The SOF file named “rc4.sof” is located in directory “*/rtl/output_files/rc4.sof”

State of the Lab: working functionalities include:

TOP LEVEL:

“/*rtl/ksa.sv”

Original written in VHDL, was translated to system Verilog. Additionally, all the other modules are written in system Verilog.

Algorithm part 1, Initialize memory S:

“*/rtl/mem_init.sv”

The memory is filled with content from 0 to 255. The writing to memory process requires a clock cycle of waiting after “write_enable” is set to on. The instantiation to memory S is included in the ksa.sv.

Algorithm part 2, swapping memory content:

“*/rtl/swap.sv”

This uses a state machine that first reads and stores the value of “S[i]”, then updates value of “j” according to secret key and reads & stores the value of S[j], and lastly swap them by writing them to the memory. Note that the reading from memory process also requires a clock cycle wait time.

Algorithm part 3, decryption:

“*/rtl/loop3.sv”

This state machine is very similar to the previous one (swapping) with additional interaction with the “check result” module. At the same time, it is more complicated than the swapping state machine since it has to interact with memory S, ROM, and the result memory K, this is implemented by the use of flags which indicate the mem/rom that the decryption module is working with (namely “rom_flag”, “s_flag”, and “k_falg”).

Check result:

“*/rtl/check_result.sv”

This state machine checks the decrypted byte every time when it is written to the memory K. If the decrypted byte is not a lower case character or spacebar, the state machine will tell module “mem_init”, “swap”, and “loop3” to restart, and ask “key_gen” to generate a new key to try. If all the bytes written to the memory K pass the check, then the state machine will see this as “secret key found” and light up LED[0].

Key generation:

“*/rtl/key_gen.sv”

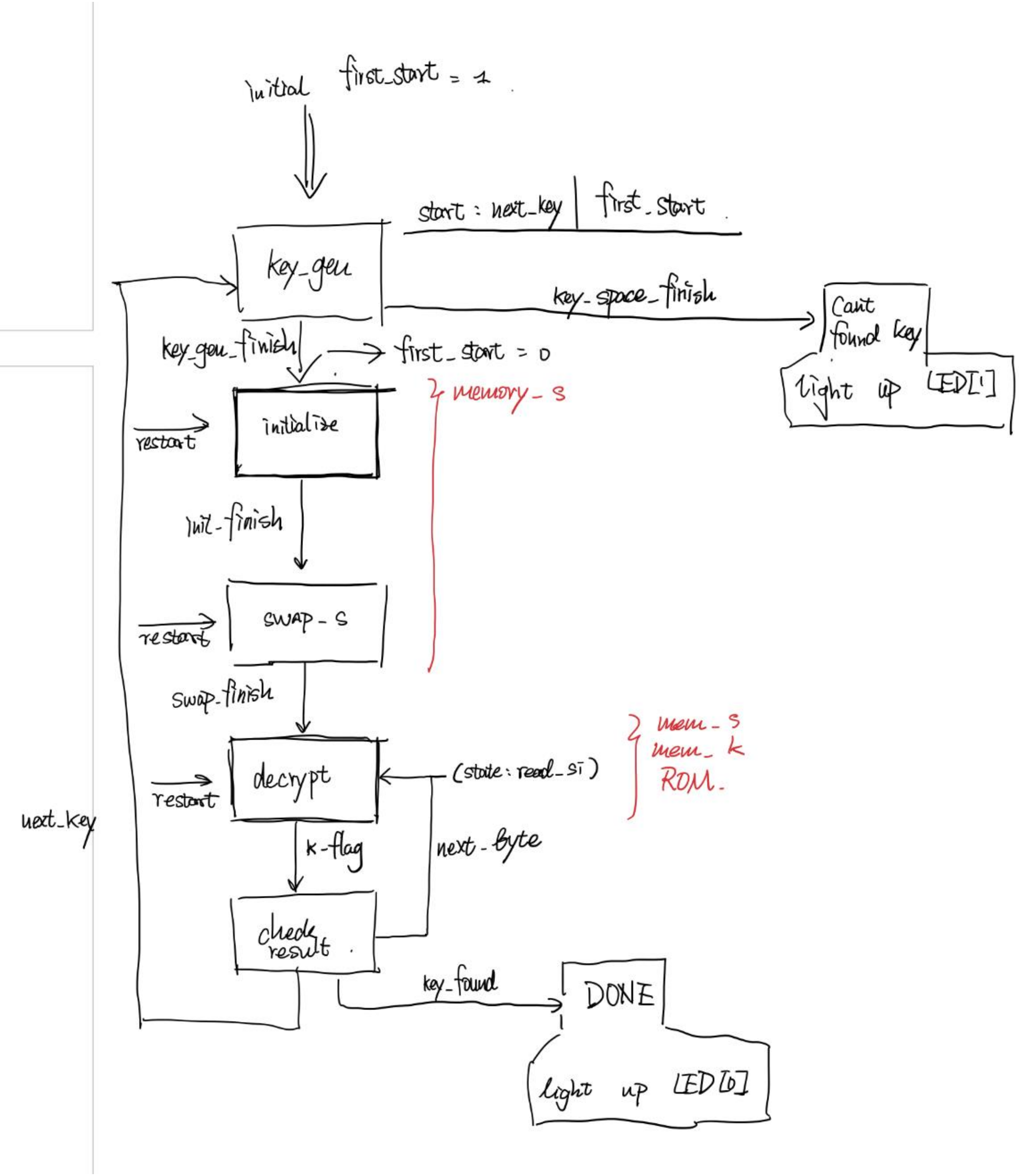
This state machine generates new key when the “check result” module ask. Besides, it generates key “24’b0” the first time the system starts without prompt from the “check result” module. If the counter in the module exceeds 22’h3FFFFF (the initial 2 bits of key are zero), in another word, when the state machine finish searching the key space, it would regard the secret key is not found and light up LED[1].

NOTE that the multi-core hasn’t been completed.

Simulations:

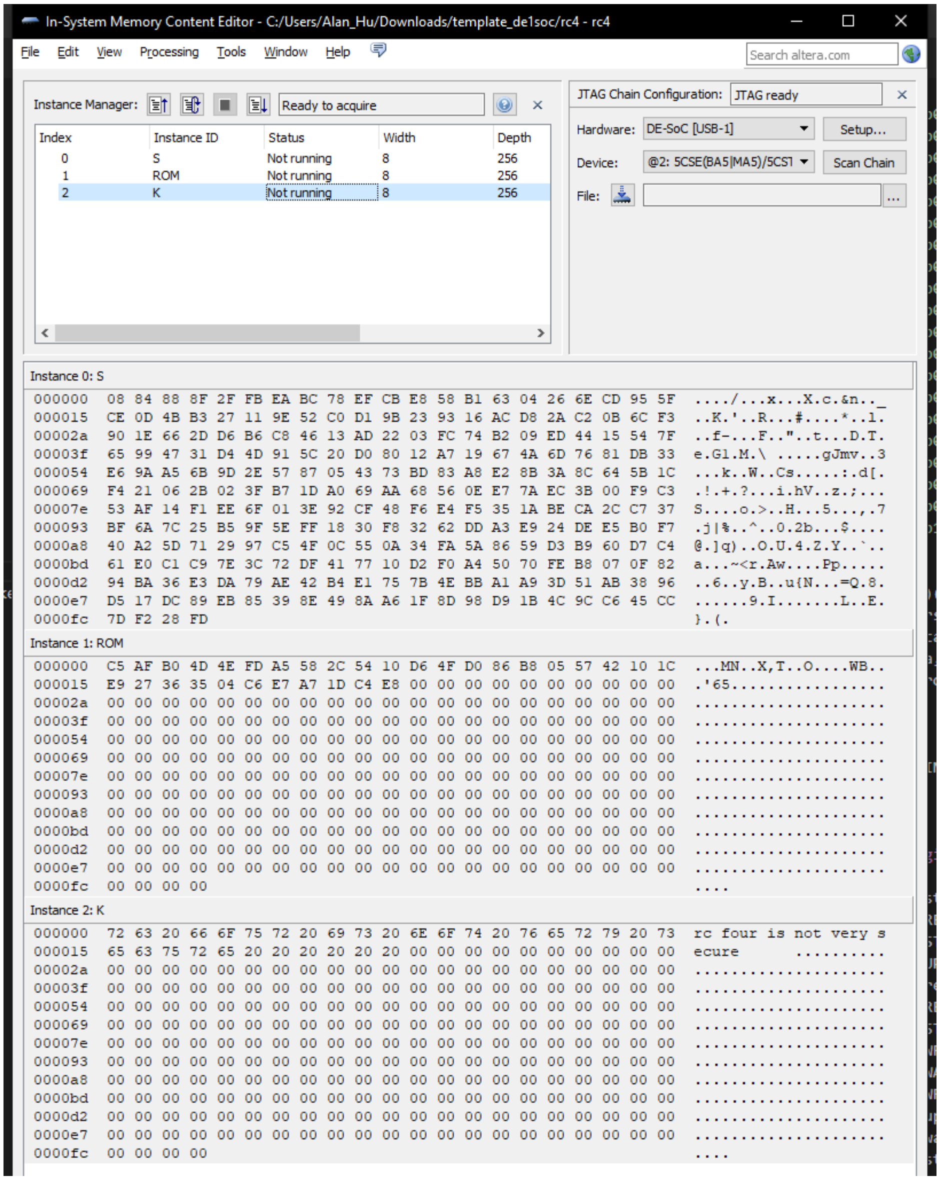
Operation & explanation of the simulation is written in the comment of every testbench code.

Flow chart:



Decryption result (for task 3):

Message 4:



Index	Instance ID	Status	Width	Depth
0	S	Not running	8	256
1	ROM	Not running	8	256
2	K	Not running	8	256

Hardware: DE-SoC [USB-1]

Device: @2: 5CSE(BA5|MA5)/5CS1

Instance 0: S

```
000000  08 84 88 8F 2F FB EA BC 78 EF CB E8 58 B1 63 04 26 6E CD 95 5F  ..../...x...X.c.&n.._
000015  CE 0D 4B B3 27 11 9E 52 C0 D1 9B 23 93 16 AC D8 2A C2 0B 6C F3  ..K.'..R...#....*..l.
00002a  90 1E 66 2D D6 B6 C8 46 13 AD 22 03 FC 74 B2 09 ED 44 15 54 7F  ..f-...F..".t...D.T.
00003f  65 99 47 31 D4 4D 91 5C 20 D0 80 12 A7 19 67 4A 6D 76 81 DB 33  e.G1.M.\ .....gJmv..3
000054  E6 9A A5 6B 9D 2E 57 87 05 43 73 BD 83 A8 E2 8B 3A 8C 64 5B 1C  ...k..W..Cs.....:.d[.
000069  F4 21 06 2B 02 3F B7 1D A0 69 AA 68 56 0E E7 7A EC 3B 00 F9 C3  .!.+.?...i.hV..z.;...
00007e  53 AF 14 F1 EE 6F 01 3E 92 CF 48 F6 E4 F5 35 1A BE CA 2C C7 37  S....o.>..H...5...,.7
000093  BF 6A 7C 25 B5 9F 5E FF 18 30 F8 32 62 DD A3 E9 24 DE E5 B0 F7  .j|%..^..0.2b...$....
0000a8  40 A2 5D 71 29 97 C5 4F 0C 55 0A 34 FA 5A 86 59 D3 B9 60 D7 C4  @.]q)..O.U.4.Z.Y..`..
0000bd  61 E0 C1 C9 7E 3C 72 DF 41 77 10 D2 F0 A4 50 70 FE B8 07 0F 82  a...~<r.Aw....Pp.....
0000d2  94 BA 36 E3 DA 79 AE 42 B4 E1 75 7B 4E BB A1 A9 3D 51 AB 38 96  ..6..y.B..u{N...=Q.8.
0000e7  D5 17 DC 89 EB 85 39 8E 49 8A A6 1F 8D 98 D9 1B 4C 9C C6 45 CC  ......9.I.......L..E.
0000fc  7D F2 28 FD                                                     }.(.
```

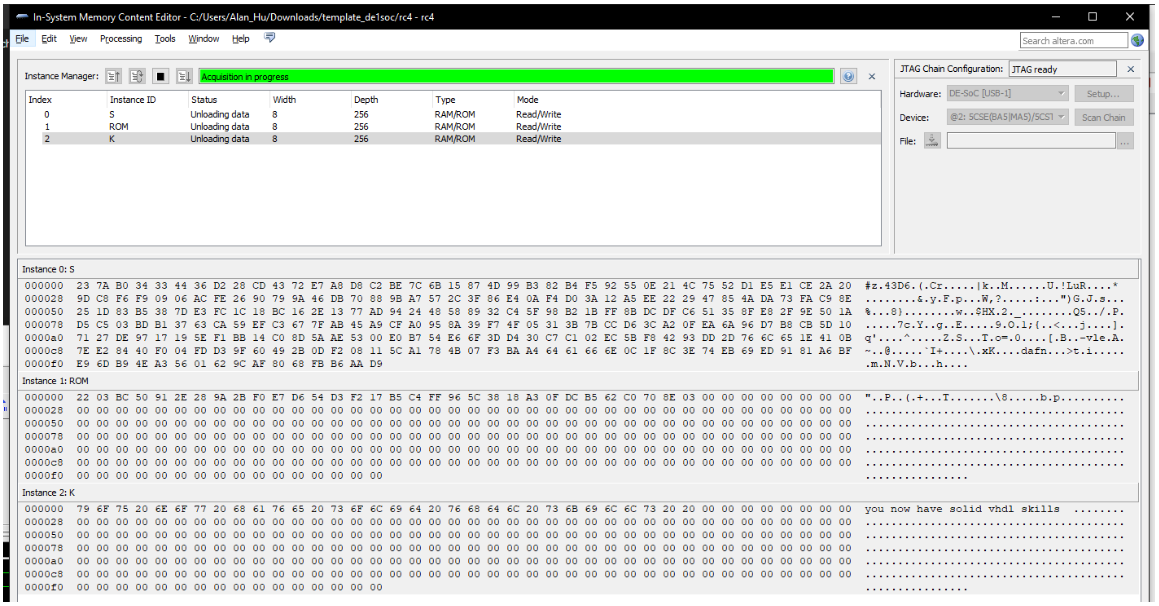
Instance 1: ROM

```
000000  C5 AF B0 4D 4E FD A5 58 2C 54 10 D6 4F D0 86 B8 05 57 42 10 1C  ...MN..X,T..O....WB..
000015  E9 27 36 35 04 C6 E7 A7 1D C4 E8 00 00 00 00 00 00 00 00 00 00  .'65.................
00002a  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
00003f  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
000054  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
000069  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
00007e  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
000093  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
0000a8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
0000bd  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
0000d2  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
0000e7  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
0000fc  00 00 00 00                                                     ....
```

Instance 2: K

```
000000  72 63 20 66 6F 75 72 20 69 73 20 6E 6F 74 20 76 65 72 79 20 73  rc four is not very s
000015  65 63 75 72 65 20 20 20 20 20 20 00 00 00 00 00 00 00 00 00 00  ecure      ..........
00002a  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
00003f  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
000054  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
000069  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
00007e  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
000093  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
0000a8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
0000bd  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
0000d2  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
0000e7  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....................
0000fc  00 00 00 00                                                     ....
```

Message 5:



JTAG Chain Configuration: JTAG ready

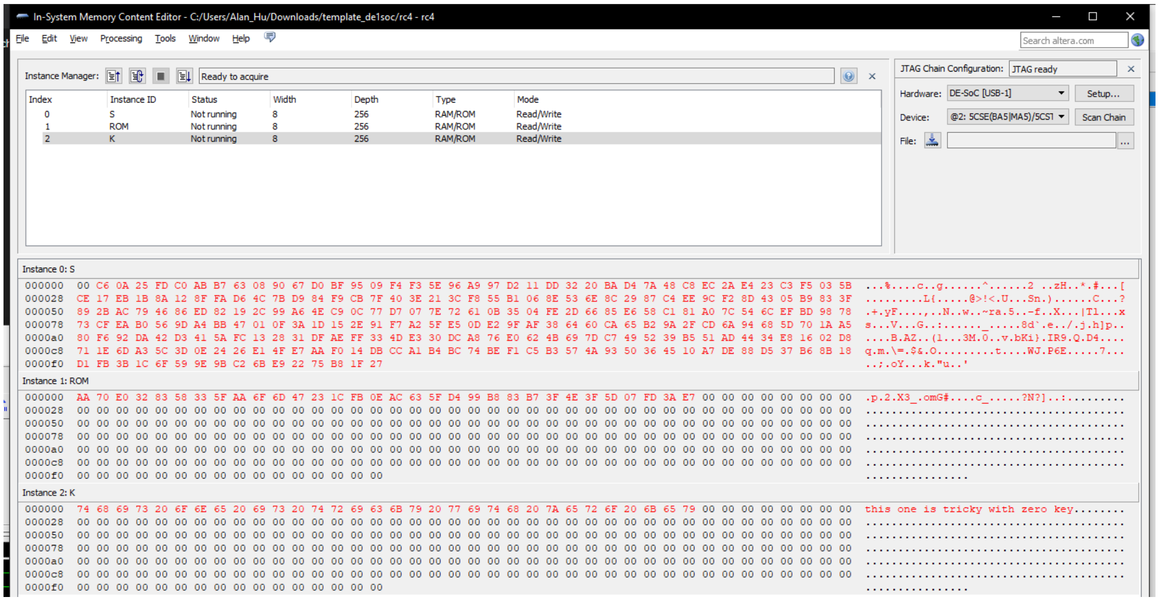
Hardware: DE-SoC [USB-1]

Device: @2: 5CSE(BA5|MA5)/5CS1

Index	Instance ID	Status	Width	Depth	Type	Mode
0	S	Unloading data	8	256	RAM/ROM	Read/Write
1	ROM	Unloading data	8	256	RAM/ROM	Read/Write
2	K	Unloading data	8	256	RAM/ROM	Read/Write

```
Instance 0: S
000000  23 7A B0 34 33 44 36 D2 28 CD 43 72 E7 A8 D8 C2 BE 7C 6B 15 87 4D 99 B3 82 B4 F5 92 55 0E 21 4C 75 52 D1 E5 E1 CE 2A 20  #z.43D6.(.Cr.....|k..M......U.!LuR....* 
000028  9D C8 F6 F9 09 06 AC FE 26 90 79 9A 46 DB 70 88 9B A7 57 2C 3F 86 E4 0A F4 D0 3A 12 A5 EE 22 29 47 85 4A DA 73 FA C9 8E  ........&.y.F.p...W,?.....:...")G.J.s...
000050  25 1D 83 B5 38 7D E3 FC 1C 18 BC 16 2E 13 77 AD 94 24 48 58 89 32 C4 5F 98 B2 1B FF 8B DC DF C6 51 35 8F E8 2F 9E 50 1A  %...8}........w..$HX.2._........Q5../.P.
000078  D5 C5 03 BD B1 37 63 CA 59 EF C3 67 7F AB 45 A9 CF A0 95 8A 39 F7 4F 05 31 3B 7B CC D6 3C A2 0F EA 6A 96 D7 B8 CB 5D 10  .....7c.Y..g..E.....9.O.1;{..<...j....].
0000a0  71 27 DE 97 17 19 5E F1 BB 14 C0 8D 5A AE 53 00 E0 B7 54 E6 6F 3D D4 30 C7 C1 02 EC 5B F8 42 93 DD 2D 76 6C 65 1E 41 0B  q'....^.....Z.S...T.o=.0....[.B..-vle.A.
0000c8  7E E2 84 40 F0 04 FD D3 9F 60 49 2B 0D F2 08 11 5C A1 78 4B 07 F3 BA A4 64 61 66 6E 0C 1F 8C 3E 74 EB 69 ED 91 81 A6 BF  ~..@.....`I+....\.xK....dafn...>t.i.....
0000f0  E9 6D B9 4E A3 56 01 62 9C AF 80 68 FB B6 AA D9                                                                          .m.N.V.b...h....
Instance 1: ROM
000000  22 03 BC 50 91 2E 28 9A 2B F0 E7 D6 54 D3 F2 17 B5 C4 FF 96 5C 38 18 A3 0F DC B5 62 C0 70 8E 03 00 00 00 00 00 00 00 00  "..P..(.+...T.......\8.....b.p..........
000028  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000078  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000c8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00                                                                          ................
Instance 2: K
000000  79 6F 75 20 6E 6F 77 20 68 61 76 65 20 73 6F 6C 69 64 20 76 68 64 6C 20 73 6B 69 6C 6C 73 20 20 00 00 00 00 00 00 00 00  you now have solid vhdl skills  ........
000028  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000078  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000c8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00                                                                          ................
```

Message6


In-System Memory Content Editor - C:/Users/Alan_Hu/Downloads/template_de1soc/rc4 - rc4
File
Edit
View
Processing
Tools
Window
Help
Search altera.com
Instance Manager:
Ready to acquire
JTAG Chain Configuration:
Setup...
Scan Chain
File:

JTAG Chain Configuration: JTAG ready

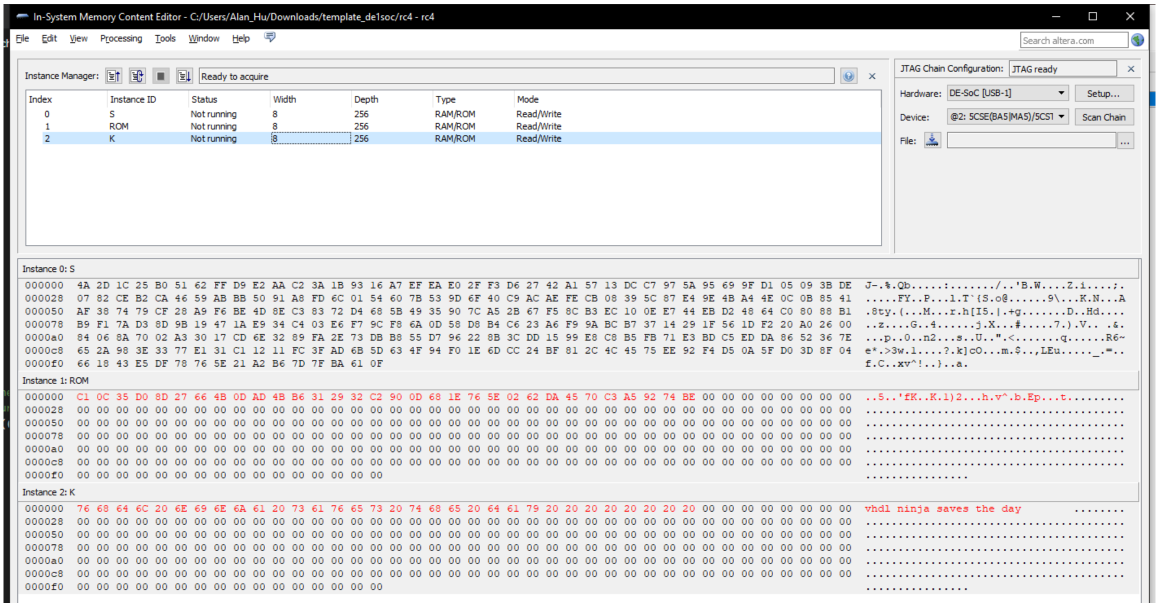
Hardware: DE-SoC [USB-1]

Device: @2: 5CSE(BA5|MA5)/5CS1

Index	Instance ID	Status	Width	Depth	Type	Mode
0	S	Not running	8	256	RAM/ROM	Read/Write
1	ROM	Not running	8	256	RAM/ROM	Read/Write
2	K	Not running	8	256	RAM/ROM	Read/Write

```
Instance 0: S
000000  00 C6 0A 25 FD C0 AB B7 63 08 90 67 D0 BF 95 09 F4 F3 5E 96 A9 97 D2 11 DD 32 20 BA D4 7A 48 C8 EC 2A E4 23 C3 F5 03 5B  ...%....c..g......^......2 ..zH..*.#...[
000028  CE 17 EB 1B 8A 12 8F FA D6 4C 7B D9 84 F9 CB 7F 40 3E 21 3C F8 55 B1 06 8E 53 6E 8C 29 87 C4 EE 9C F2 8D 43 05 B9 83 3F  .........L{.....@>!<.U...Sn.)......C...?
000050  89 2B AC 79 46 86 ED 82 19 2C 99 A6 4E C9 0C 77 D7 07 7E 72 61 0B 35 04 FE 2D 66 85 E6 58 C1 81 A0 7C 54 6C EF BD 98 78  .+.yF....,..N..w..~ra.5..-f..X...|Tl...x
000078  73 CF EA B0 56 9D A4 BB 47 01 0F 3A 1D 15 2E 91 F7 A2 5F E5 0D E2 9F AF 38 64 60 CA 65 B2 9A 2F CD 6A 94 68 5D 70 1A A5  s...V...G..:......_.....8d`.e../.j.h]p..
0000a0  80 F6 92 DA 42 D3 41 5A FC 13 28 31 DF AE FF 33 4D E3 30 DC A8 76 E0 62 4B 69 7D C7 49 52 39 B5 51 AD 44 34 E8 16 02 D8  ....B.AZ..(1....3M.0..v.bKi}.IR9.Q.D4....
0000c8  71 1E 6D A3 5C 3D 0E 24 26 E1 4F E7 AA F0 14 DB CC A1 B4 BC 74 BE F1 C5 B3 57 4A 93 50 36 45 10 A7 DE 88 D5 37 B6 8B 18  q.m.\=.$&.O.........t....WJ.P6E.....7...
0000f0  D1 FB 3B 1C 6F 59 9E 9B C2 6B E9 22 75 B8 1F 27                                                                          ..;.oY...k."u..'
Instance 1: ROM
000000  AA 70 E0 32 83 58 33 5F AA 6F 6D 47 23 1C FB 0E AC 63 5F D4 99 B8 83 B7 3F 4E 3F 5D 07 FD 3A E7 00 00 00 00 00 00 00 00  .p.2.X3_.omG#....c_.....?N?]..:.........
000028  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000078  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000c8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00                                                                          ................
Instance 2: K
000000  74 68 69 73 20 6F 6E 65 20 69 73 20 74 72 69 63 6B 79 20 77 69 74 68 20 7A 65 72 6F 20 6B 65 79 00 00 00 00 00 00 00 00  this one is tricky with zero key........
000028  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000078  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000c8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00                                                                          ................
```

Message 7



In-System Memory Content Editor - C:/Users/Alan_Hu/Downloads/template_de1soc/rc4 - rc4

File Edit View Processing Tools Window Help

Instance Manager: Ready to acquire

Index	Instance ID	Status	Width	Depth	Type	Mode
0	S	Not running	8	256	RAM/ROM	Read/Write
1	ROM	Not running	8	256	RAM/ROM	Read/Write
2	K	Not running	8	256	RAM/ROM	Read/Write

JTAG Chain Configuration: JTAG ready

Hardware: DE-SoC [USB-1]

Device: @2: 5CSE(BA5|MA5)/5CS1

Instance 0: S

```
000000  4A 2D 1C 25 B0 51 62 FF D9 E2 AA C2 3A 1B 93 16 A7 EF EA E0 2F F3 D6 27 42 A1 57 13 DC C7 97 5A 95 69 9F D1 05 09 3B DE  J-.%.Qb.....:......./..'B.W....Z.i....;.
000028  07 82 CE B2 CA 46 59 AB BB 50 91 A8 FD 6C 01 54 60 7B 53 9D 6F 40 C9 AC AE FE CB 08 39 5C 87 E4 9E 4B A4 4E 0C 0B 85 41  .....FY..P...l.T`{S.o@......9\...K.N...A
000050  AF 38 74 79 CF 28 A9 F6 BE 4D 8E C3 83 72 D4 68 5B 49 35 90 7C A5 2B 67 F5 8C B3 EC 10 0E E7 44 EB D2 48 64 C0 80 88 B1  .8ty.(...M...r.h[I5.|.+g.......D..Hd....
000078  B9 F1 7A D3 8D 9B 19 47 1A E9 34 C4 03 E6 F7 9C F8 6A 0D 58 D8 B4 C6 23 A6 F9 9A BC B7 37 14 29 1F 56 1D F2 20 A0 26 00  ..z....G..4......j.X...#.....7.).V.. .&.
0000a0  84 06 8A 70 02 A3 30 17 CD 6E 32 89 FA 2E 73 DB B8 55 D7 96 22 8B 3C DD 15 99 E8 C8 B5 FB 71 E3 BD C5 ED DA 86 52 36 7E  ...p..0..n2...s..U..".<.......q......R6~
0000c8  65 2A 98 3E 33 77 E1 31 C1 12 11 FC 3F AD 6B 5D 63 4F 94 F0 1E 6D CC 24 BF 81 2C 4C 45 75 EE 92 F4 D5 0A 5F D0 3D 8F 04  e*.>3w.1....?.k]cO...m.$..,LEu....._.=..
0000f0  66 18 43 E5 DF 78 76 5E 21 A2 B6 7D 7F BA 61 0F                                                                          f.C..xv^!..}..a.
```

Instance 1: ROM

```
000000  C1 0C 35 D0 8D 27 66 4B 0D AD 4B B6 31 29 32 C2 90 0D 68 1E 76 5E 02 62 DA 45 70 C3 A5 92 74 BE 00 00 00 00 00 00 00 00  ..5..'fK..K.1)2...h.v^.b.Ep...t.........
000028  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000078  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000c8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00                                                                          ................
```

Instance 2: K

```
000000  76 68 64 6C 20 6E 69 6E 6A 61 20 73 61 76 65 73 20 74 68 65 20 64 61 79 20 20 20 20 20 20 20 20 00 00 00 00 00 00 00 00  vhdl ninja saves the day        ........
000028  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
000078  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000c8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................................
0000f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00                                                                          ................
```

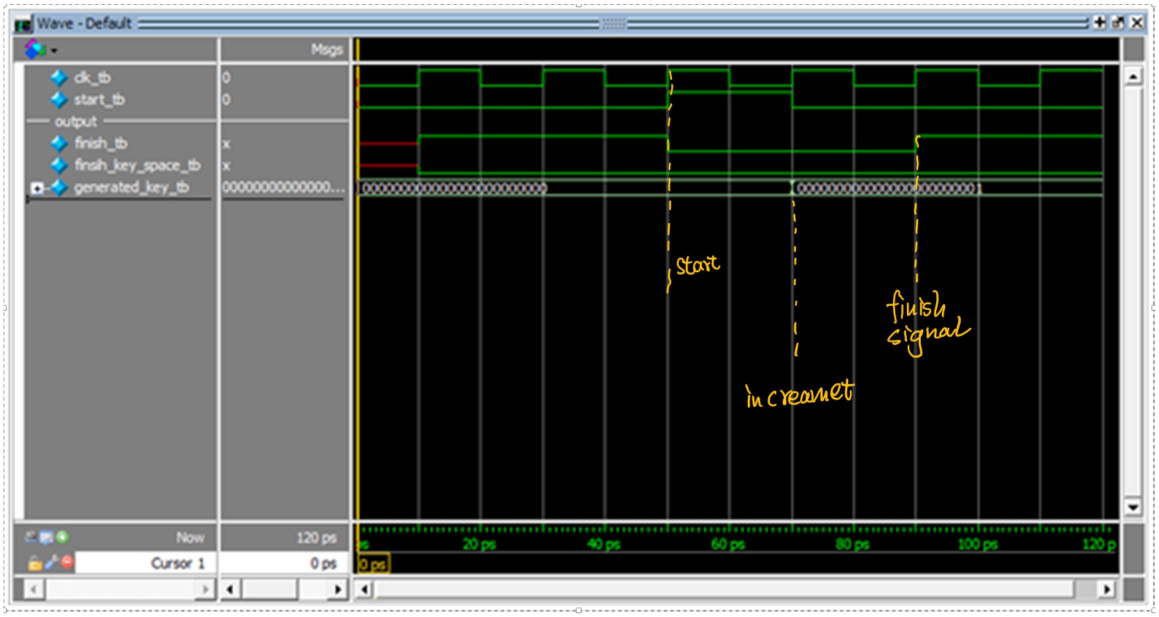
Message 8：

No key found

Test bench:

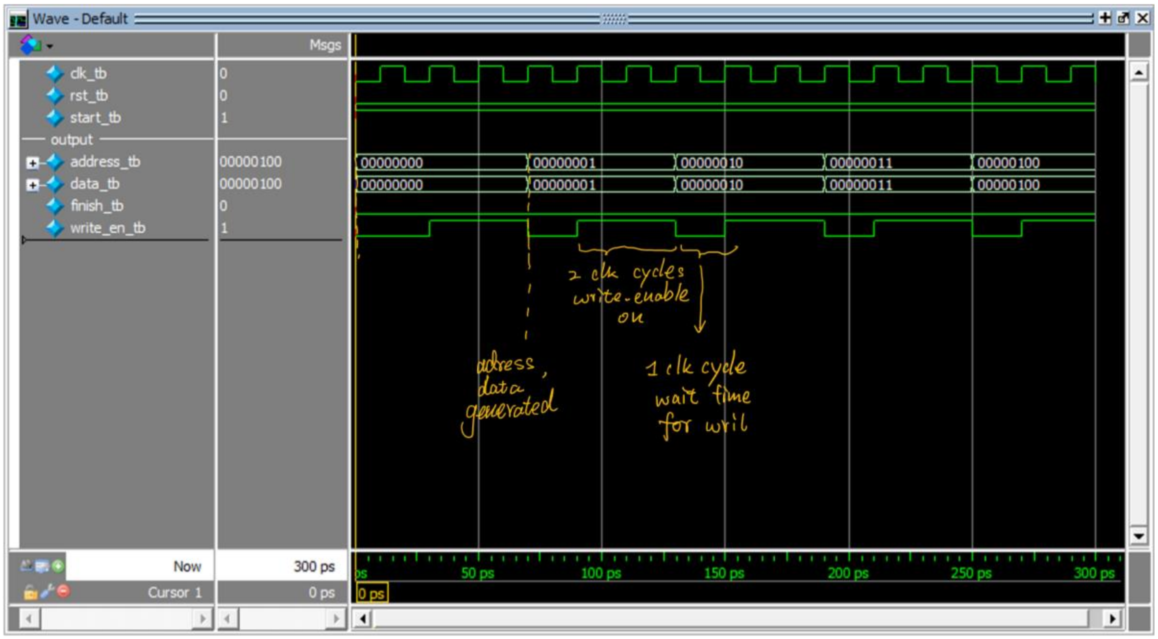
For Key generator:

File "*/rtl/key_gen_tb.sv" is the testbench for “key_gen.sv”



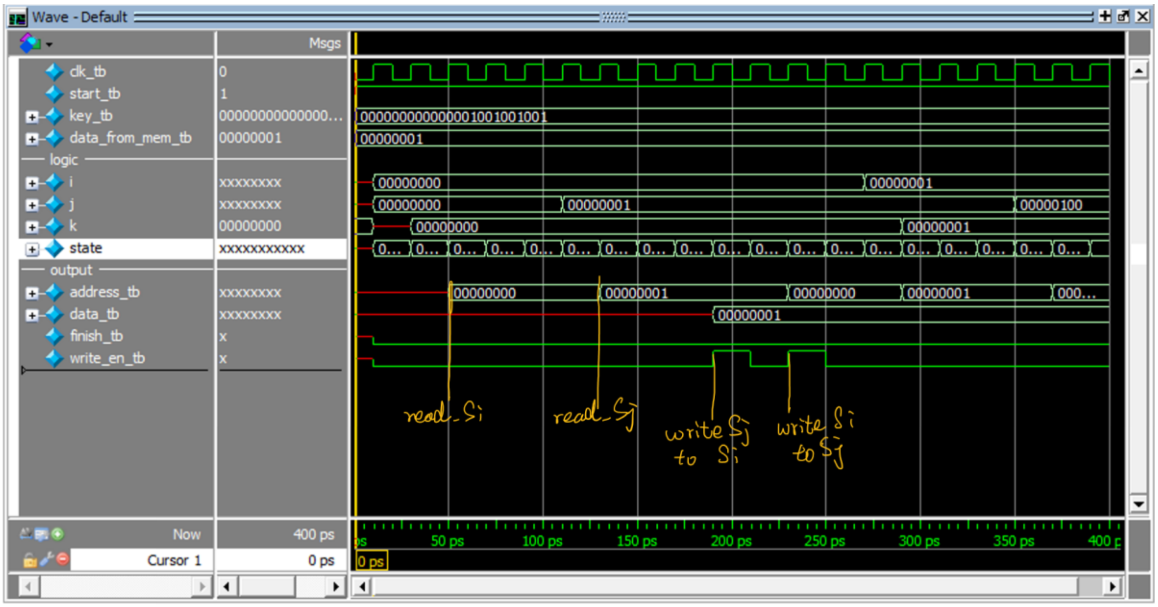
For initialize memory:

File "*/rtl/mem_init_tb.sv" is the testbench for “mem_init.sv”.



For swap:

File "*/rtl/swap_tb.sv" is the testbench for “swap.sv”



For decryption & check result:

Since decryption is really similar to swap, a simulation is non-necessary.