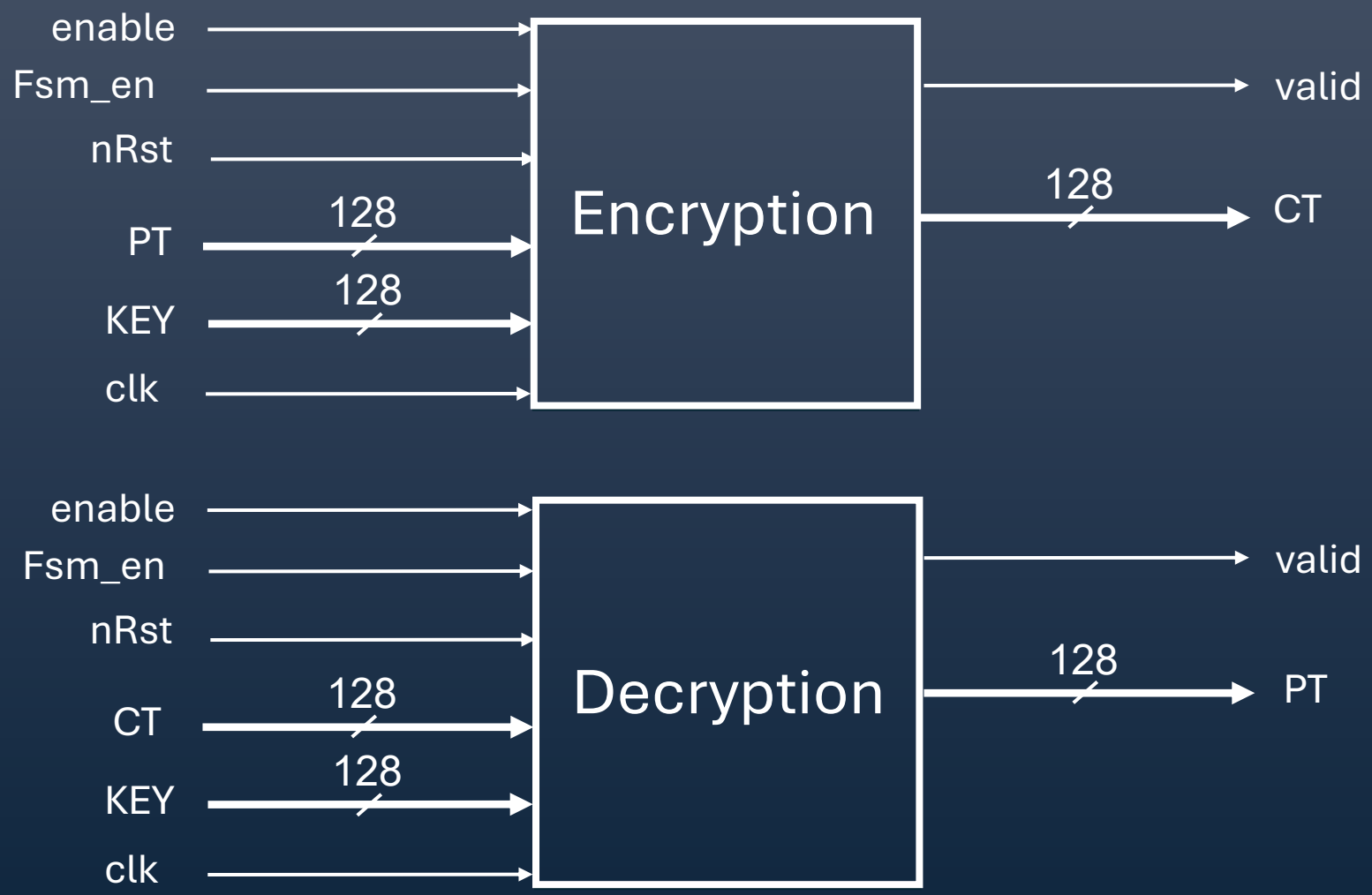
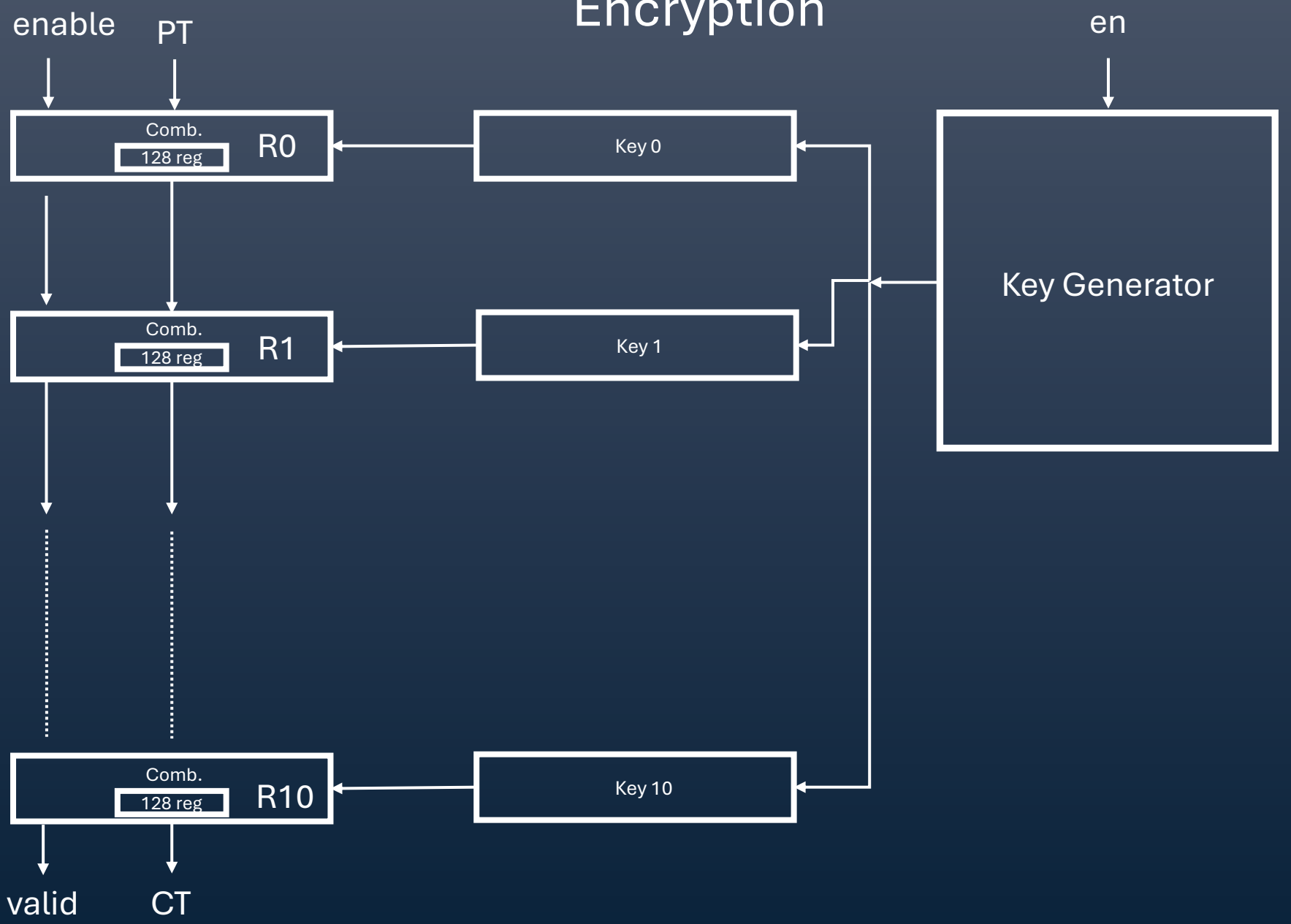
System diagram

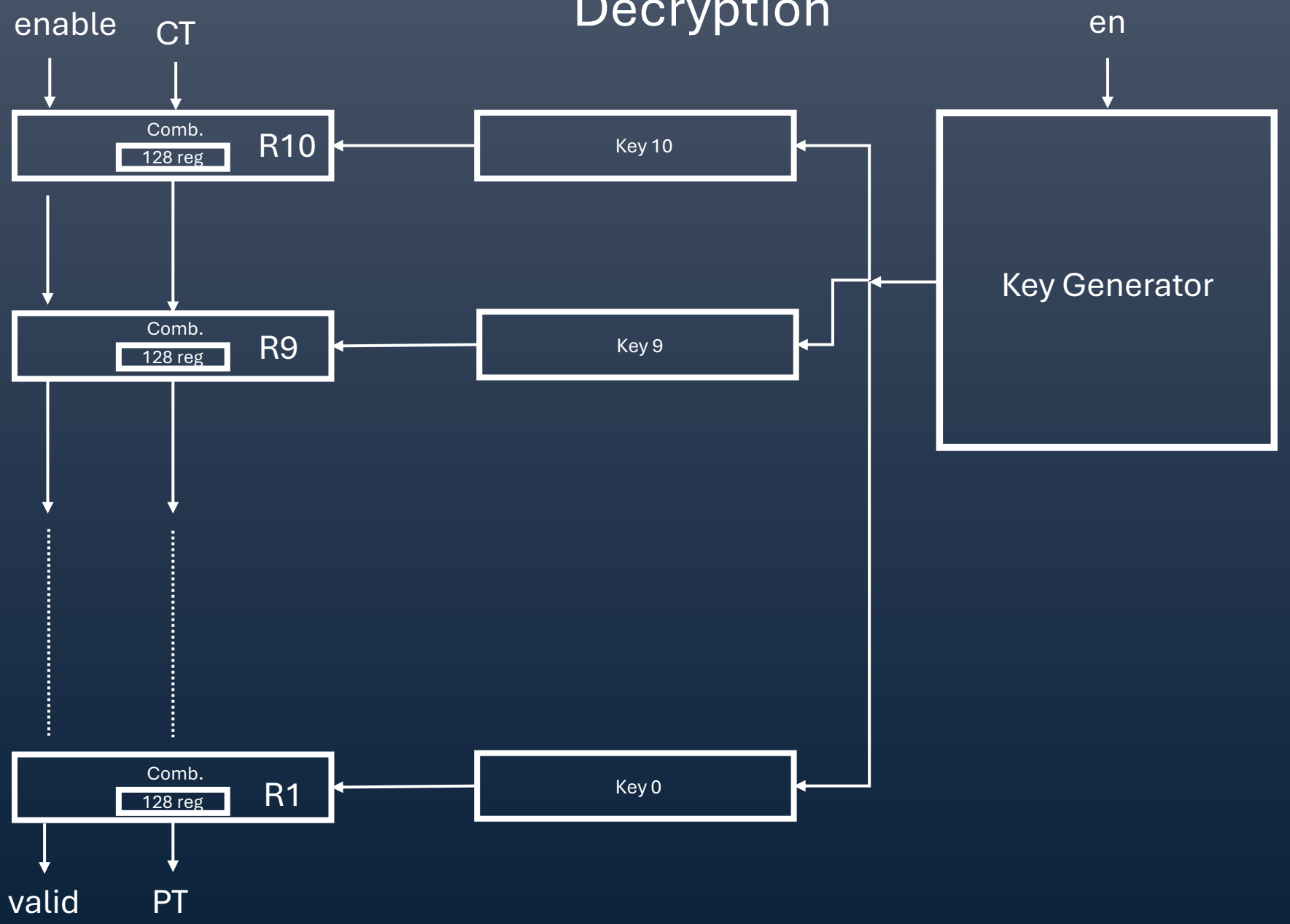


Pin name	Function
enable	Enable signal added to tell data is correct
Fsm_en	Enable signal for the FSM to start the key generation
nRst	Active low asynchronous reset
PT	Plain text sent
KEY	The key to be used
clk	Clock
valid	Valid signal to tell that the data sent are valid
CT	Cipher text received

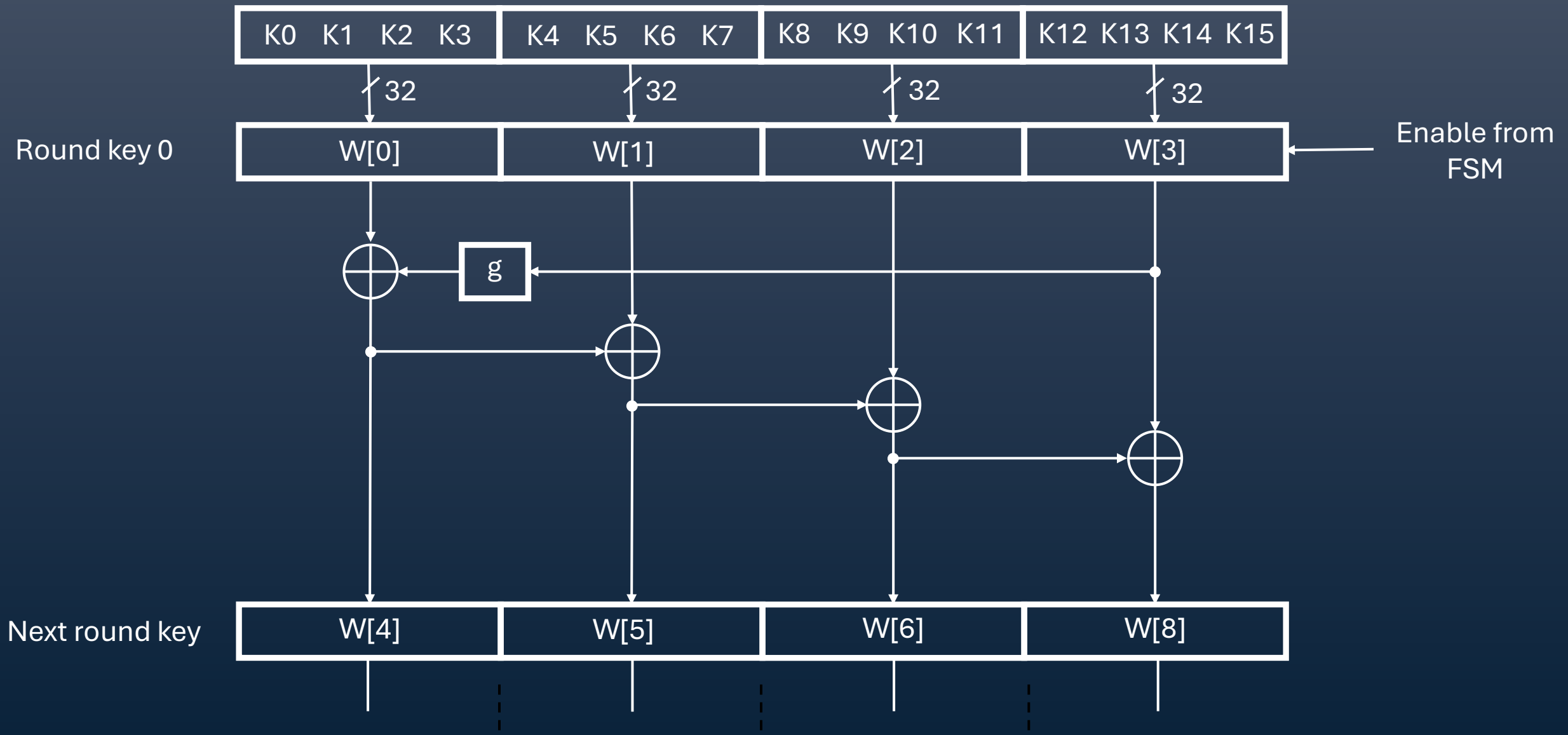
Encryption


enable
PT
en
Comb.
128 reg
R0
Key 0
Key Generator
Comb.
128 reg
R1
Key 1
Comb.
128 reg
R10
Key 10
valid
CT

Decryption


enable
CT
en
Comb.
128 reg
R10
Key 10
Key Generator
Comb.
128 reg
R9
Key 9
Comb.
128 reg
R1
Key 0
valid
PT

Key Generator

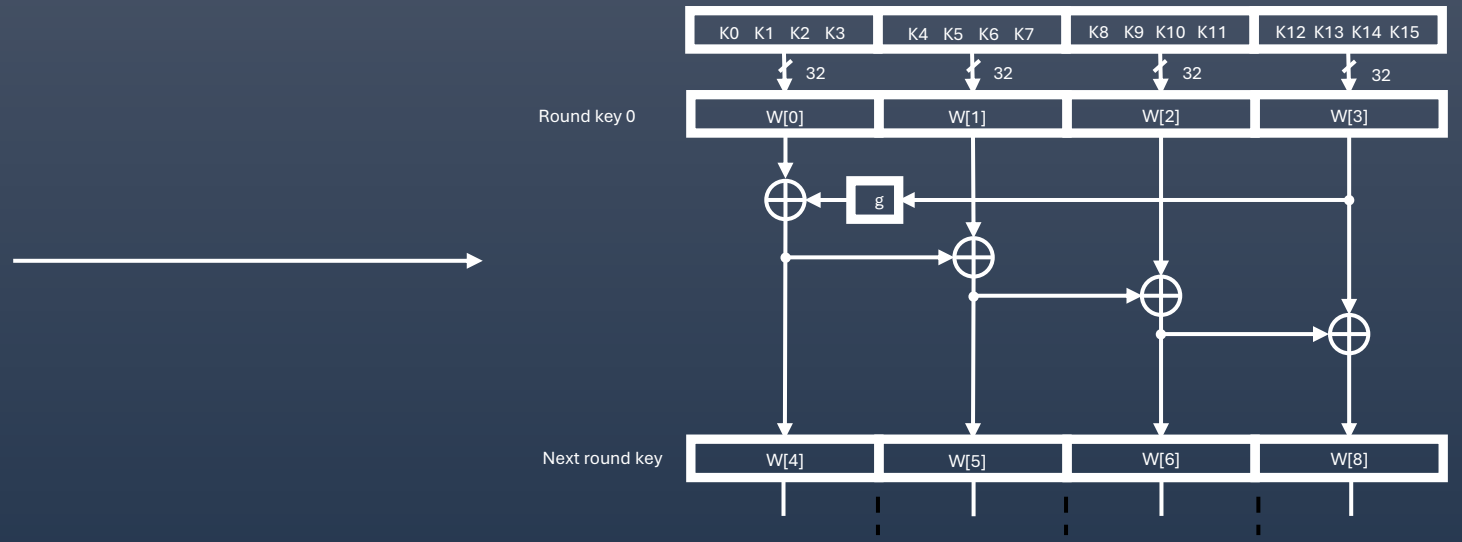


Key Generator

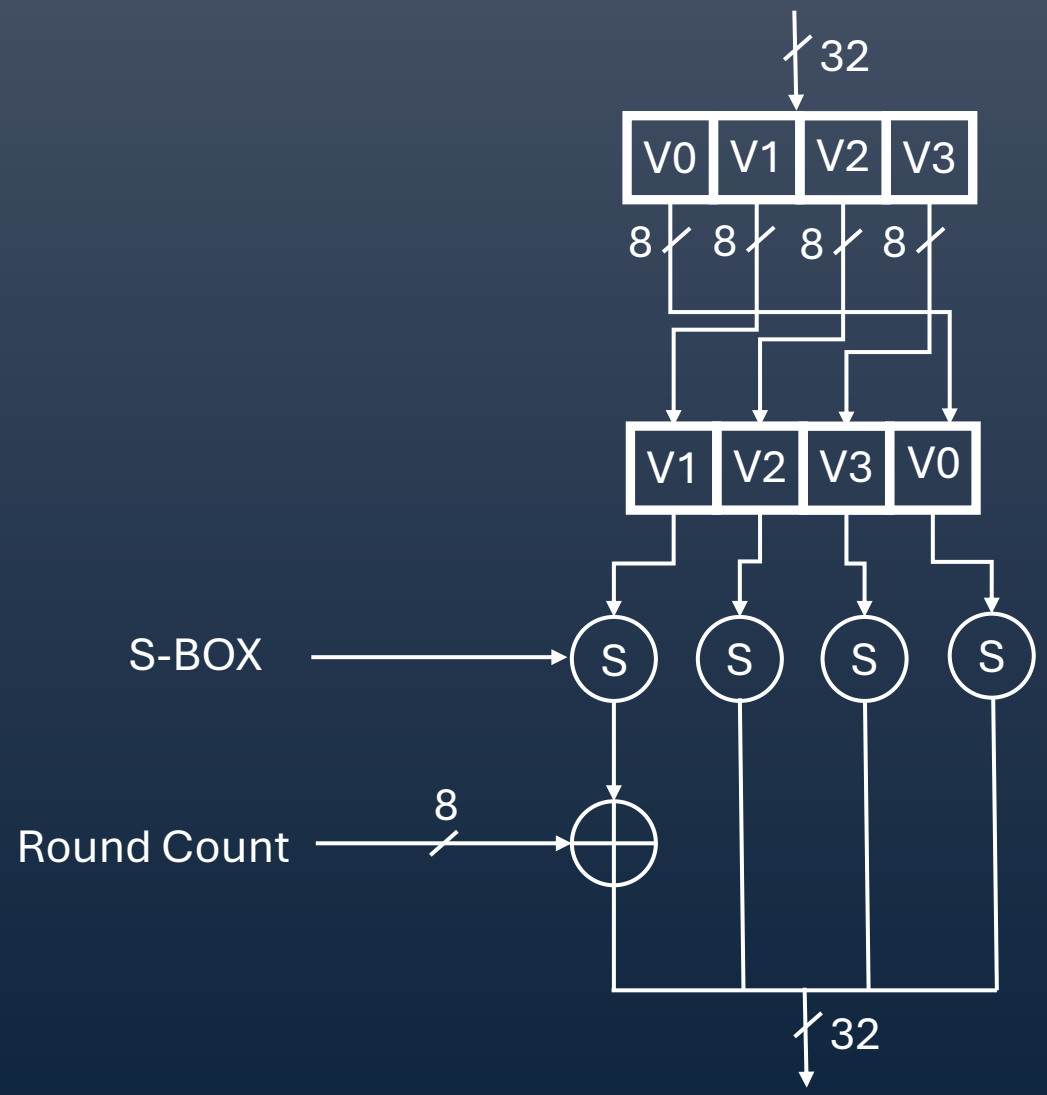
One comb. Block with FSM to calculate the next key and put it in the round key register.

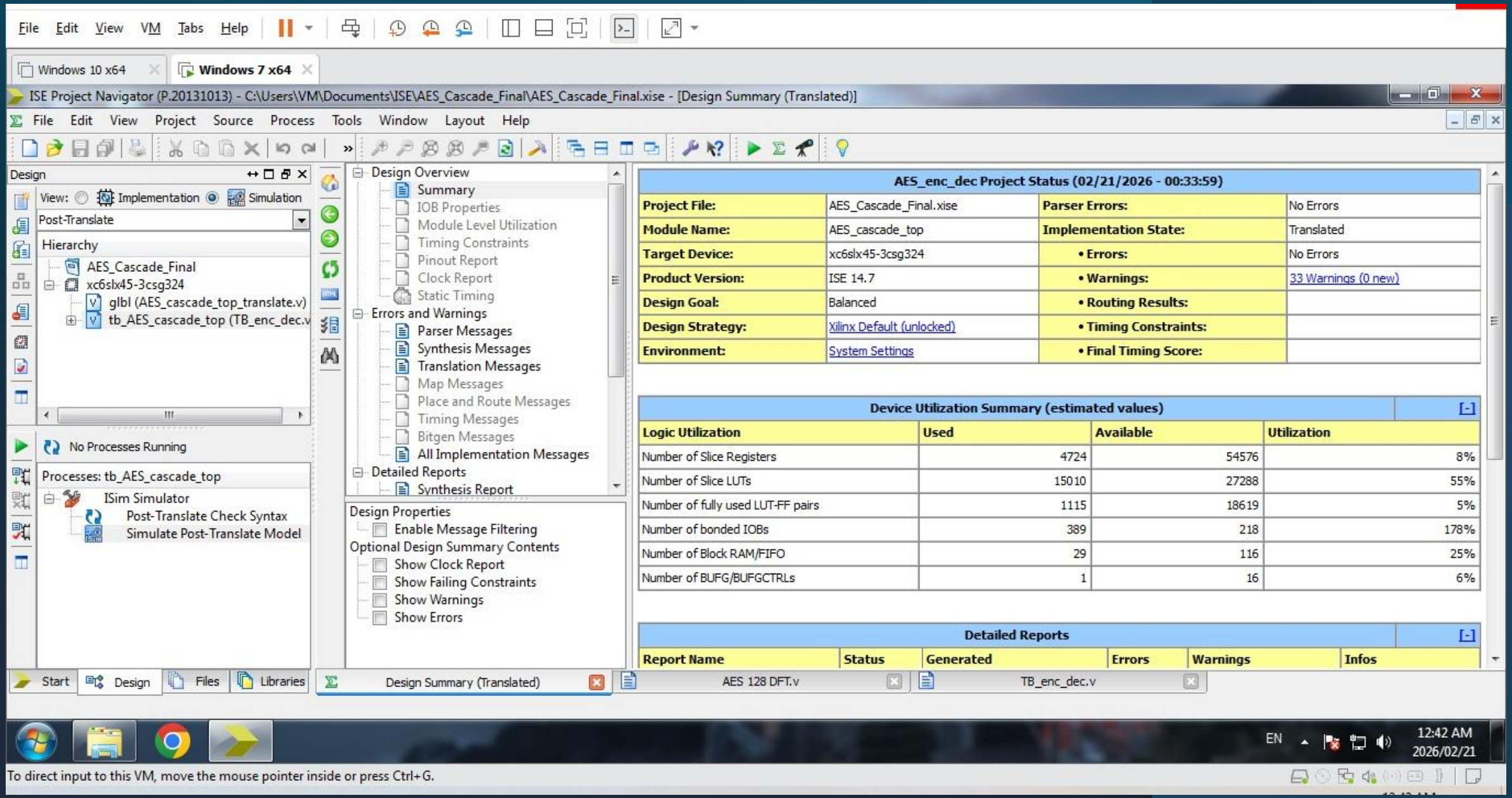
Then the previous key is used to calculate the next key and store it in the register.

An enable signal is provided from the FSM for 11 cycles to calculate all the keys and then every key is assigned to its correct register.



g-function




File Edit View VM Tabs Help
Windows 10 x64
Windows 7 x64
ISE Project Navigator (P.20131013) - C:\Users\VM\Documents\ISE\AES_Cascade_Final\AES_Cascade_Final.xise - [Design Summary (Translated)]
File Edit View Project Source Process Tools Window Layout Help
Design
View: Implementation Simulation
Post-Translate
Hierarchy
AES_Cascade_Final
xc6slx45-3csg324
glbl (AES_cascade_top_translate.v)
tb_AES_cascade_top (TB_enc_dec.v
No Processes Running
Processes: tb_AES_cascade_top
ISim Simulator
Post-Translate Check Syntax
Simulate Post-Translate Model
Design Overview
Summary
IOB Properties
Module Level Utilization
Timing Constraints
Pinout Report
Clock Report
Static Timing
Errors and Warnings
Parser Messages
Synthesis Messages
Translation Messages
Map Messages
Place and Route Messages
Timing Messages
Bitgen Messages
All Implementation Messages
Detailed Reports
Synthesis Report
Design Properties
Enable Message Filtering
Optional Design Summary Contents
Show Clock Report
Show Failing Constraints
Show Warnings
Show Errors
AES_enc_dec Project Status (02/21/2026 - 00:33:59)
Project File: AES_Cascade_Final.xise
Parser Errors: No Errors
Module Name: AES_cascade_top
Implementation State: Translated
Target Device: xc6slx45-3csg324
• Errors: No Errors
Product Version: ISE 14.7
• Warnings: 33 Warnings (0 new)
Design Goal: Balanced
• Routing Results:
Design Strategy: Xilinx Default (unlocked)
• Timing Constraints:
Environment: System Settings
• Final Timing Score:
Device Utilization Summary (estimated values)
Logic Utilization | Used | Available | Utilization
Number of Slice Registers | 4724 | 54576 | 8%
Number of Slice LUTs | 15010 | 27288 | 55%
Number of fully used LUT-FF pairs | 1115 | 18619 | 5%
Number of bonded IOBs | 389 | 218 | 178%
Number of Block RAM/FIFO | 29 | 116 | 25%
Number of BUFG/BUFGCTRLs | 1 | 16 | 6%
Detailed Reports
Report Name | Status | Generated | Errors | Warnings | Infos
Start Design Files Libraries
Design Summary (Translated)
AES 128 DFT.v
TB_enc_dec.v
EN
12:42 AM
2026/02/21
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.