AEP Project: PRESENT Block Cipher

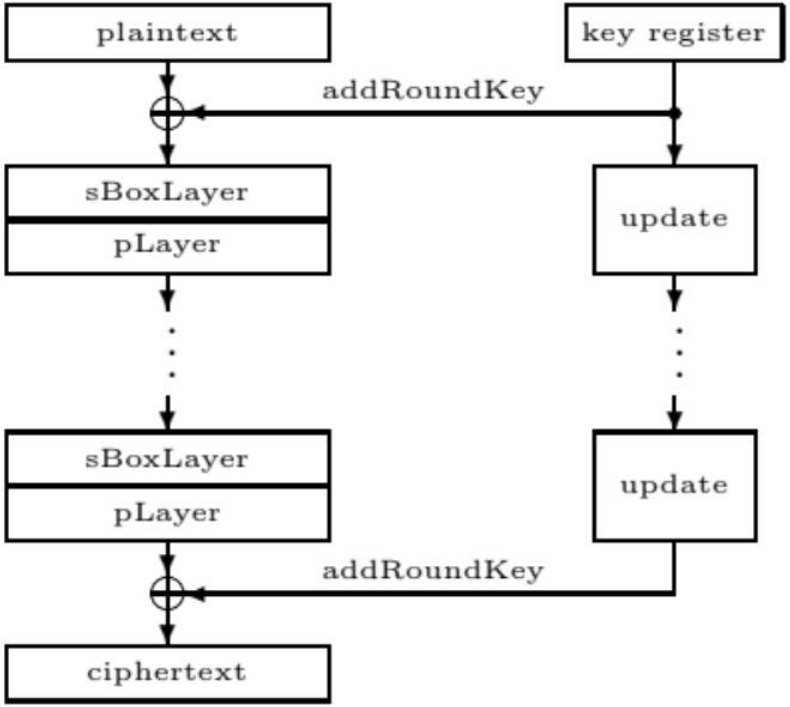
TEAM MEMBERS	STUDENT ID
Marius-Mihail Gurgu	453084
Alexandre Thomas Janin	454457
Tamil Selvi Pandiyan	453060
Matteo Spallanzani	454451
Wei-Heng Ke	454447

Table of Contents

PRESENT Overview

- Standardized by ISO in 2012
- 64-bit blocks processed with 80 or 128 bit keys
- Good level of security
- Small amount of resources needed

Structure


plaintext
key register
addRoundKey
sBoxLayer
pLayer
update
sBoxLayer
pLayer
update
addRoundKey
ciphertext

Bit substitution

Non-linear substitution through 4-bits S-box

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

Bit permutation

Linear permutation with the following order

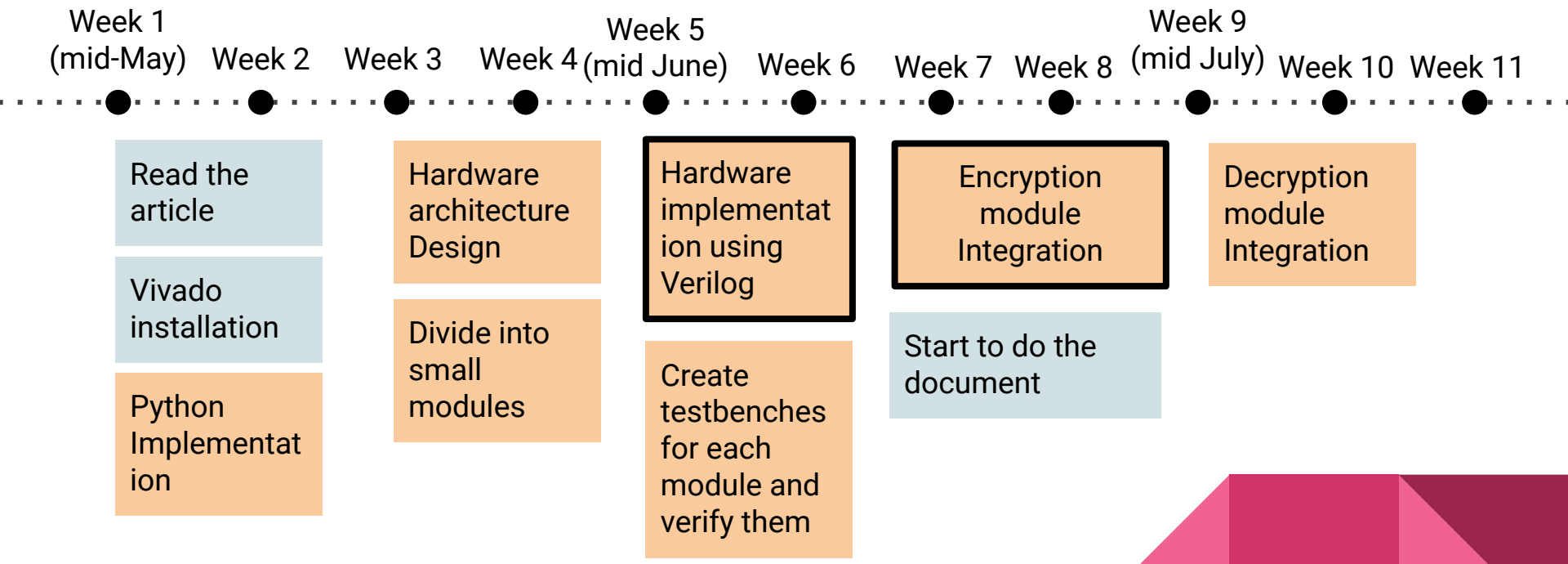
P	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
i	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
P	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
i	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
P	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
i	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62
P	48	49	50	51	52	53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

Motivation

- Adequate size
- Popularity makes research easy
- We liked it

Working Process

Technical part + Organization part



pyPresent.py

```
39
40  class Present:
41      def __init__(self, key, rounds=32):
42          """Create a PRESENT cipher object
43
44          key:    the key as a 128-bit or 80-bit rawstring
45          rounds: the number of rounds as an integer, 32 by default
46          """
47          self.rounds = rounds
48          if len(key) * 8 == 80:
49              self.roundkeys = generateRoundkeys80(string2number(key), self.rounds)
50          elif len(key) * 8 == 128:
51              self.roundkeys = generateRoundkeys128(string2number(key), self.rounds)
52          else:
53              raise ValueError, "Key must be a 128-bit or 80-bit rawstring"
54
55      def encrypt(self, block):
56          """Encrypt 1 block (8 bytes)
57
58          Input:  plaintext block as raw string
59          Output: ciphertext block as raw string
60          """
61          state = string2number(block)
62          for i in xrange(self.rounds - 1):
63              state = addRoundKey(state, self.roundkeys[i])
64              state = sBoxLayer(state)
65              state = pLayer(state)
66          cipher = addRoundKey(state, self.roundkeys[-1])
67          return number2string_N(cipher, 8)
68
69      def decrypt(self, block):
70          """Decrypt 1 block (8 bytes)
71
72          Input:  ciphertext block as raw string
73          Output: plaintext block as raw string
74          """
```

A part of the reference python code

Data set 1:

Key: 00000000000000000000
Plaintext: 0000000000000000

Roundkey 0 : 0000000000000000
…
Roundkey 31 : 6dab31744f41d700

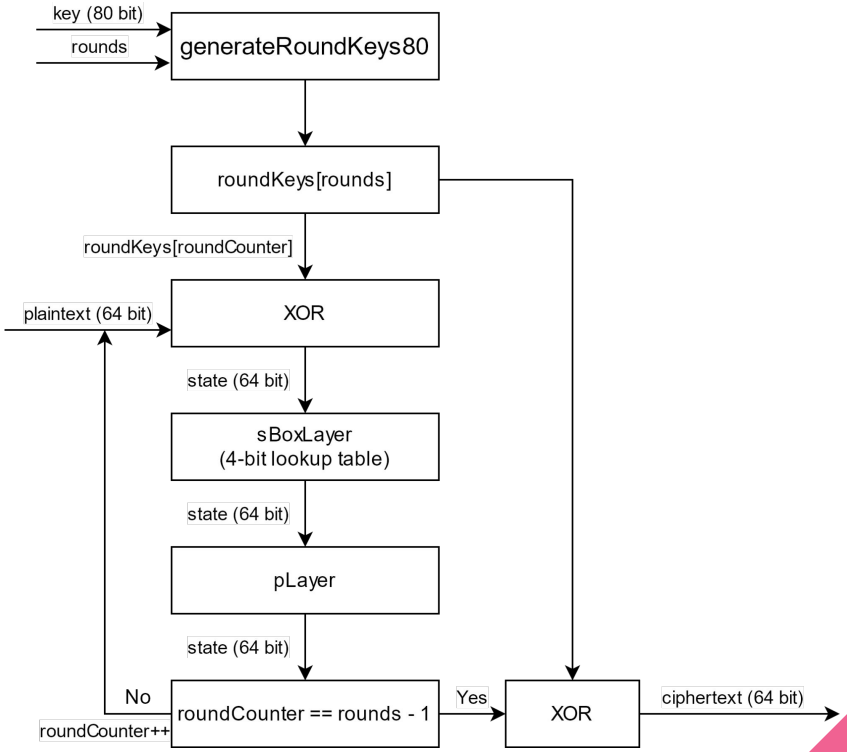
**********Encryption**********:
Round 0
sBoxLayer INPUT: 0000000000000000
sBoxLayer OUTPUT: cccccccccccccccc
pLayer OUTPUT: ffffffff00000000
…
Round 30
sBoxLayer INPUT: c19abfeebafbc168
sBoxLayer OUTPUT: 45ef82118f2845a3
pLayer OUTPUT: 38d2f04c34635345
Ciphertext: 5579c1387b228445

**********Decryption**********:
Round 0
pLayer_dec INPUT: 38d2f04c34635345
pLayer_dec OUTPUT: 45ef82118f2845a3
sBoxLayer_dec OUTPUT: c19abfeebafbc168
…
Round 30
pLayer_dec INPUT: ffffffff00000000
pLayer_dec OUTPUT: cccccccccccccccc
sBoxLayer_dec OUTPUT: 0000000000000000
Decrypted text: 0000000000000000

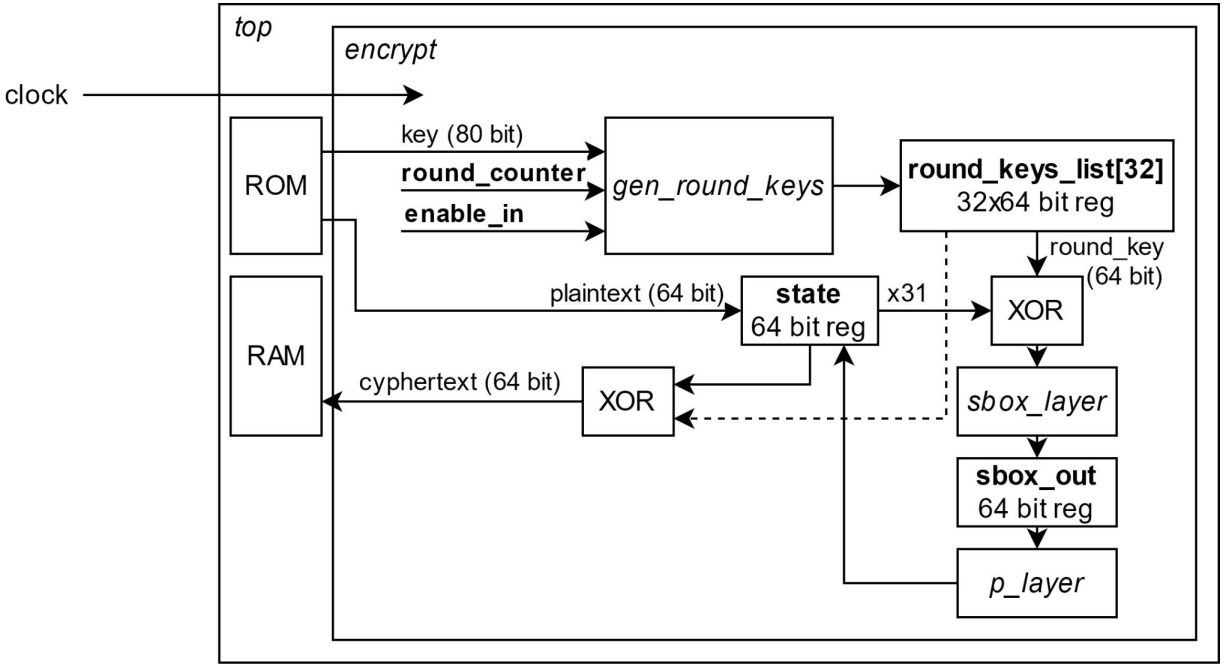
Data set 2…
Data set 3…
Data set 4…
Data set 5…

Hardware Schemes

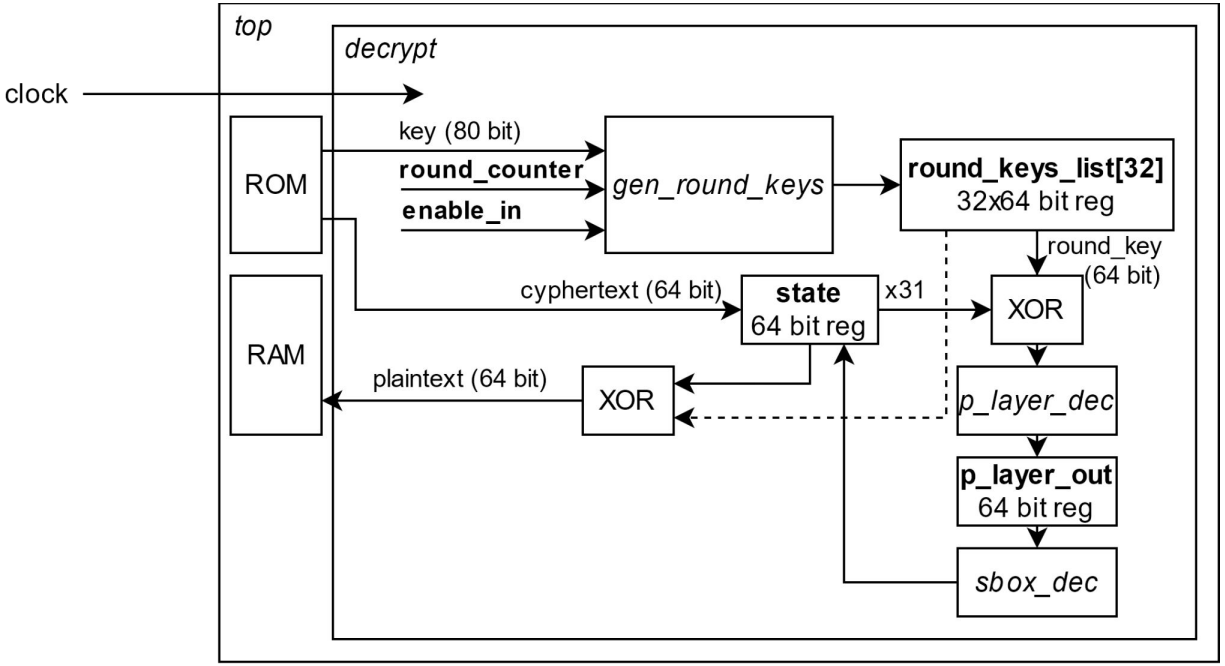
Python flowchart v.s. Hardware schemes



Python flowchart v.s. Hardware schemes



Python flowchart v.s Hardware schemes

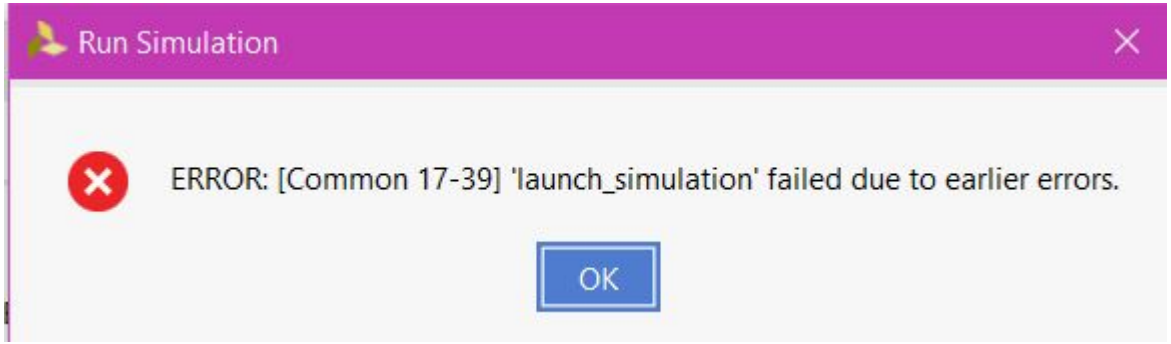


Implementation Challenges and Bugs

A Confusing Bug (Vivado 2020.2)

- Console message:

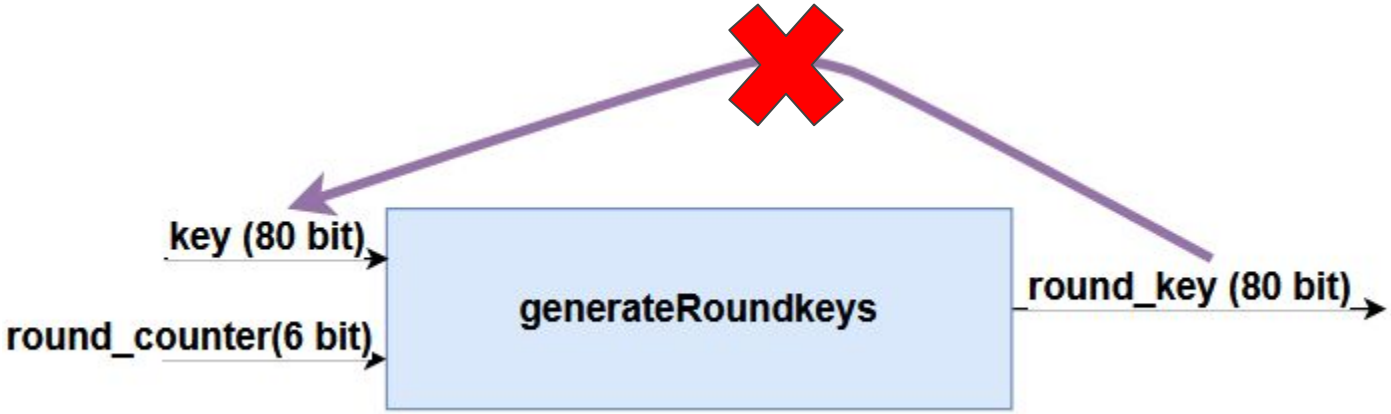
ERROR: [Simulator 45-7] No such file 'F:/Vivado_Projects/aep_project/PRESENT_Cipher_Verilog/decrypt/decrypt.srcs/sources_1/new/decrypt.vF:/Vivado_Projects/aep_project/PRESENT_Cipher_Verilog/decrypt/decrypt.srcs/sources_1/new/decrypt.v' in the design.



What causes the bug?

- Reason: Setting multiple breakpoints
- Tried updating Vivado to v2021.1 -> has no support for our board
- Solution: Delete “TempBreakPointFile.txt”
- Path: F:\Vivado_Projects\aep_project\PRESENT_Cipher_Verilog\decrypt\decrypt.sim\sim_1\behav\xsim\xsim.dir\decrypt_tb_behav

Combinatorial Loop Problem

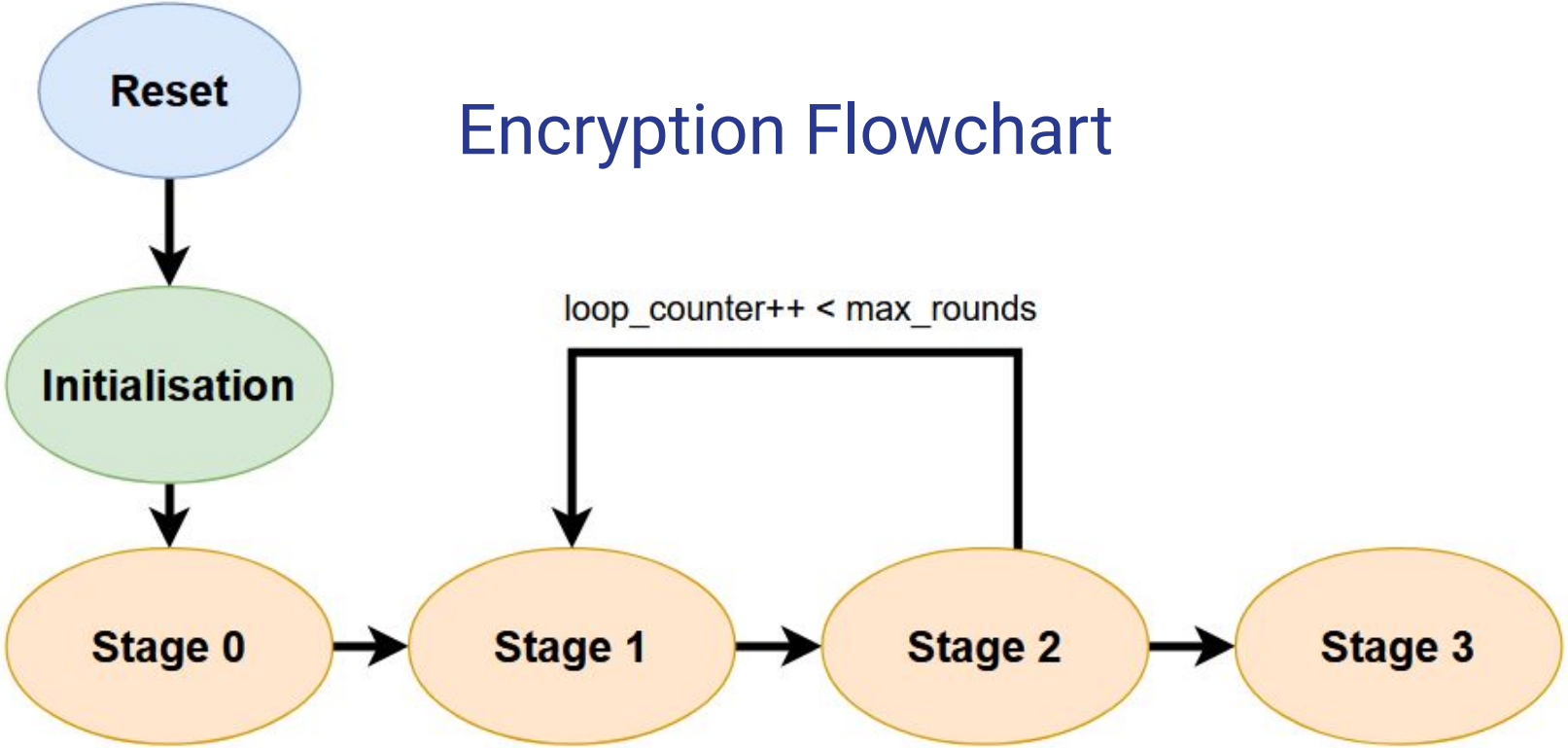


- **Solution: Break the loop by providing the updated key at the input of the module**

```
always @ (round_counter)
    begin: GENERATE
        if (enable_in == 1'b1) begin
            round_out = aux[79:16];
            aux = {aux[18:0], aux[79:19]}; //rotate left by 61 bits
            case (aux[79:76])
                4'h0: aux[79:76] = 4'hc;
                4'h1: aux[79:76] = 4'h5;
                4'h2: aux[79:76] = 4'h6;
                4'h3: aux[79:76] = 4'hb;
                4'h4: aux[79:76] = 4'h9;
                4'h5: aux[79:76] = 4'h0;
                4'h6: aux[79:76] = 4'ha;
                4'h7: aux[79:76] = 4'hd;
                4'h8: aux[79:76] = 4'h3;
                4'h9: aux[79:76] = 4'he;
                4'ha: aux[79:76] = 4'hf;
                4'hb: aux[79:76] = 4'h8;
                4'hc: aux[79:76] = 4'h4;
                4'hd: aux[79:76] = 4'h7;
                4'he: aux[79:76] = 4'h1;
                4'hf: aux[79:76] = 4'h2;
            endcase
            aux[19:15] = aux[19:15] ^ round_counter;
        end
        else begin
            aux = key;
        end
```

```
always @ (round_counter)
    begin: GENERATE
        if (enable_in == 1'b0) begin
            aux = key;
            round_out = aux;
        end
        else begin
            aux = {key[18:0], key[79:19]}; //rotate left by 61 bits
            case (key[18:15])
                4'h0: aux[79:76] = 4'hc;
                4'h1: aux[79:76] = 4'h5;
                4'h2: aux[79:76] = 4'h6;
                4'h3: aux[79:76] = 4'hb;
                4'h4: aux[79:76] = 4'h9;
                4'h5: aux[79:76] = 4'h0;
                4'h6: aux[79:76] = 4'ha;
                4'h7: aux[79:76] = 4'hd;
                4'h8: aux[79:76] = 4'h3;
                4'h9: aux[79:76] = 4'he;
                4'ha: aux[79:76] = 4'hf;
                4'hb: aux[79:76] = 4'h8;
                4'hc: aux[79:76] = 4'h4;
                4'hd: aux[79:76] = 4'h7;
                4'he: aux[79:76] = 4'h1;
                4'hf: aux[79:76] = 4'h2;
            endcase
            aux[19:15] = key[38:34] ^ round_counter;
            round_out = aux;
        end
    end
```

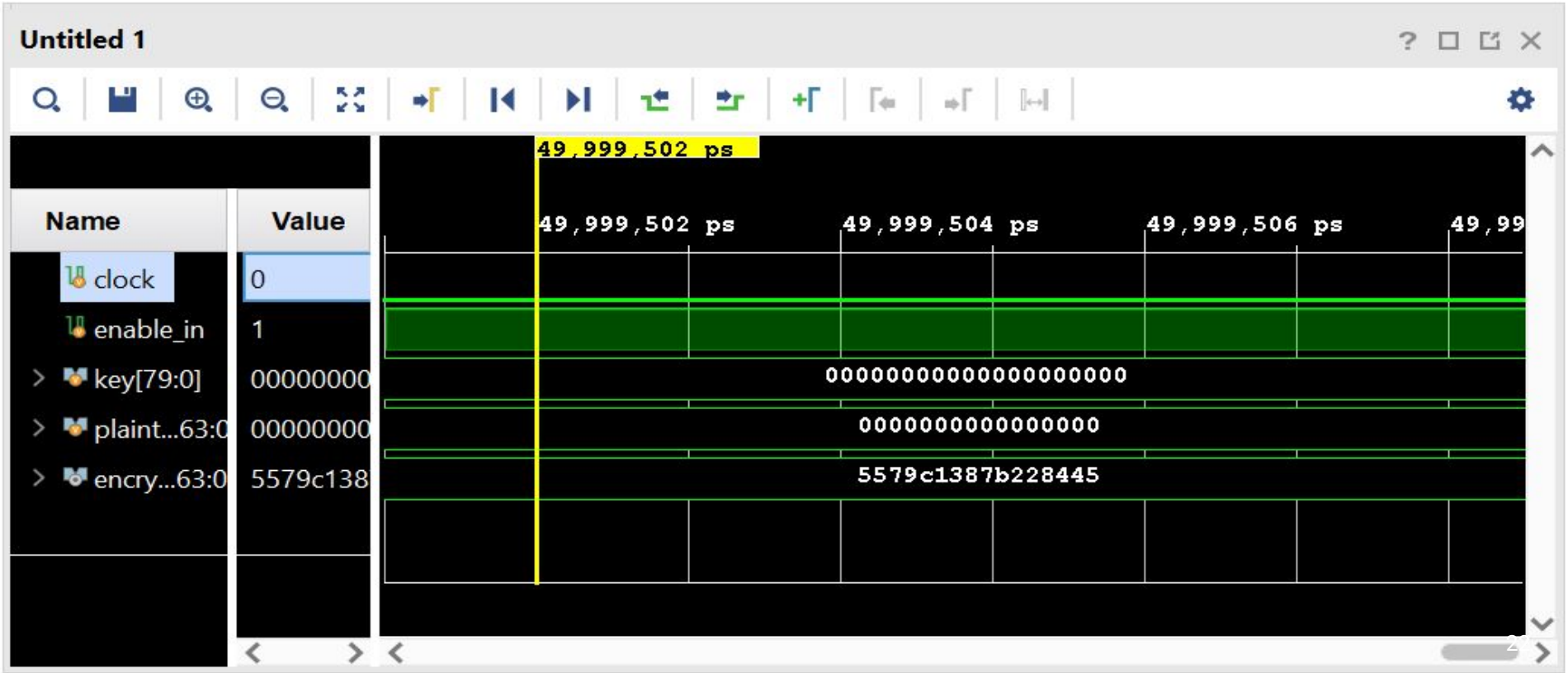
Not a bug, but still a challenge: integrating modules



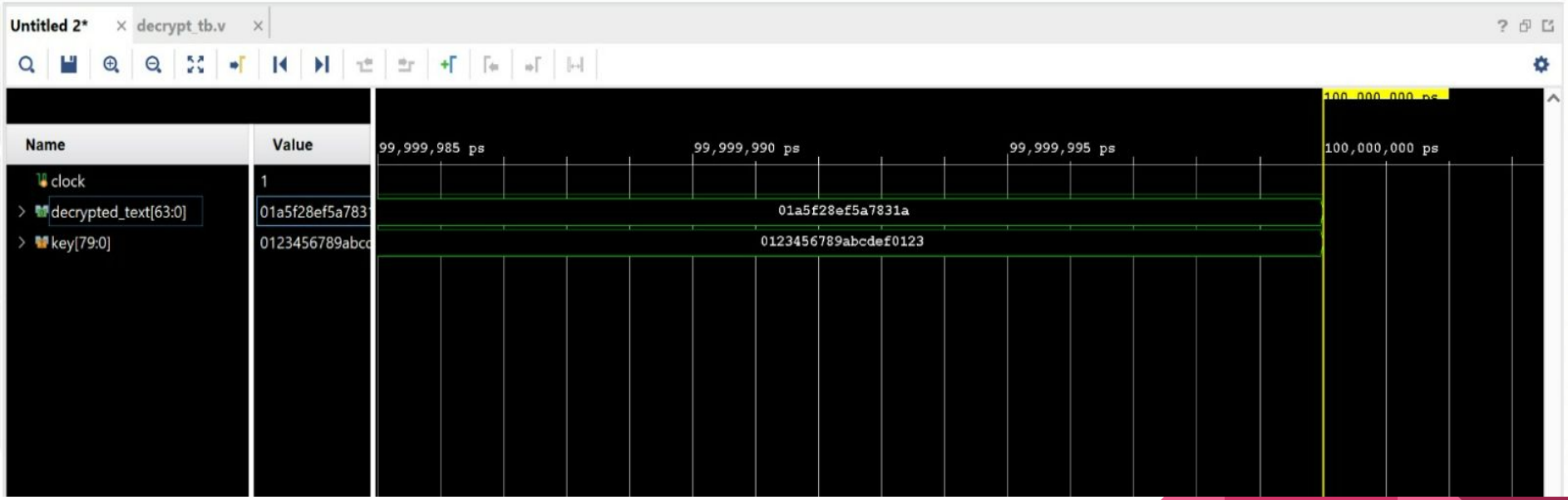
Encryption Flowchart

Vivado Report

Results from Vivado- Encryption



Results from Vivado- Decryption

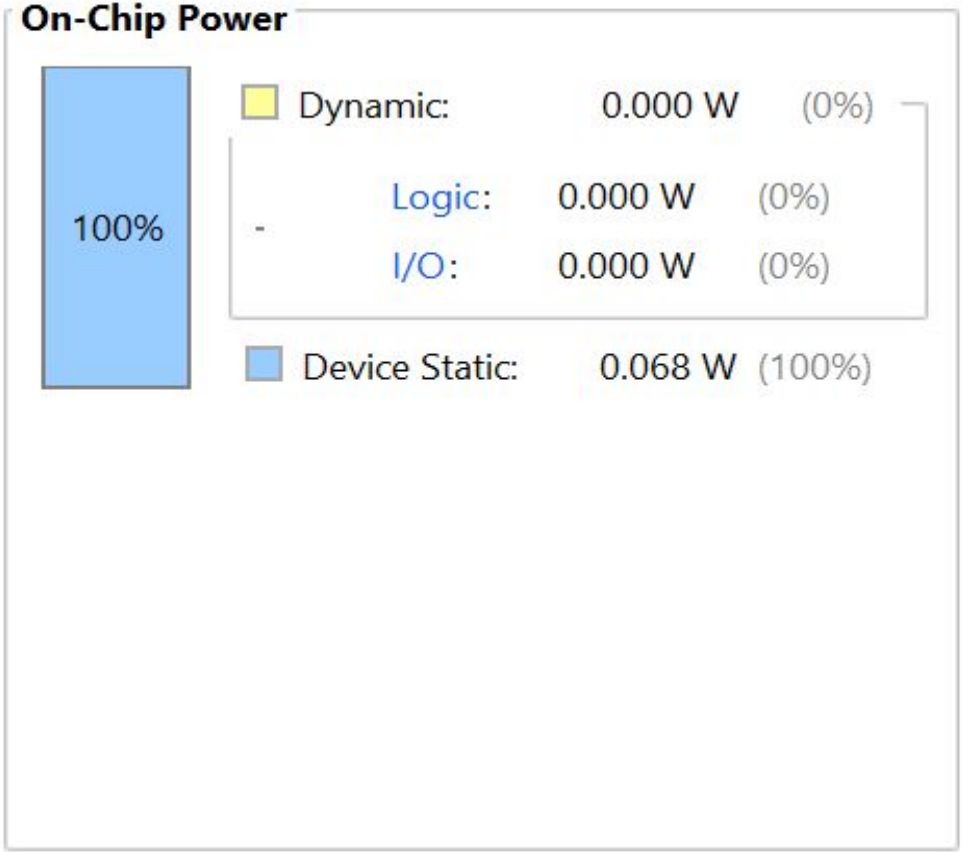


Power consumption- Encryption/decryption

Power analysis from Implemented netlist. Activity derived from constraints files, simulation files or vectorless analysis.

Total On-Chip Power:	**0.068 W**
Design Power Budget:	**Not Specified**
Power Budget Margin:	**N/A**
Junction Temperature:	**25.3°C**
Thermal Margin:	59.7°C (11.9 W)
Effective ϑJA:	5.0°C/W
Power supplied to off-chip devices:	0 W
Confidence level:	High

Launch Power Constraint Advisor to find and fix invalid switching activity



Basys3 ideal power supplies

Supply	Circuits	Device	Current (max/typical)
3.3V	FPGA I/O, USB ports, Clocks, Flash, PMODs	IC10: LTC3633	2A/0.1 to 1.5A
1.0V	FPGA Core	IC10: LTC3633	2A/ 0.2 to 1.3A
1.8V	FPGA Auxiliary and Ram	IC11: LTC3621	300mA/ 0.05 to 0.15A


Thank you!