RISC-V.br - SoC PLC

AES – IP

PEM

Center of Electrical Engineering and Informatics
Federal University of Campina Grande

- Sumário
  - Equipe AES
  - Objetivos da equipe
  - Importância do IP
  - AES – IP
    - Arquitetura proposta
    - Uso do IP
    - O que foi desenvolvido?
    - Testes iniciais e seus resultados
    - O que falta?
  - Verificação do IP
    - Modelo de referência
      - Objetivos
      - Software em C++
      - Resultados
      - O que falta?
    - UVM
      - Objetivos
      - O que foi desenvolvido?
      - O que falta?

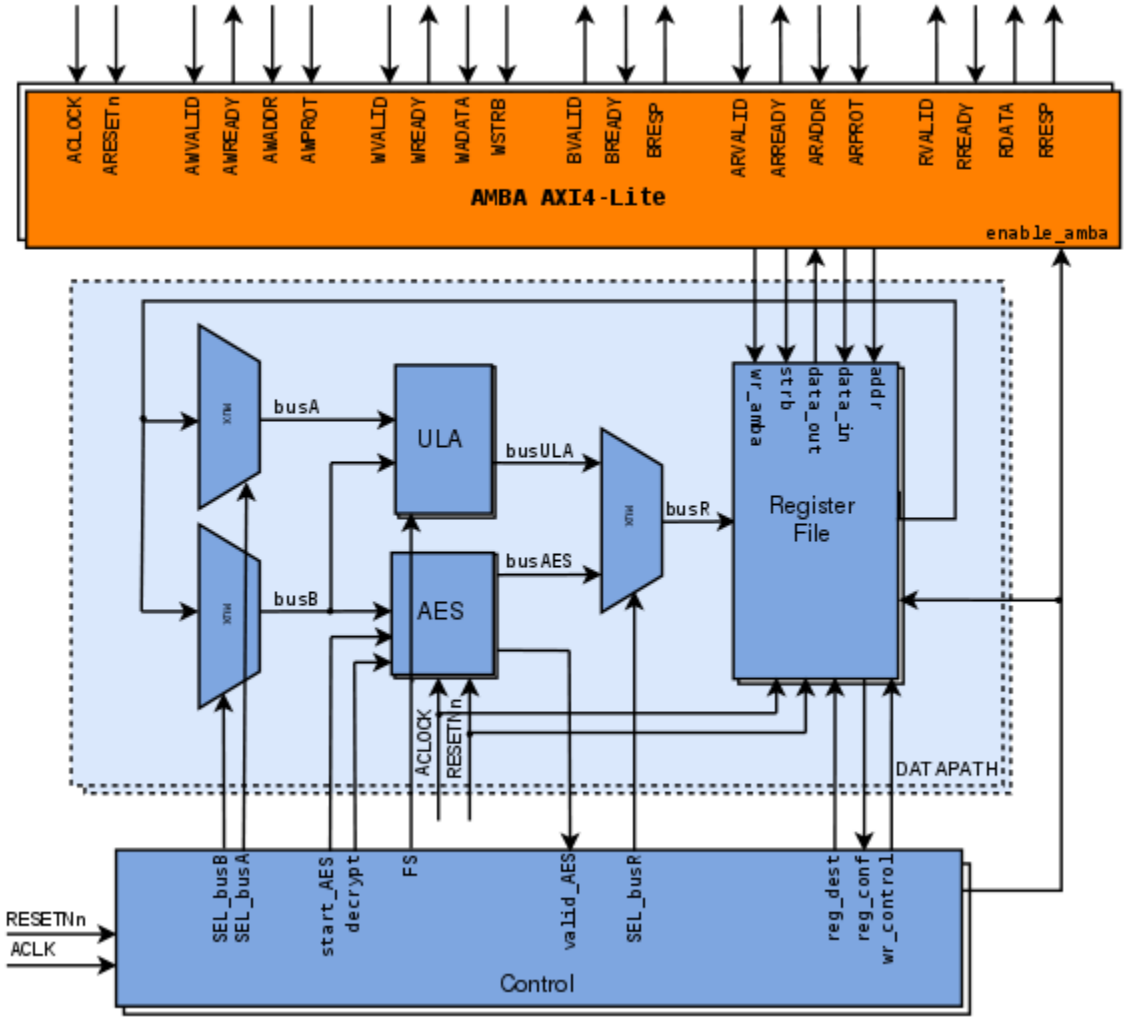
- Equipe AES
  - Atualmente a equipe conta com 7 membros que trabalham nas seguintes áreas de desenvolvimento do IP:
    - Gabriel Villanova (**sub-líder**)
    - José Samuel (**desenvolvedor de hardware**)
    - Rubens Roux (**desenvolvedor de hardware**)
    - Pedro Cavalcante (**desenvolvedor de verificação**)
    - Lucas Eliseu (**desenvolvedor de verificação**)
    - Dimas Germano (**desenvolvendor de modelo de referência**)
    - Cícero (**desenvolvendor de modelo de referência**)

- Objetivos da equipe
  - O objetivo da equipe é desenvolver em hardware o algoritmo de encriptação AES (**Advanced Encryption Standard**) e alguns de seus modos de operação, sendo eles:
    - ECB (**Electronic Codebook**)
    - CBC (**Cipher Block Chaining**)
    - PCBC (**Propagating Cipher Block Chaining**)
    - CFB (**Cipher Feedback**)
    - OFB (**Output Feedback**)
    - CTR (**Counter**)

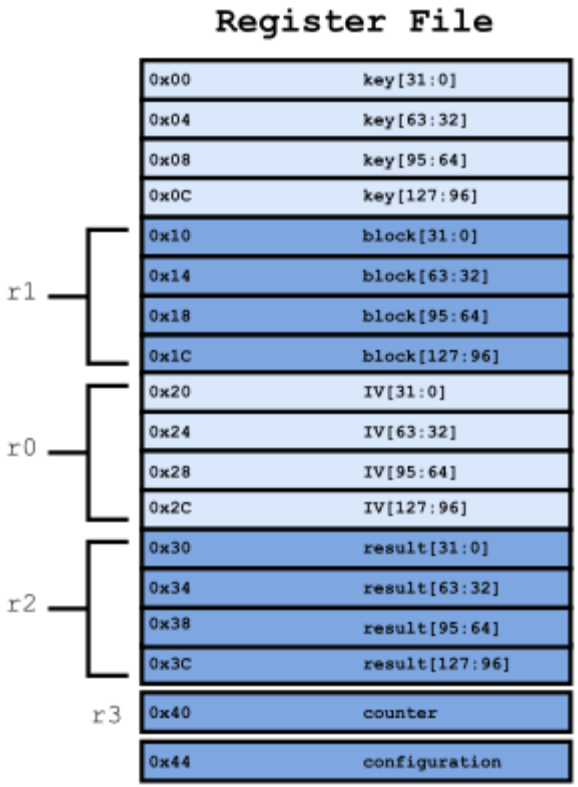
- Importância do IP
  - O algoritmo do AES junto de seus modos de operação dão ao SoC segurança e confidencialidade nas mensagens transmitidas e recebidas
  - Os modos configuráveis de operações implementados no IP facilitam a implementação de diferentes padrões
  - O AES em hardware tem maior velocidade de processamento em relação a sua implementação em software

- Arquitetura proposta
  - A arquitetura foi desenvolvida para implementar o AES e seus modos de operação
  - A escrita nos registradores se faz através da interface **AMBA AXI4 – Lite**

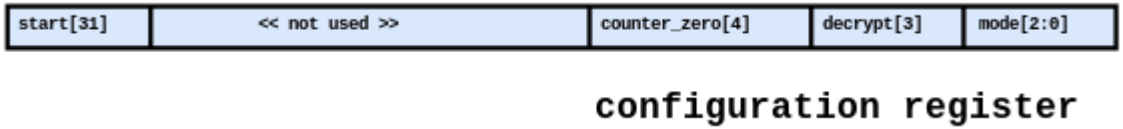
- Arquitetura proposta



- Arquitetura proposta
  - Os registradores foram definidos como segue



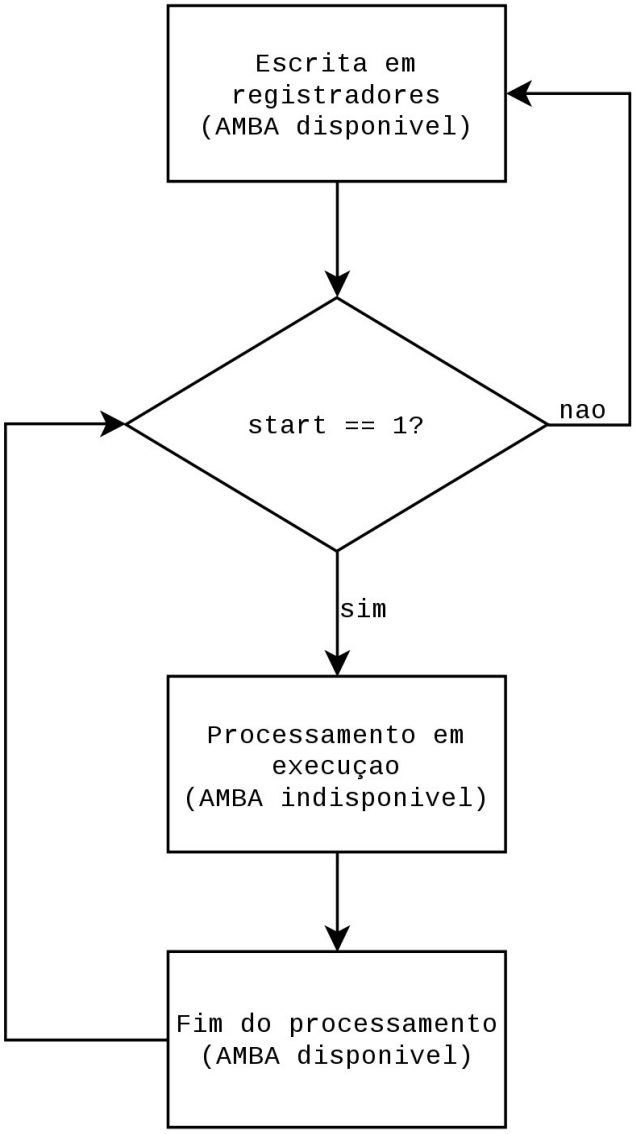
- Arquitetura proposta
  - O registrador de configuração está definido como:



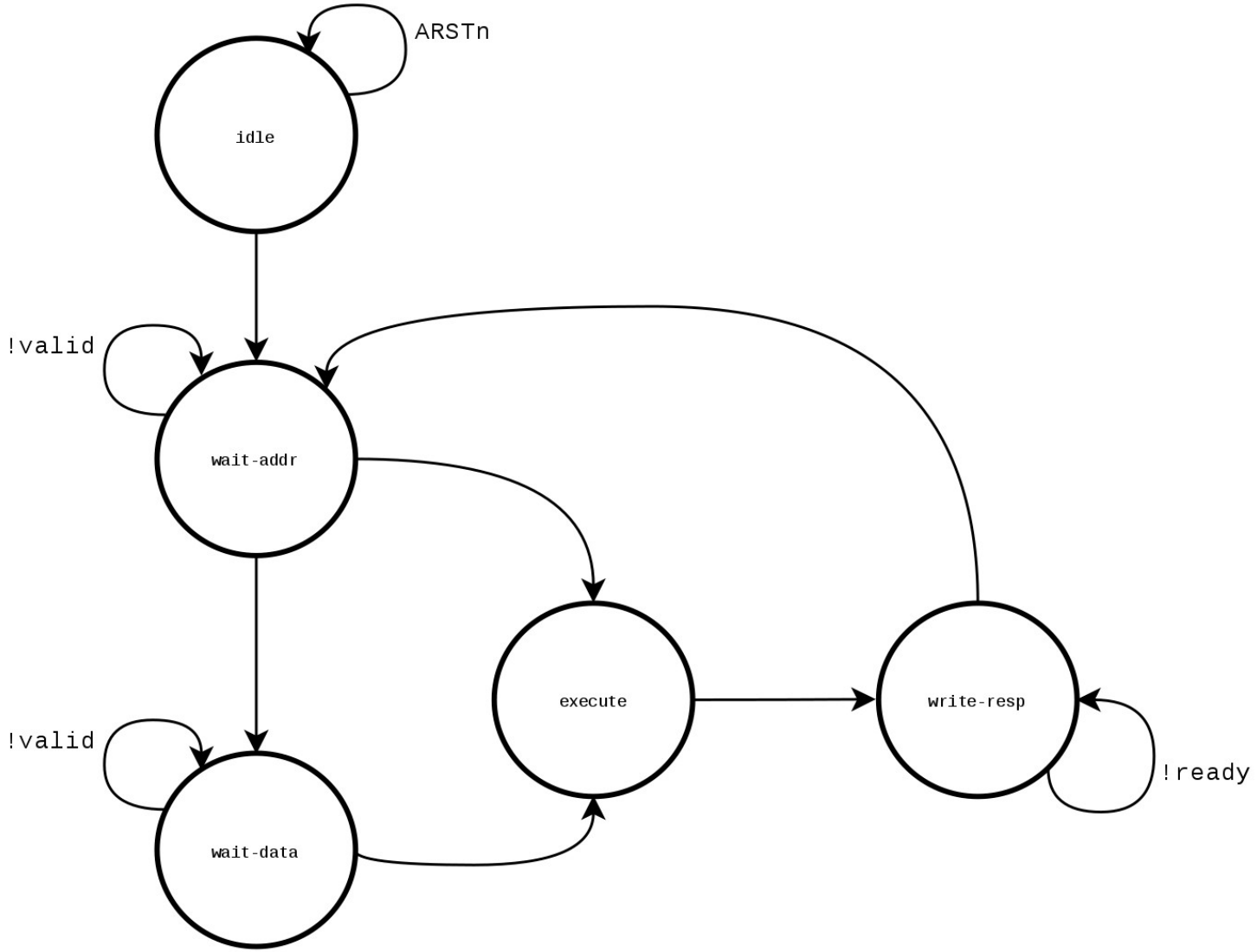
configuration register

  - **start[31]:** '1' inicia o processamento do IP
  - **counter_zero[4]:** '1' reseta o valor do registrador r3 para zero
  - **decrypt[3]:** '1' operação de decriptação, '0' encriptação
  - **mode[2:0]:** define os modos de operação
    - ECB (**000**) (**default**)
    - CBC (**001**)
    - PCBC (**010**)
    - CFB (**011**)
    - OFB (**100**)
    - CTR (**101**)

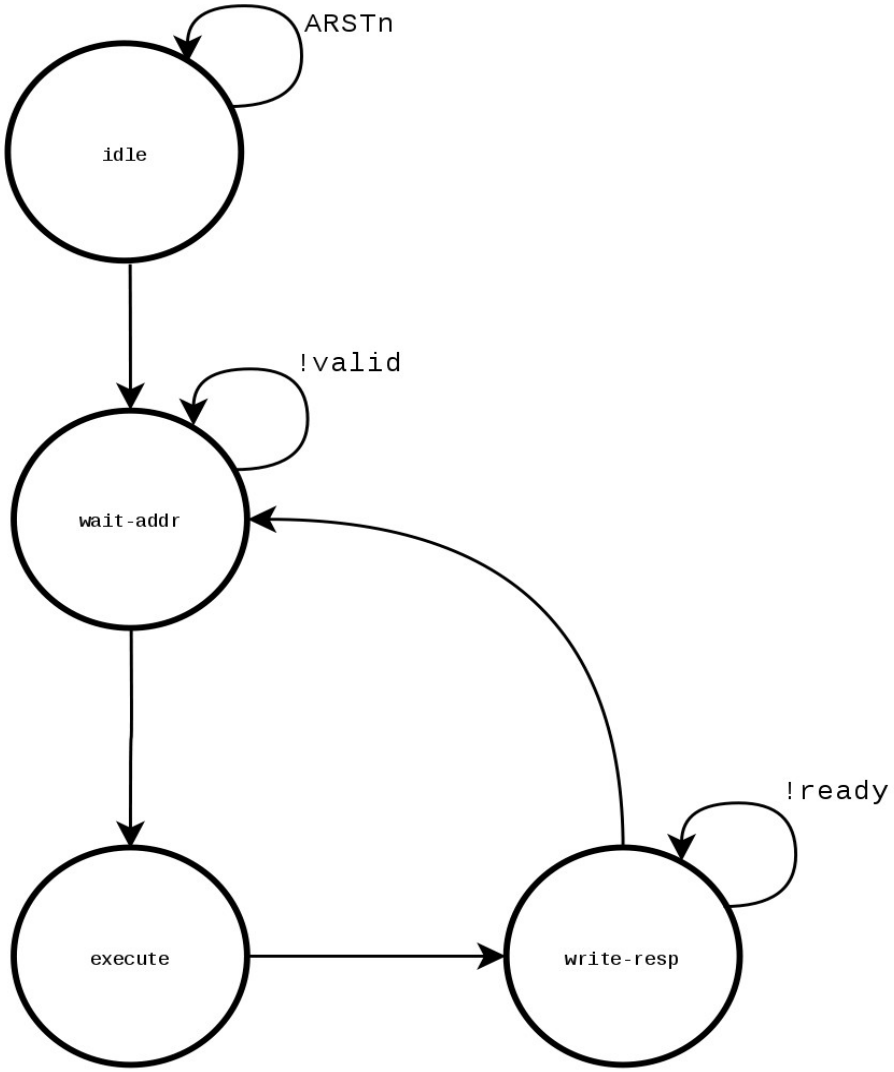
- Uso do IP


Escrita em registradores (AMBA disponivel)
start == 1?
nao
sim
Processamento em execuçao (AMBA indisponivel)
Fim do processamento (AMBA disponivel)

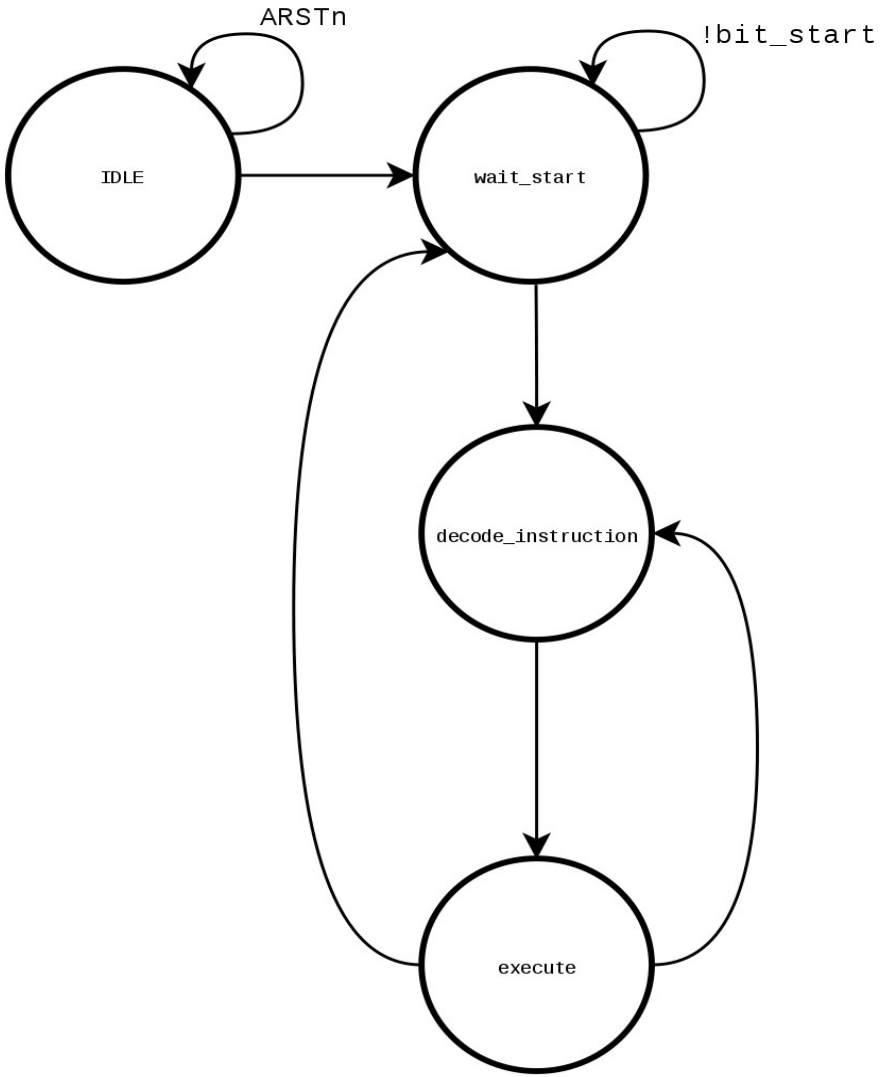
AMBA 4LITE - WRITE CHANNEL



AMBA 4LITE - READ CHANNEL

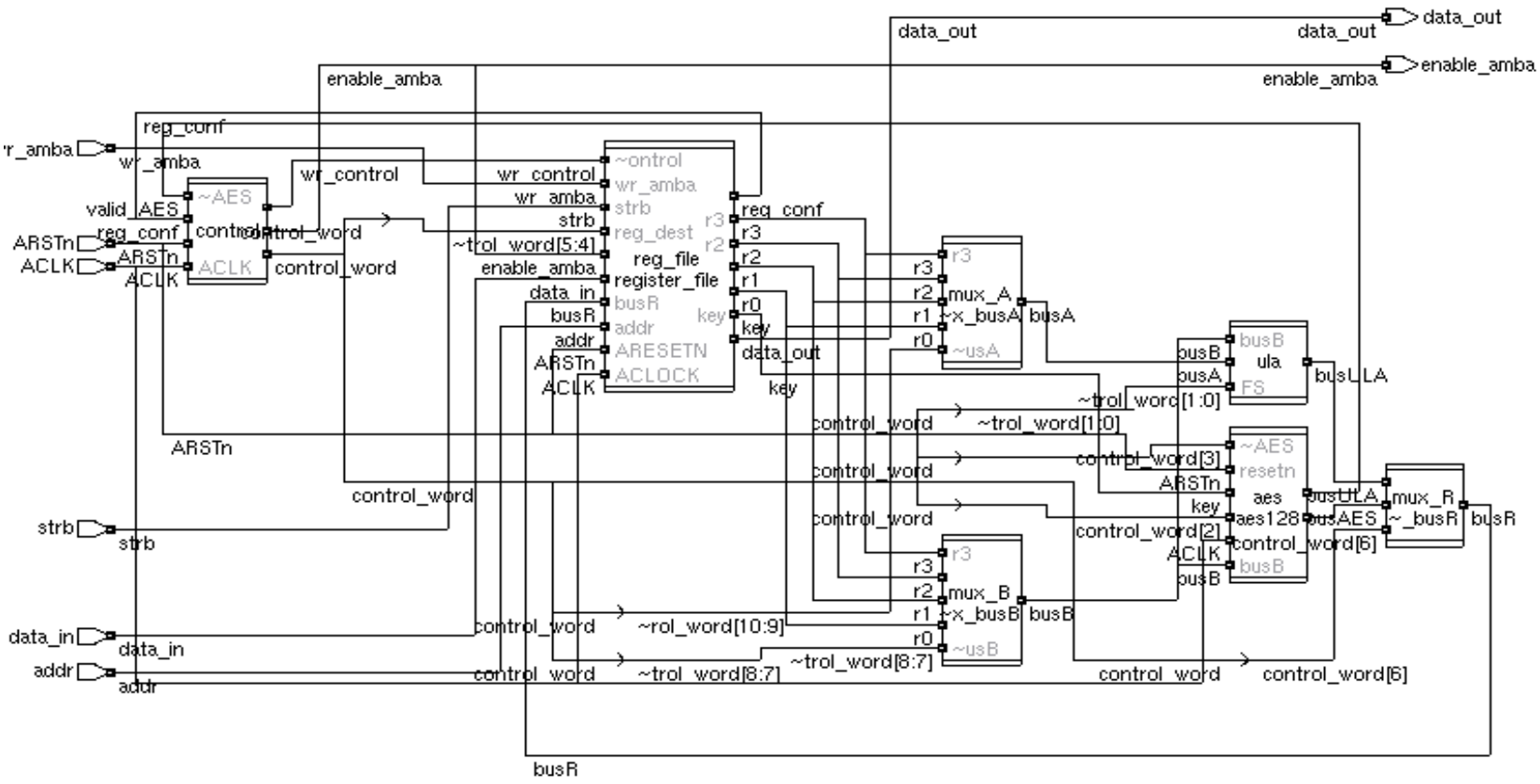


CONTROL


ARSTn
!bit_start
IDLE
wait_start
decode_instruction
execute

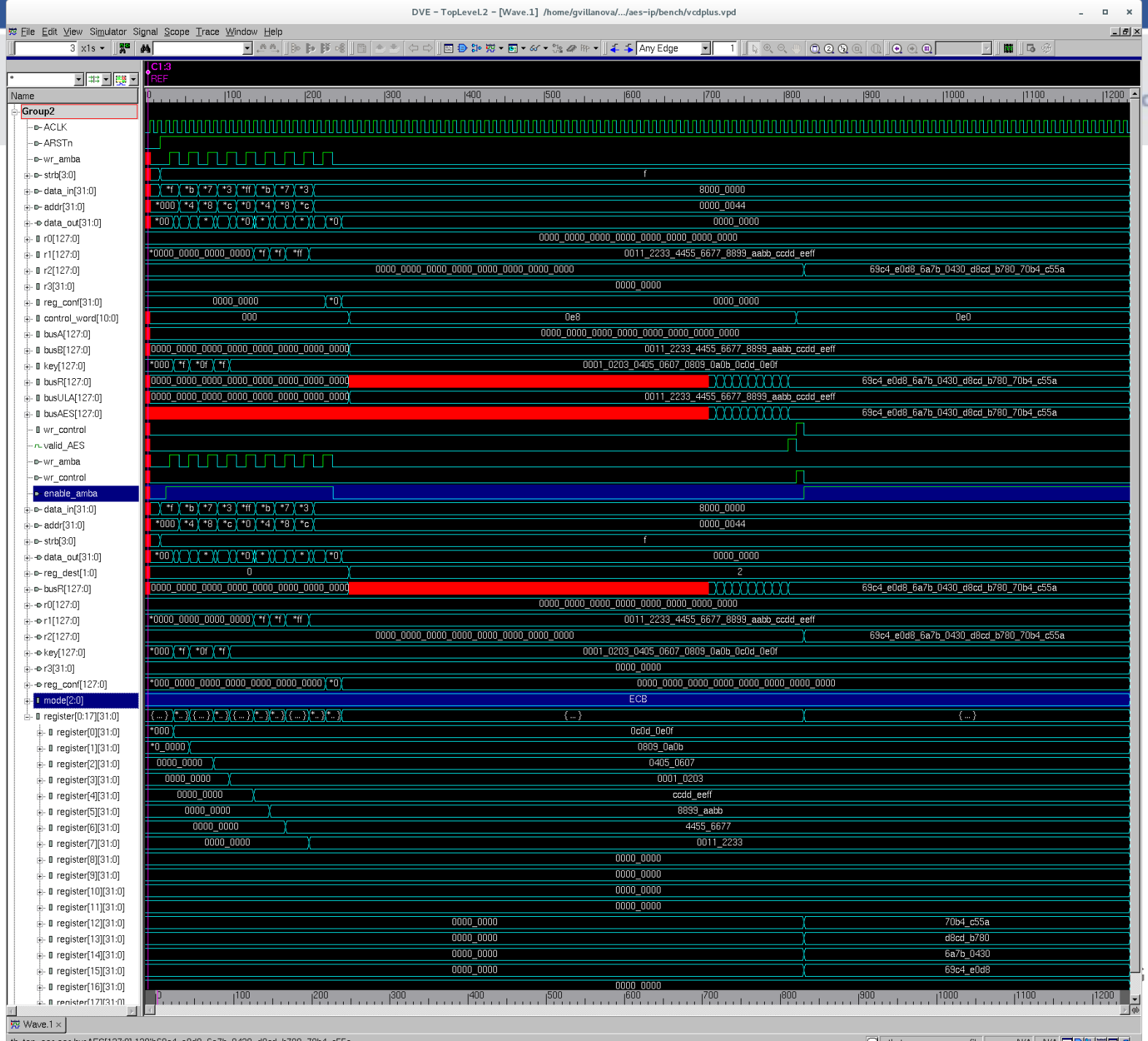
- O que foi desenvolvido?
  - Atualmente o **hardware encontra-se quase completo**, faltando somente a interface AMBA que está em fim de desenvolvimento
  - Os teste iniciais (sem UVM e sem AMBA) estão sendo realizados e mostrando bons resultados
  - As figuras seguintes mostram o esquema RTL criado pelo DVE e algumas formas de ondas dos testes realizados

- O que foi desenvolvido?



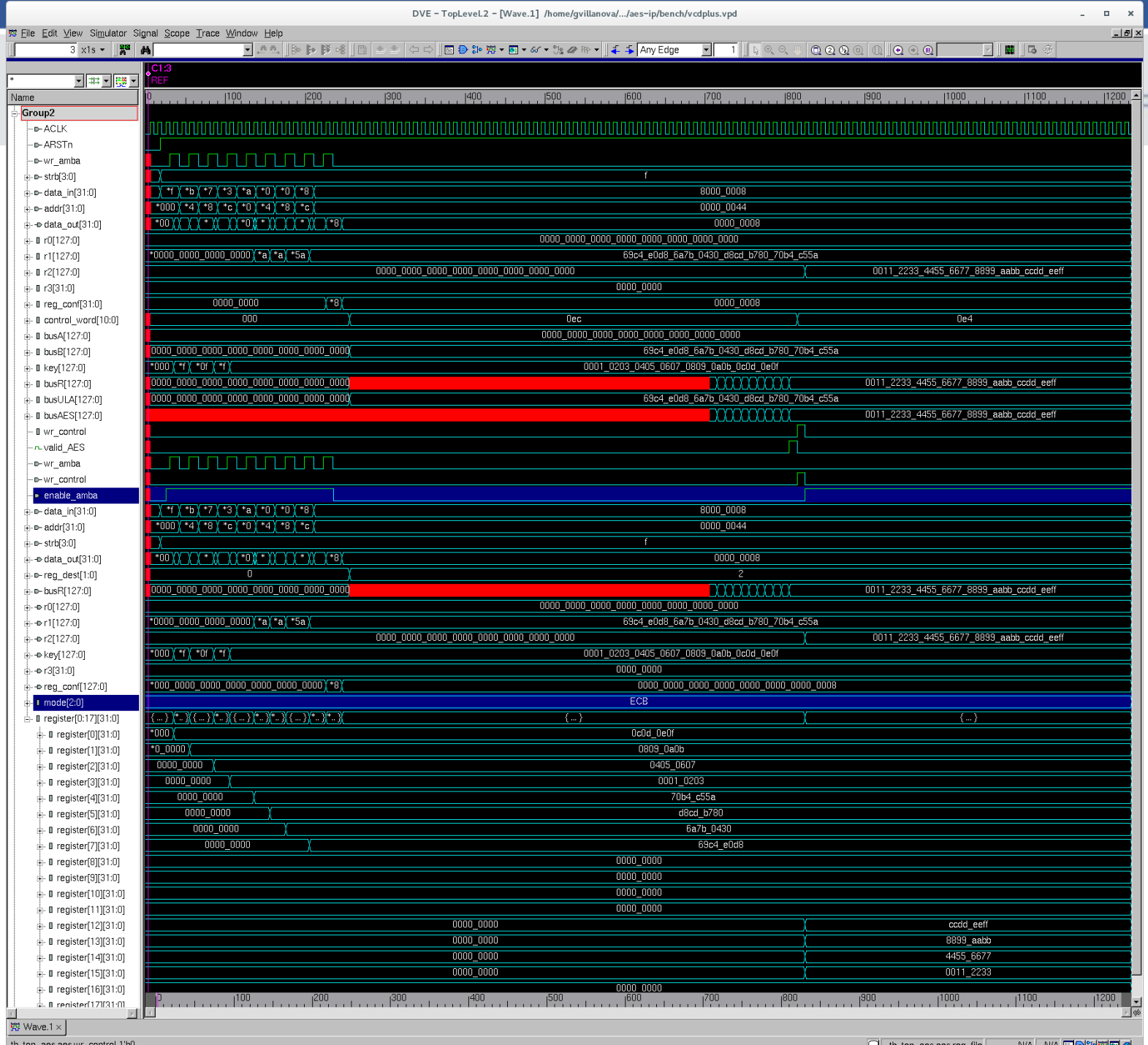
- Testes iniciais e resultados
  - **Encriptação em modo ECB**

```
42      initial begin
43          $vcdpluson;
44          $vcdplusmemon;
45
46          // key    = 00010203_04050607_08090a0b_0c0d0e0f
47          // block  = 00112233_44556677_8899aabb_ccddeeff
48          // cipher = 69c4e0d8_6a7b0430_d8cdb780_70b4c55a
49
50          reset();
51
52          // ** Write KEY, Block and Reg Conf (mode ECB) ** //
53          write_key(128'h00010203_04050607_08090a0b_0c0d0e0f);
54          write_block(128'h00112233_44556677_8899aabb_ccddeeff);
55          write_reg_conf({1'b1,26'b0,1'b0,1'b0,3'b000});
56
57          // ** Fim simulacao ** //
58          #1000
59          $finish;
```


DVE – TopLevel.2 – [Wave.1] /home/gvillanova/.../aes-ip/bench/vcdplus.vpd
File Edit View Simulator Signal Scope Trace Window Help
Any Edge
C1:3
REF
Name
Group2
ACLK
ARSTn
wr_amba
strb[3:0]
data_in[31:0]
addr[31:0]
data_out[31:0]
r0[127:0]
r1[127:0]
r2[127:0]
r3[31:0]
reg_conf[31:0]
control_word[10:0]
busA[127:0]
busB[127:0]
key[127:0]
busR[127:0]
busULA[127:0]
busAES[127:0]
wr_control
valid_AES
wr_amba
wr_control
enable_amba
data_in[31:0]
addr[31:0]
strb[3:0]
data_out[31:0]
reg_dest[1:0]
busR[127:0]
r0[127:0]
r1[127:0]
r2[127:0]
key[127:0]
r3[31:0]
reg_conf[127:0]
mode[2:0]
register[0:17][31:0]
register[0][31:0]
register[1][31:0]
register[2][31:0]
register[3][31:0]
register[4][31:0]
register[5][31:0]
register[6][31:0]
register[7][31:0]
register[8][31:0]
register[9][31:0]
register[10][31:0]
register[11][31:0]
register[12][31:0]
register[13][31:0]
register[14][31:0]
register[15][31:0]
register[16][31:0]
register[17][31:0]
8000_0000
0000_0044
0000_0000
0011_2233_4455_6677_8899_aabb_ccdd_eeff
69c4_e0d8_6a7b_0430_d8cd_b780_70b4_c55a
0e8
0e0
0001_0203_0405_0607_0809_0a0b_0c0d_0e0f
ECB
0c0d_0e0f
0809_0a0b
0405_0607
0001_0203
ccdd_eeff
8899_aabb
4455_6677
0011_2233
70b4_c55a
d8cd_b780
6a7b_0430
69c4_e0d8
Wave.1
tb_top_aes.aes.busAES[127:0] 128'h69c4_e0d8_6a7b_0430_d8cd_b780_70b4_c55a
tb_top_aes.aes.reg_file
N/A
N/A

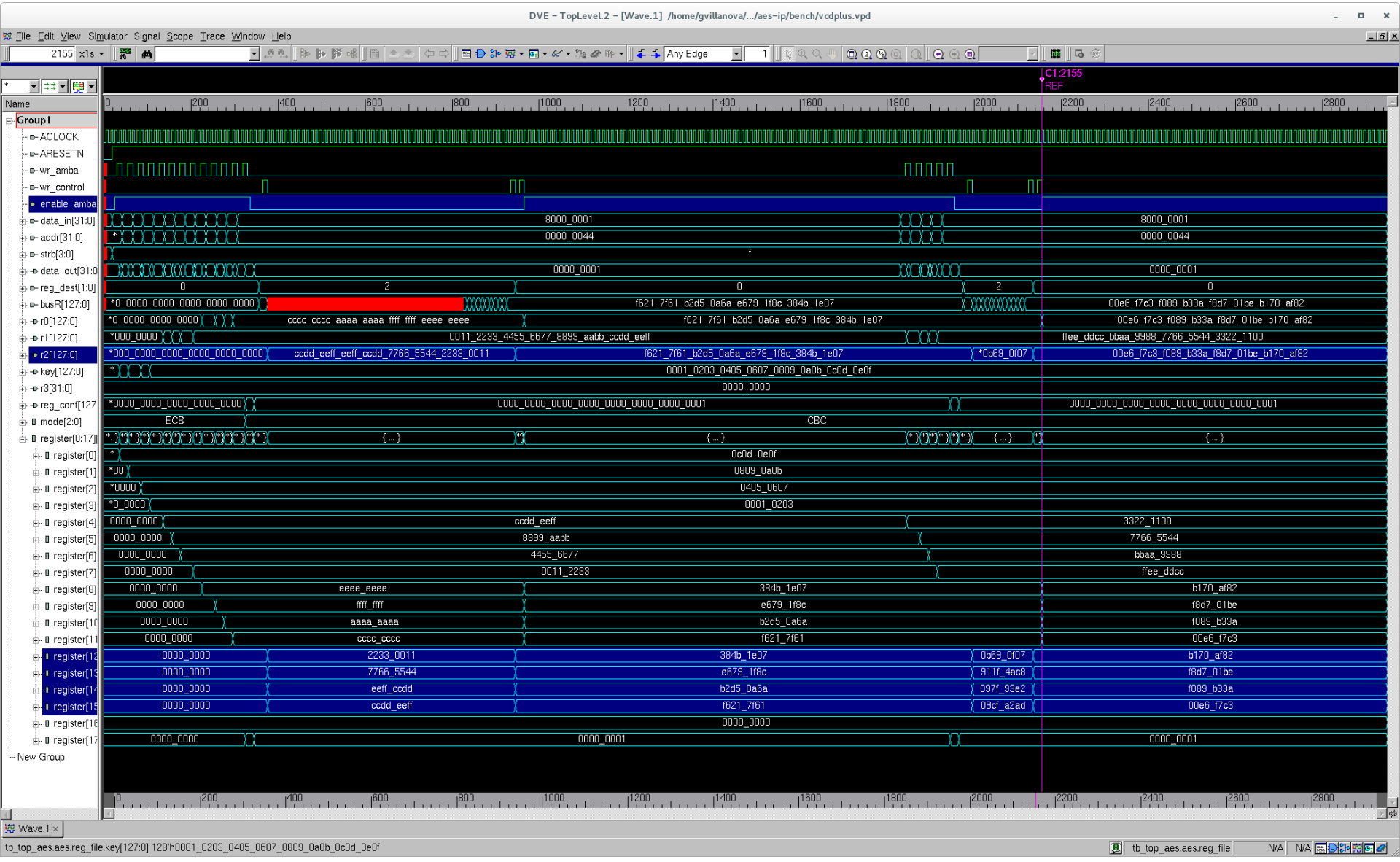
- Testes iniciais e resultados
  - **Decriptação em modo ECB**

```
42      initial begin
43          $vcdpluson;
44          $vcdplusmemon;
45
46          // key    = 00010203_04050607_08090a0b_0c0d0e0f
47          // block  = 00112233_44556677_8899aabb_ccddeeff
48          // cipher = 69c4e0d8_6a7b0430_d8cdb780_70b4c55a
49
50          reset();
51
52          // ** Write KEY, Block and Reg Conf (mode ECB) ** //
53          write_key(128'h00010203_04050607_08090a0b_0c0d0e0f);
54          write_block(128'h69c4e0d8_6a7b0430_d8cdb780_70b4c55a);
55          write_reg_conf({1'b1,26'b0,1'b0,1'b1,3'b000});
56
57          // ** Fim simulacao ** //
58          #1000
59          $finish;
60      end
```


DVE – TopLevel.2 – [Wave.1] /home/gvillanova/.../aes-ip/bench/vcdplus.vpd
File Edit View Simulator Signal Scope Trace Window Help
Name
Group2
ACLK
ARSTn
wr_amba
strb[3:0]
data_in[31:0]
addr[31:0]
data_out[31:0]
r0[127:0]
r1[127:0]
r2[127:0]
r3[31:0]
reg_conf[31:0]
control_word[10:0]
busA[127:0]
busB[127:0]
key[127:0]
busR[127:0]
busULA[127:0]
busAES[127:0]
wr_control
valid_AES
wr_amba
wr_control
enable_amba
data_in[31:0]
addr[31:0]
strb[3:0]
data_out[31:0]
reg_dest[1:0]
busR[127:0]
r0[127:0]
r1[127:0]
r2[127:0]
key[127:0]
r3[31:0]
reg_conf[127:0]
mode[2:0]
register[0:17][31:0]
register[0][31:0]
register[1][31:0]
register[2][31:0]
register[3][31:0]
register[4][31:0]
register[5][31:0]
register[6][31:0]
register[7][31:0]
register[8][31:0]
register[9][31:0]
register[10][31:0]
register[11][31:0]
register[12][31:0]
register[13][31:0]
register[14][31:0]
register[15][31:0]
register[16][31:0]
register[17][31:0]
C1:3
REF
ECB
Wave.1
tb_top_aes.aes.wr_control 1'b0
tb_top_aes.aes.reg_file

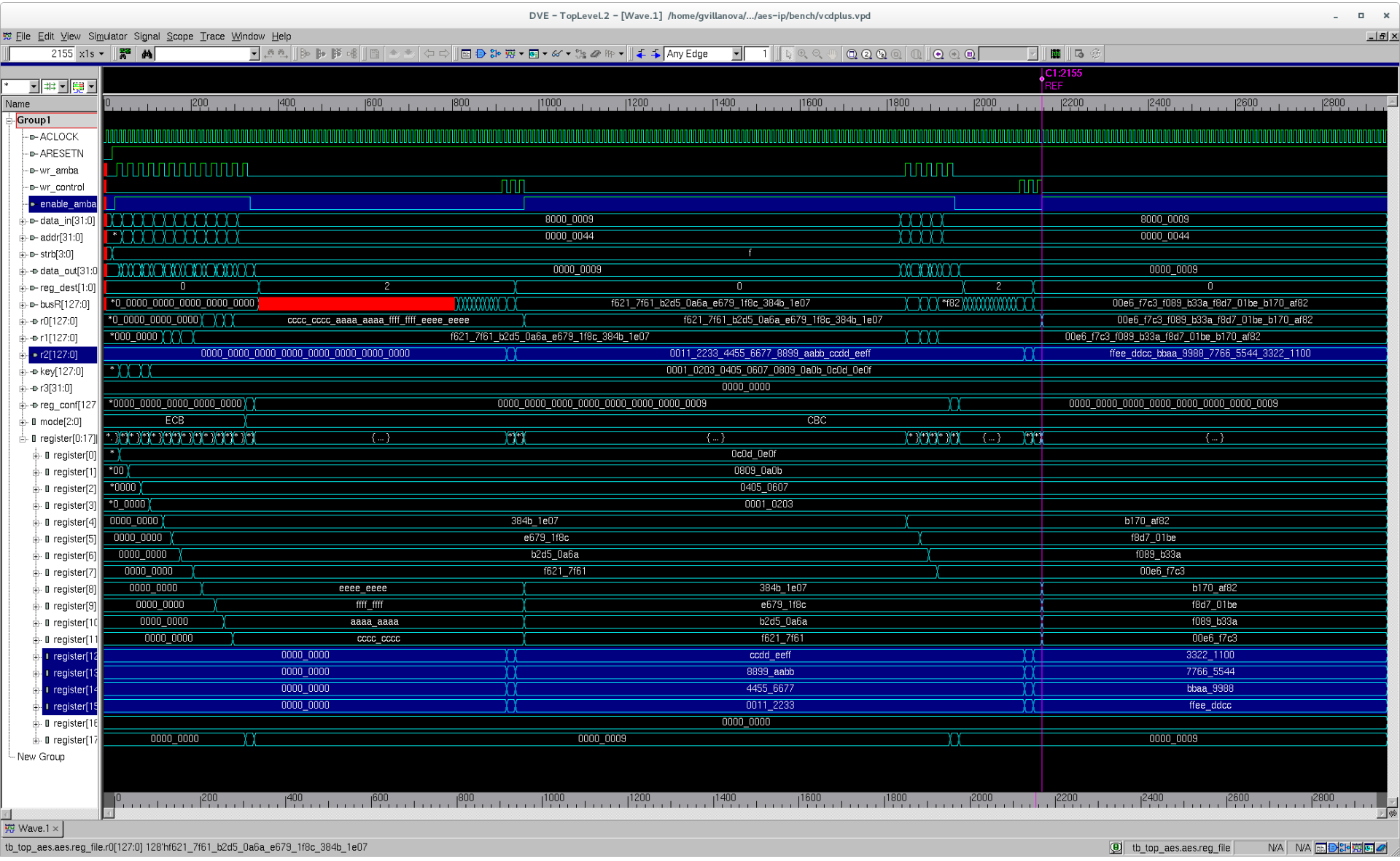
- Testes iniciais e resultados
  - **Encriptação em modo CBC**

```
42      initial begin
43          $vcdpluson;
44          $vcdplusmemon;
45
46          // key     = 00010203_04050607_08090a0b_0c0d0e0f
47          // data1   = 00112233_44556677_8899aabb_ccddeeff
48          // cipher1 = 69c4e0d8_6a7b0430_d8cdb780_70b4c55a
49          // data2   = FFEEDDCC_BBAA9988_77665544_33221100
50          // cipher2 = 00E6F7C3_F089B33A_F8D701BE_B170AF82
51
52          reset();
53
54          // ** Write KEY, Block and Reg Conf (mode CBC) data1 ** //
55          write_key(128'h00010203_04050607_08090a0b_0c0d0e0f);
56          write_block(128'h00112233_44556677_8899aabb_ccddeeff);
57          write_iv(128'hcccccccc_aaaaaaaa_ffffffff_eeeeeeee);
58          write_reg_conf({1'b1,26'b0,1'b0,1'b0,3'b001});
59
60          // ** Write Block and Reg Conf (mode CBC) data2 ** //
61          #1500
62          write_block(128'hFFEEDDCC_BBAA9988_77665544_33221100);
63          write_reg_conf({1'b1,26'b0,1'b0,1'b0,3'b001});
64
65          // ** Fim simulacao ** //
66          #1000
67          $finish;
68      end
```


DVE – TopLevel.2 – [Wave.1] /home/gvillanova/.../aes-ip/bench/vcdplus.vpd
File Edit View Simulator Signal Scope Trace Window Help
C1:2155
REF
Name
Group1
ACLOCK
ARESETN
wr_amba
wr_control
enable_amba
data_in[31:0]
addr[31:0]
strb[3:0]
data_out[31:0]
reg_dest[1:0]
busR[127:0]
r0[127:0]
r1[127:0]
r2[127:0]
key[127:0]
r3[31:0]
reg_conf[127
mode[2:0]
register[0:17]
register[0]
register[1]
register[2]
register[3]
register[4]
register[5]
register[6]
register[7]
register[8]
register[9]
register[10]
register[11]
register[12]
register[13]
register[14]
register[15]
register[16]
register[17]
New Group
8000_0001
0000_0044
f
0000_0001
f621_7f61_b2d5_0a6a_e679_1f8c_384b_1e07
00e6_f7c3_f089_b33a_f8d7_01be_b170_af82
cccc_cccc_aaaa_aaaa_ffff_ffff_eeee_eeee
0011_2233_4455_6677_8899_aabb_ccdd_eeff
ffee_ddcc_bbaa_9988_7766_5544_3322_1100
ccdd_eeff_eeff_ccdd_7766_5544_2233_0011
0b69_0f07
0001_0203_0405_0607_0809_0a0b_0c0d_0e0f
0000_0000
0000_0000_0000_0000_0000_0000_0000_0001
ECB
CBC
{...}
0c0d_0e0f
0809_0a0b
0405_0607
0001_0203
ccdd_eeff
3322_1100
8899_aabb
7766_5544
4455_6677
bbaa_9988
0011_2233
ffee_ddcc
eeee_eeee
384b_1e07
b170_af82
ffff_ffff
e679_1f8c
f8d7_01be
aaaa_aaaa
b2d5_0a6a
f089_b33a
cccc_cccc
f621_7f61
00e6_f7c3
2233_0011
911f_4ac8
7766_5544
eeff_ccdd
097f_93e2
09cf_a2ad
Wave.1
tb_top_aes.aes.reg_file.key[127:0] 128'h0001_0203_0405_0607_0809_0a0b_0c0d_0e0f
tb_top_aes.aes.reg_file
N/A

- Testes iniciais e resultados
  - **Decriptação em modo CBC**

```
42      initial begin
43          $vcdpluson;
44          $vcdplusmemon;
45
46          // key      = 00010203_04050607_08090a0b_0c0d0e0f
47          // data1    = F6217F61_B2D50A6A_E6791F8C_384B1E07
48          // data2    = 00E6F7C3_F089B33A_F8D701BE_B170AF82
49
50          reset();
51
52          // ** Write KEY, Block and Reg Conf (mode CBC) data1 ** //
53          write_key(128'h00010203_04050607_08090a0b_0c0d0e0f);
54          write_block(128'hF6217F61_B2D50A6A_E6791F8C_384B1E07);
55          write_iv(128'hcccccccc_aaaaaaaa_ffffffff_eeeeeeee);
56          write_reg_conf({1'b1,26'b0,1'b0,1'b1,3'b001});
57
58          // ** Write Block and Reg Conf (mode CBC) data2 ** //
59          #1500
60          write_block(128'h00E6F7C3_F089B33A_F8D701BE_B170AF82);
61          write_reg_conf({1'b1,26'b0,1'b0,1'b1,3'b001});
62
63          // ** Fim simulacao ** //
64          #1000
65          $finish;
66      end
```


DVE – TopLevel.2 – [Wave.1] /home/gvillanova/.../aes-ip/bench/vcdplus.vpd
File Edit View Simulator Signal Scope Trace Window Help
Any Edge
C1:2155
REF
Name
Group1
ACLOCK
ARESETN
wr_amba
wr_control
enable_amba
data_in[31:0]
addr[31:0]
strb[3:0]
data_out[31:0]
reg_dest[1:0]
busR[127:0]
r0[127:0]
r1[127:0]
r2[127:0]
key[127:0]
r3[31:0]
reg_conf[127
mode[2:0]
register[0:17]
register[0]
register[1]
register[2]
register[3]
register[4]
register[5]
register[6]
register[7]
register[8]
register[9]
register[10]
register[11]
register[12]
register[13]
register[14]
register[15]
register[16]
register[17]
New Group
8000_0009
0000_0044
f
0000_0009
f621_7f61_b2d5_0a6a_e679_1f8c_384b_1e07
00e6_f7c3_f089_b33a_f8d7_01be_b170_af82
cccc_cccc_aaaa_aaaa_ffff_ffff_eeee_eeee
0000_0000_0000_0000_0000_0000_0000_0000
0011_2233_4455_6677_8899_aabb_ccdd_eeff
ffee_ddcc_bbaa_9988_7766_5544_3322_1100
0001_0203_0405_0607_0809_0a0b_0c0d_0e0f
ECB
CBC
0c0d_0e0f
0809_0a0b
0405_0607
0001_0203
384b_1e07
b170_af82
e679_1f8c
f8d7_01be
b2d5_0a6a
f089_b33a
f621_7f61
00e6_f7c3
eeee_eeee
ffff_ffff
aaaa_aaaa
cccc_cccc
ccdd_eeff
3322_1100
8899_aabb
7766_5544
4455_6677
bbaa_9988
0011_2233
ffee_ddcc
Wave.1
tb_top_aes.aes.reg_file.r0[127:0] 128'hf621_7f61_b2d5_0a6a_e679_1f8c_384b_1e07
tb_top_aes.aes.reg_file
N/A
N/A

- O que falta?
  - Testar e depurar os outros modos de operações
  - Integrar o AMBA ao circuito atual
  - Testar o circuito com o AMBA
  - Passar para o teste em UVM

- Verificação do IP
  - Modelo de referência
    - Objetivos
      - Criar um software que implemente o AES e seus modos de encriptação e decriptação
      - Criar o modelo de referência (UVM) usando o software desenvolvido

- Verificação do IP
  - Modelo de referência
    - Software em C++
      - Foi criado um software que usa a biblioteca **cryptopp** como base para criação de uma API mais adaptada à necessidade
      - Os métodos atuais desenvolvidos dessa API são:
        - void **setKey**(byte *);
        - void **setPlainText**(byte *);
        - void **setCipher**(byte *);
        - void **encrypt**();
        - void **decrypt**();
        - byte* **getKey**();
        - byte* **getPlainText**();
        - byte* **getCipher**();
        - byte* **getDecrypted**();

- Verificação do IP
  - Modelo de referência
    - Resultados

Usando a API criada foi desenvolvida a função main que implementa os modos de operação usados no hardware, que apresentou resultados coerentes como mostrado na figura ao lado

```
[gvillanova@dione refmod]$ ./prog
data1 : 00112233445566778899AABBCCDDEEFF
data2 : FFEEDDCCBBAA99887766554433221100
key : 000102030405060708090A0B0C0D0E0F
IV : CCCCCCCCAAAAAAAAFFFFFFFFEEEEEEEE

ECB MODE
first cipher block : 69C4E0D86A7B0430D8CDB78070B4C55A
second cipher block : 1B872378795F4FFD772855FC87CA964D
first decrypted block : 00112233445566778899AABBCCDDEEFF
second decrypted block : FFEEDDCCBBAA99887766554433221100

CBC MODE
first cipher block : F6217F61B2D50A6AE6791F8C384B1E07
second cipher block : 00E6F7C3F089B33AF8D701BEB170AF82
first decrypted block : 00112233445566778899AABBCCDDEEFF
second decrypted block : FFEEDDCCBBAA99887766554433221100

PCBC MODE
first cipher block : F6217F61B2D50A6AE6791F8C384B1E07
second cipher block : 1766EA65883AE0BE5DE323B1431CBD54
first decrypted block : 00112233445566778899AABBCCDDEEFF
second decrypted block : FFEEDDCCBBAA99887766554433221100

CFB MODE
first cipher block : 79C571F93E6E91590576009881A3AB8E
second cipher block : 3F778AF1BA19E580C751137195BCFF23
first decrypted block : 00112233445566778899AABBCCDDEEFF
second decrypted block : FFEEDDCCBBAA99887766554433221100

OFB MODE
first cipher block : 79C571F93E6E91590576009881A3AB8E
second cipher block : 03219503DD5973187FADC74474E3F047
first decrypted block : 00112233445566778899AABBCCDDEEFF
second decrypted block : FFEEDDCCBBAA99887766554433221100

CTR MODE
first cipher block : 79C571F93E6E91590576009881A3AB8E
second cipher block : B67227E386B21BBD7B374B8A2A404481
first decrypted block : 00112233445566778899AABBCCDDEEFF
second decrypted block : FFEEDDCCBBAA99887766554433221100
```

- Verificação do IP
  - Modelo de referência
    - O que falta?
      - Terminar a API criando os métodos feitos na função main
      - Testar e validar o software
      - Desenvolver o modelo de referência

- Verificação do IP
  - UVM
    - Objetivos
      - Desenvolver um testbench em UVM para o IP
      - Testar todos os modos de operação do IP de forma automática
      - Elaborar o plano de cobertura
      - Validar o IP

- Verificação do IP
  - UVM
    - O que foi desenvolvido?
      – Atualmente a equipe está executando os exemplos disponíveis
      – Está sendo criado uma metodologia de uso da UVM que servirá como base para criar o teste em UVM para o IP

Obrigado!

Contact

Angelo Perkusich, D.Sc.
Professor, CEO
angelo.perkusich@embedded.ufcg.edu.br
+55 83 8811.9545

Hyggo Almeida, D.Sc.
Professor, CTO
hyggo.almeida@embedded.ufcg.edu.br
+55 83 8875.1894

Gabriel Villanova
Aluno, DEE
gabriel.magalhaes@embedded.ufcg.edu.br
+55 87 98866.2012