM_INFO /apps/vcsmx/vcs/U-2023.03-SP2//etc/uvm-1.2/src/base/uvm_report_server.svh(904) @ 46720: reporter [UVM/REPORT/SERVER]
--- UVM Report Summary ---

** Report counts by severity
UVM_INFO :  556
UVM_WARNING :    0
UVM_ERROR :    0
UVM_FATAL :    0
** Report counts by id
[RNTST]     1
[UVM/RELNOTES]     1
[scoreboard]   274
[simple_test]     2
[start_phase]     3
[uvm_test_top.env0.cmd_agt.monitor]   212
[uvm_test_top.env0.ctrl_agt.monitor]     2
[uvm_test_top.env0.out_agt.monitor]    61

$finish called from file "/apps/vcsmx/vcs/U-2023.03-SP2//etc/uvm-1.2/src/base/uvm_root.svh", line 527.
$finish at simulation time                46720
          V C S   S i m u l a t i o n   R e p o r t
Time: 46720 ns
CPU Time:      1.040 seconds;       Data structure size:   0.4Mb
```

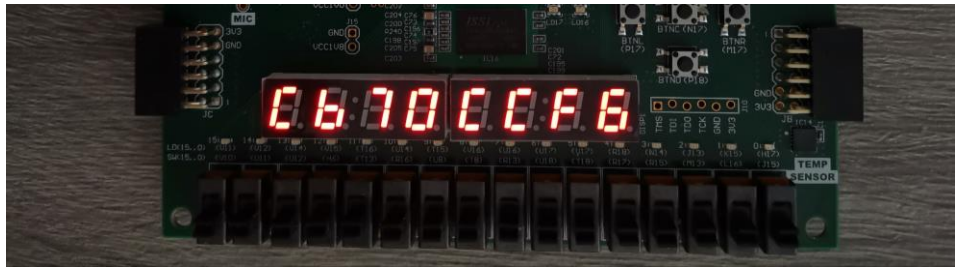
Rezultate experimentale

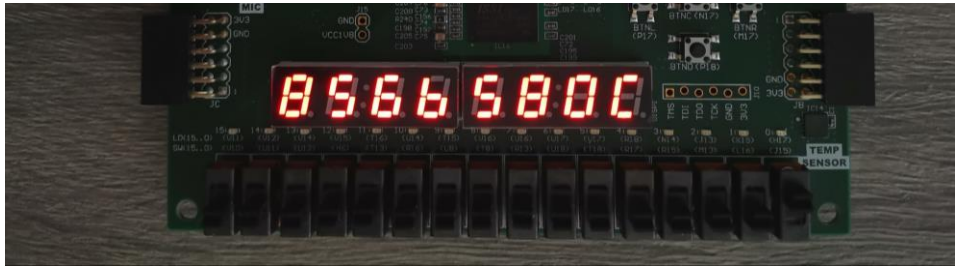
Rezultatele testelor pentru criptare

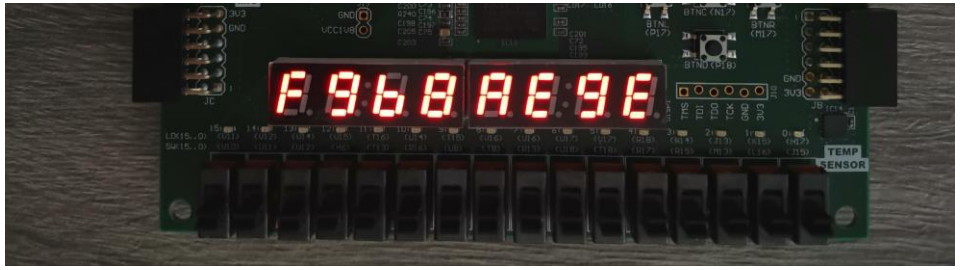
```
UVM_INFO test_lib.sv(46) @ 46720: uvm_test_top [simple_test] ** UVM TEST PASSED **
UVM_INFO /apps/vcsmx/vcs/U-2023.03-SP2//etc/uvm-1.2/src/base/uvm_report_server.svh(904) @ 46720: reporter [UVM/REPORT/SERVER]
--- UVM Report Summary ---

** Report counts by severity
UVM_INFO :  584
UVM_WARNING :    0
UVM_ERROR :    0
UVM_FATAL :    0
** Report counts by id
[RNTST]     1
[UVM/RELNOTES]     1
[scoreboard]   274
[simple_test]     2
[start_phase]     3
[uvm_test_top.env0.cmd_agt.monitor]   212
[uvm_test_top.env0.ctrl_agt.monitor]     2
[uvm_test_top.env0.out_agt.monitor]    89

$finish called from file "/apps/vcsmx/vcs/U-2023.03-SP2//etc/uvm-1.2/src/base/uvm_root.svh", line 527.
$finish at simulation time                46720
          V C S   S i m u l a t i o n   R e p o r t
Time: 46720 ns
CPU Time:      1.080 seconds;       Data structure size:   0.4Mb
```

Rezultate experimentale









5 Concluzii

Concluzii

În concluzie, acest proiect demonstrează posibilitatea realizării unei arhitecturi hardware modulare capabile să efectueze operațiuni de criptare și decriptare, asigurând totodată funcționalitatea corectă prin intermediul unui mediu de verificare dedicat.

MULȚUMESC