High-speed Implementation of Authenticated Ciphers Competing in the CAESAR Contest

Abubakr Abdulgadir

Abstract

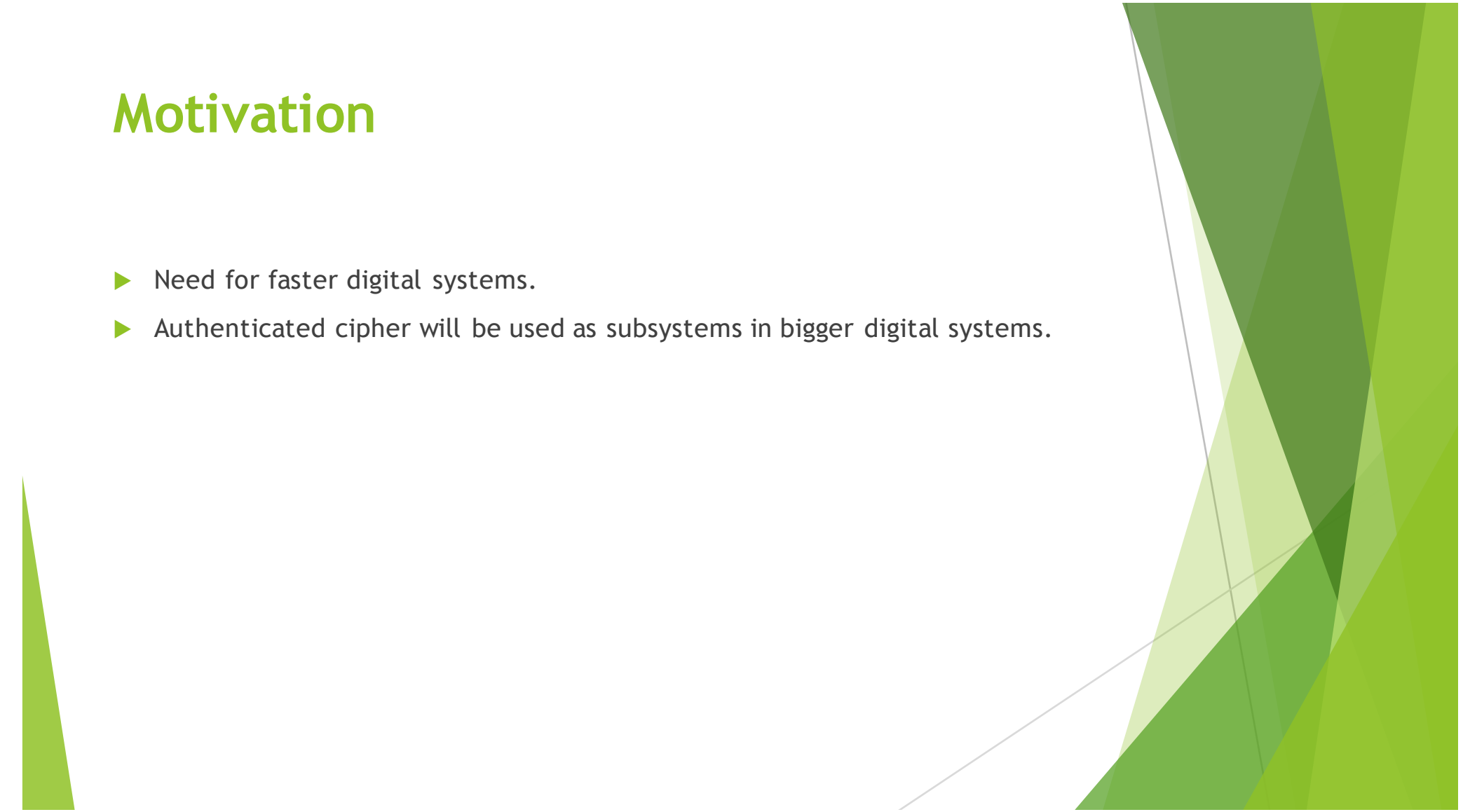
- Authenticated Cipher is a new class of ciphers that offers encryption/decryption and authentication.
- One of the most important criteria to evaluate ciphers is throughput. Throughput is often used as a tie breaker when ciphers offer adequate security.
- Deoxys ≠ 128-128 CAECAR candidate.
- Although the implementation is not complete yet, the work done here can be used to save some time in future work.

Introduction

- CAECAR is a contest aimed to identify a portfolio of authenticated ciphers better than AES-GCM and can be widely adopted.
- Hardware evaluation is the next step in the contest.
- The metrics used for hardware evaluation are: area, throughput, throughput to area ratio and clock rate.
- Of these metrics, Throughput was chosen as a target for optimization in this project

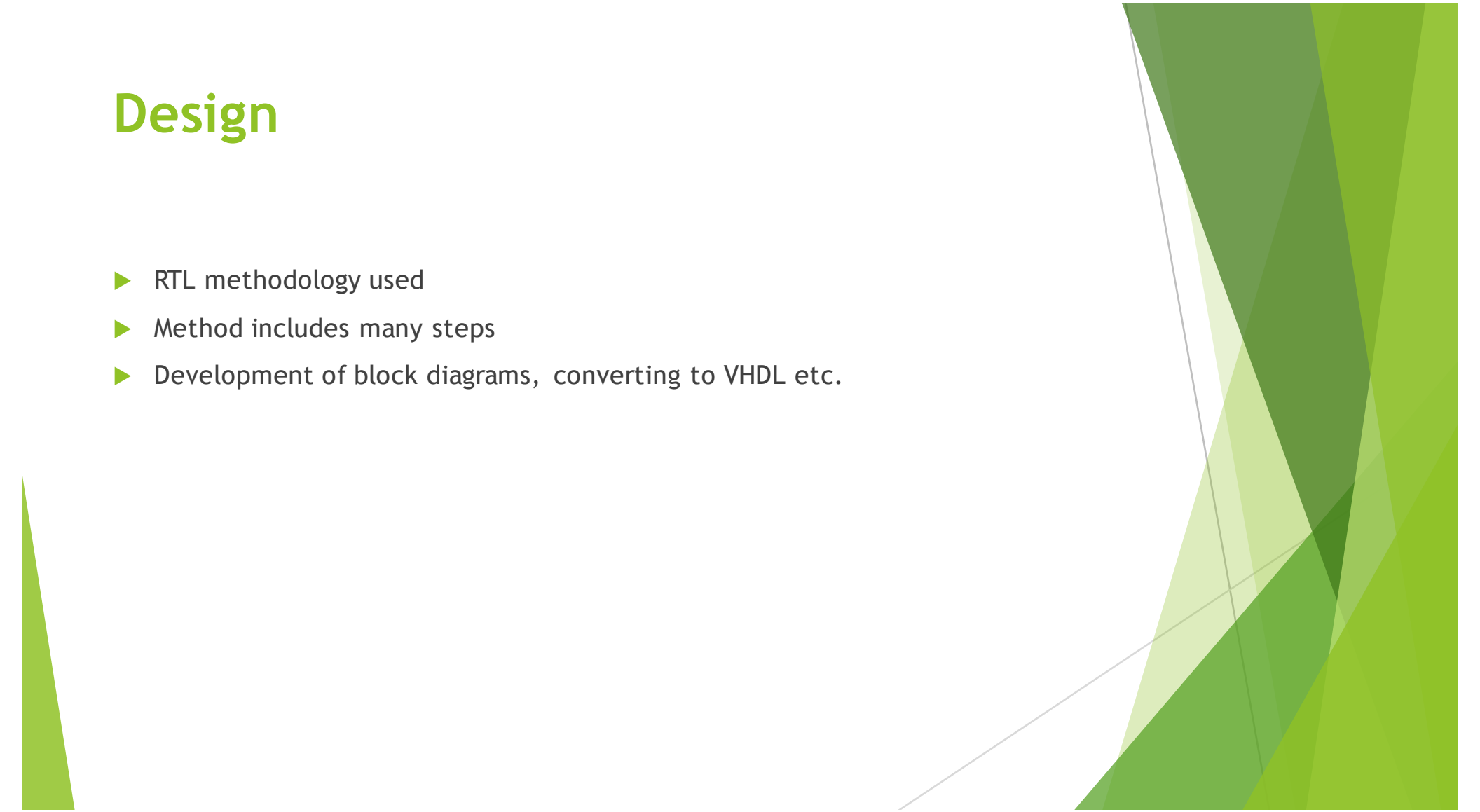
Motivation

- Need for faster digital systems.
- Authenticated cipher will be used as subsystems in bigger digital systems.

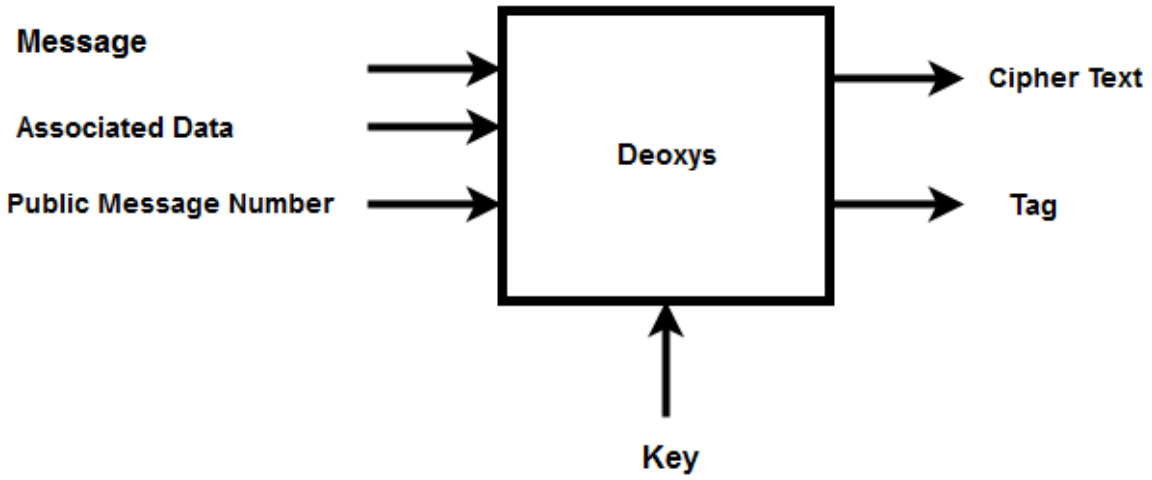


Design

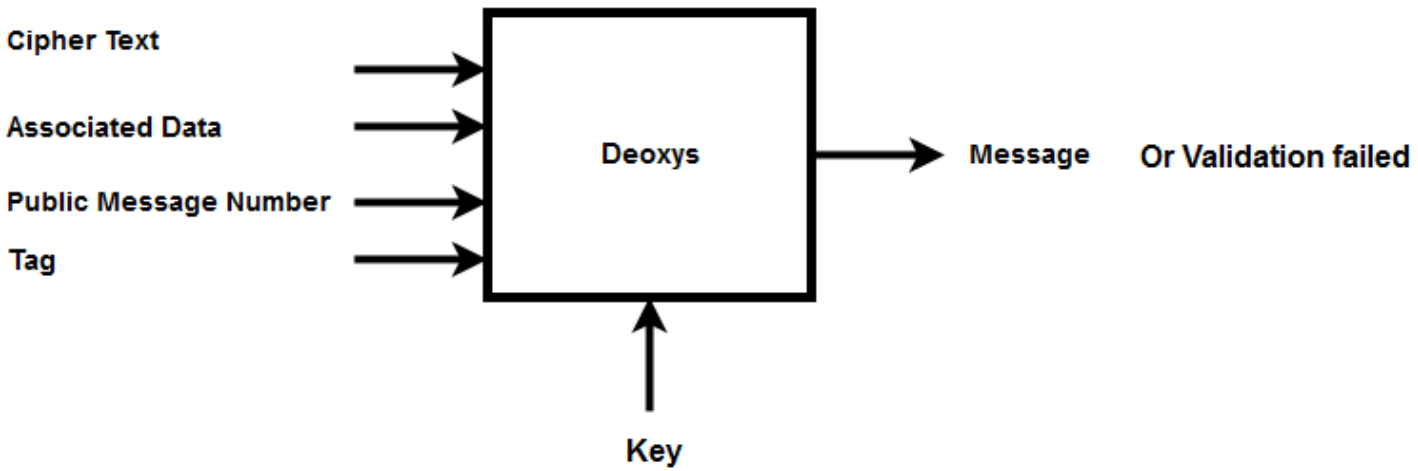
- RTL methodology used
- Method includes many steps
- Development of block diagrams, converting to VHDL etc.



Deoxys - Encryption

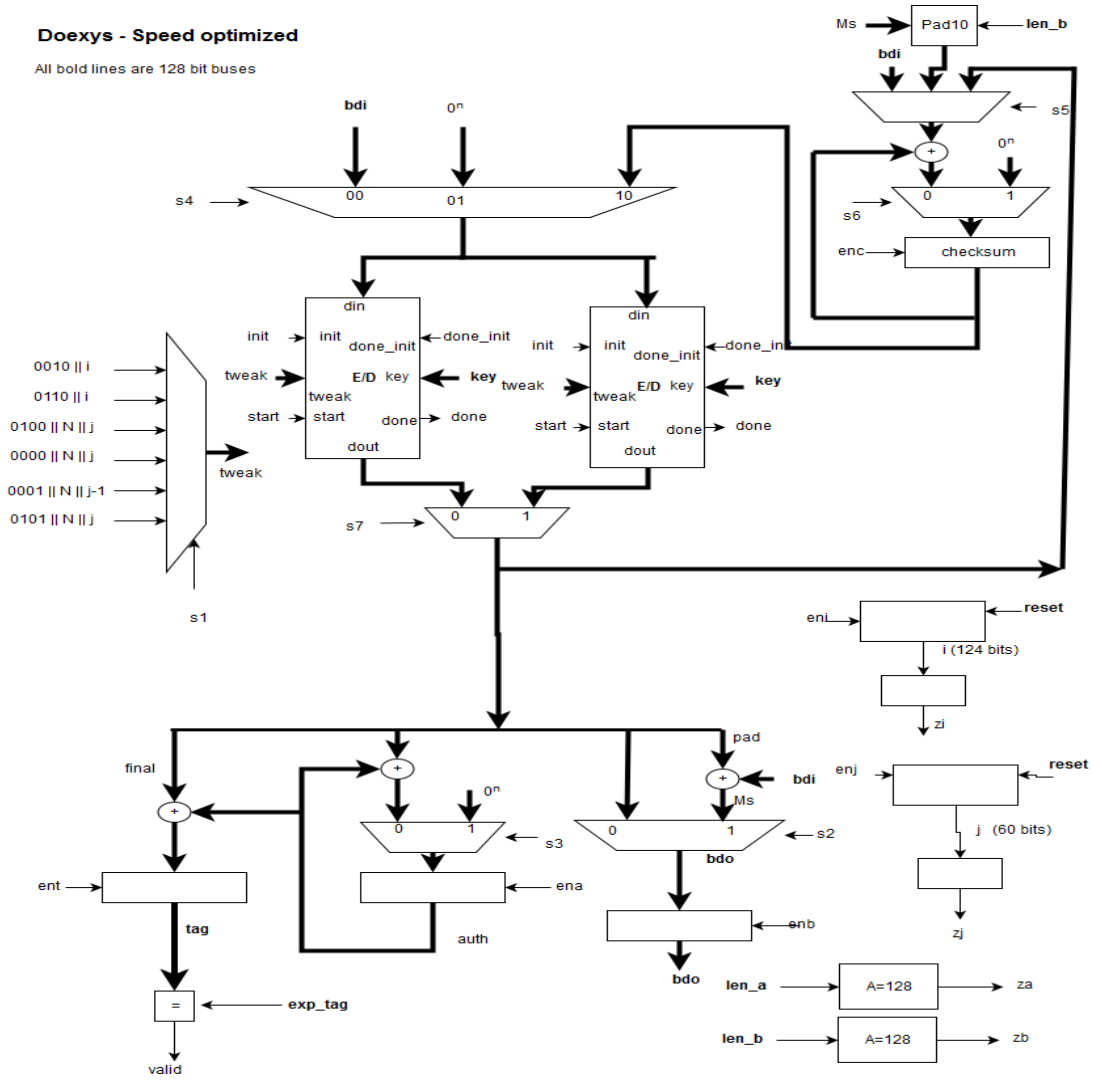


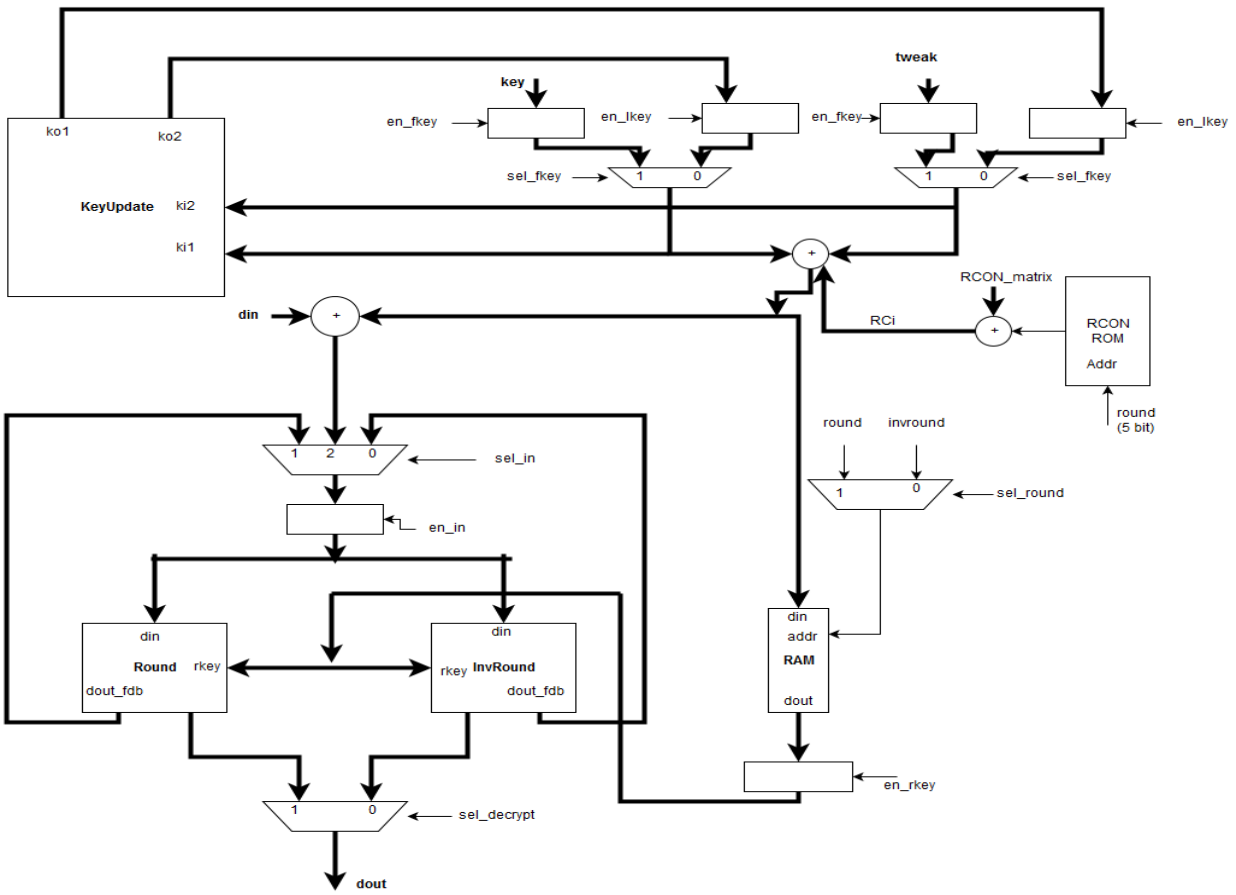
Deoxys – Decryption/ Validation



Tools

- Xilinx ISE
- ISim
- Xilinx SDK
- GMU AETVgen script to generate test vectors.


Doexys - Speed optimized
All bold lines are 128 bit buses
Ms
Pad10
len_b
bdi
s5
0^n
s6
enc
checksum
s4
00
01
10
din
init
done_init
E/D
key
tweak
start
done
dout
0010 || i
0110 || i
0100 || N || j
0000 || N || j
0001 || N || j-1
0101 || N || j
s1
s7
eni
reset
i (124 bits)
zi
pad
final
ent
tag
=
exp_tag
valid
s3
ena
auth
s2
bdo
enb
enj
j (60 bits)
zj
len_a
len_b
A=128
za
zb

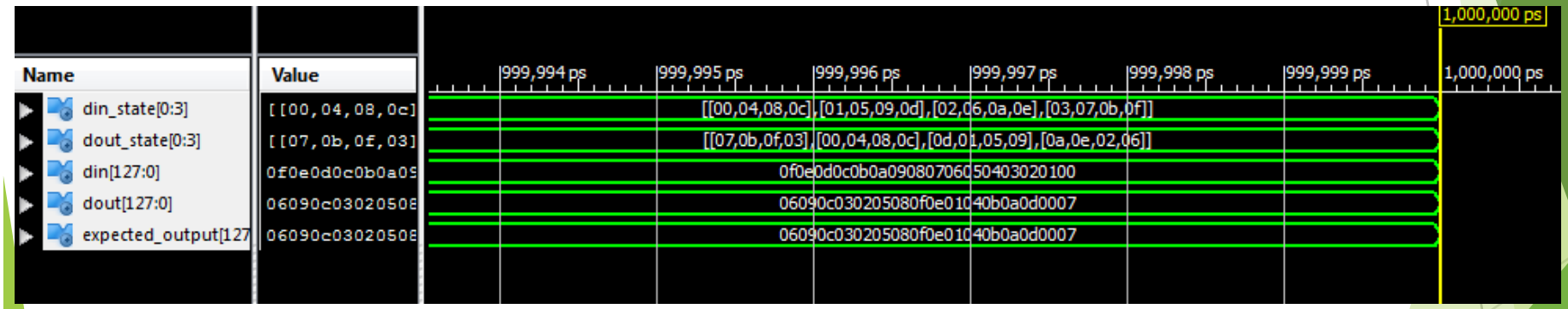

key
tweak
en_fkey
en_lkey
en_fkey
en_lkey
ko1
ko2
KeyUpdate
ki2
ki1
sel_fkey
1
0
1
0
sel_fkey
RCON_matrix
din
RCi
RCON
ROM
Addr
round
(5 bit)
round
invround
1
2
0
sel_in
1
0
sel_round
en_in
din
Round
rkey
dout_fdb
din
rkey
InvRound
dout_fdb
din
addr
RAM
dout
en_rkey
1
0
sel_decrypt
dout

Dexys-BC

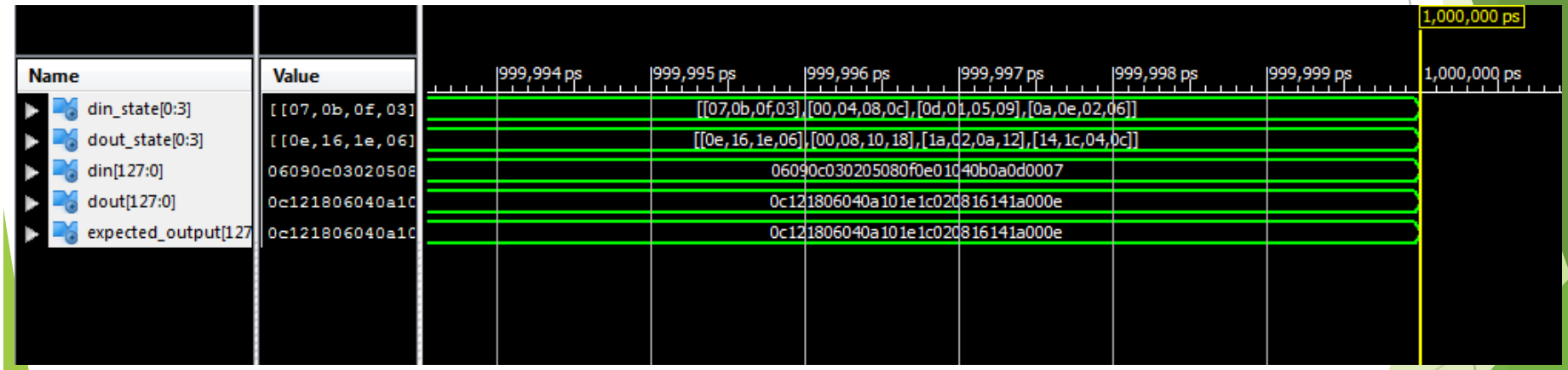
Results and discussion

- Debugging datapath is still in progress.
- Debugged components of key scheduling and they worked successfully.
- Block diagrams can help in future work.

Debugging h function



Debugging g function



?