VLSI PROJECT FALL 2015

HARDWARE ASSISTED ENCRYPTION ENGINES FOR SECURING CRITICAL DATA

CONTENTS

WHY HARDWARE ASSISTED?

- Difficult to connect unless hardware address is known (communication protocol)
- With Smartly secured encryption engines it is difficult to breach

HOW VLSI WILL PLAY CRUCIAL ROLE?

- System on chip design will enable an excess module to interact with system but will protect the critical data
- VLSI Chip design is robust as it helps to modify the chip based on application as in this case the severity of the attack.

ENCRYPTION AND DECRYPTION MECHANISMS

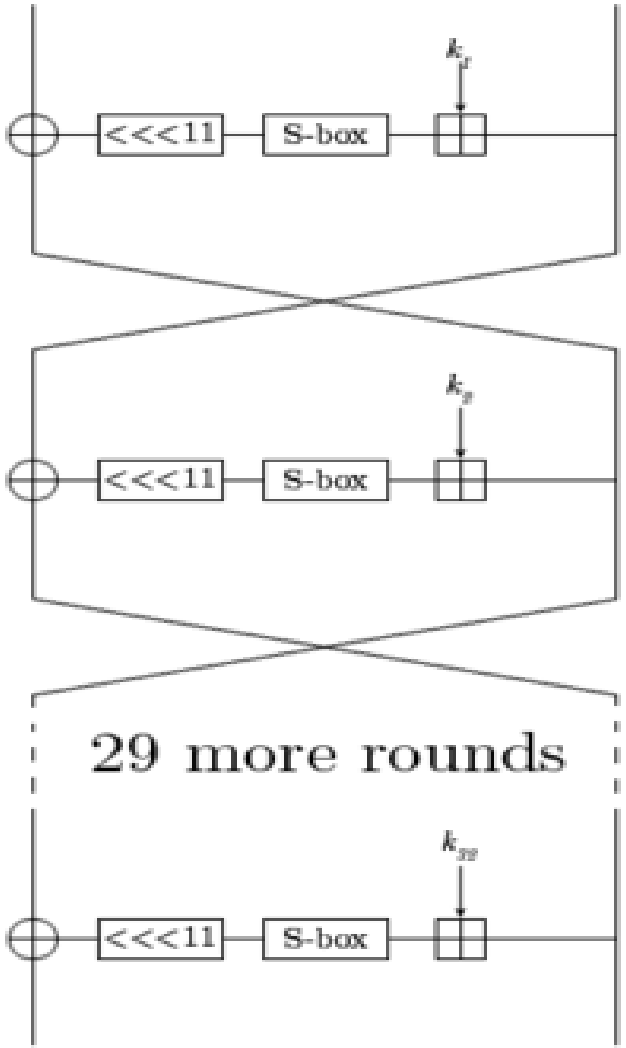
- GOST STANDARD ENCRYPTION MECHANISMS (Designed by Russian Federation and certified ISO/IEC)

- WHAT IS GOST? – A SYMMETRIC BLOCK CIPHER
  - -> 64 BIT BLOCK DATA
  - -> 256 BIT KEY

TYPES OF GOST STANDARD MODES USED

- ECB (ELECTRONIC CODEBOOK MODE)
- Pipelined (ELECTRONIC CODEBOOK MODE)
- CFB (CIPHER FEEDBACK MODE)
- MAC (MESSAGE AUTHENTICATION CODE)

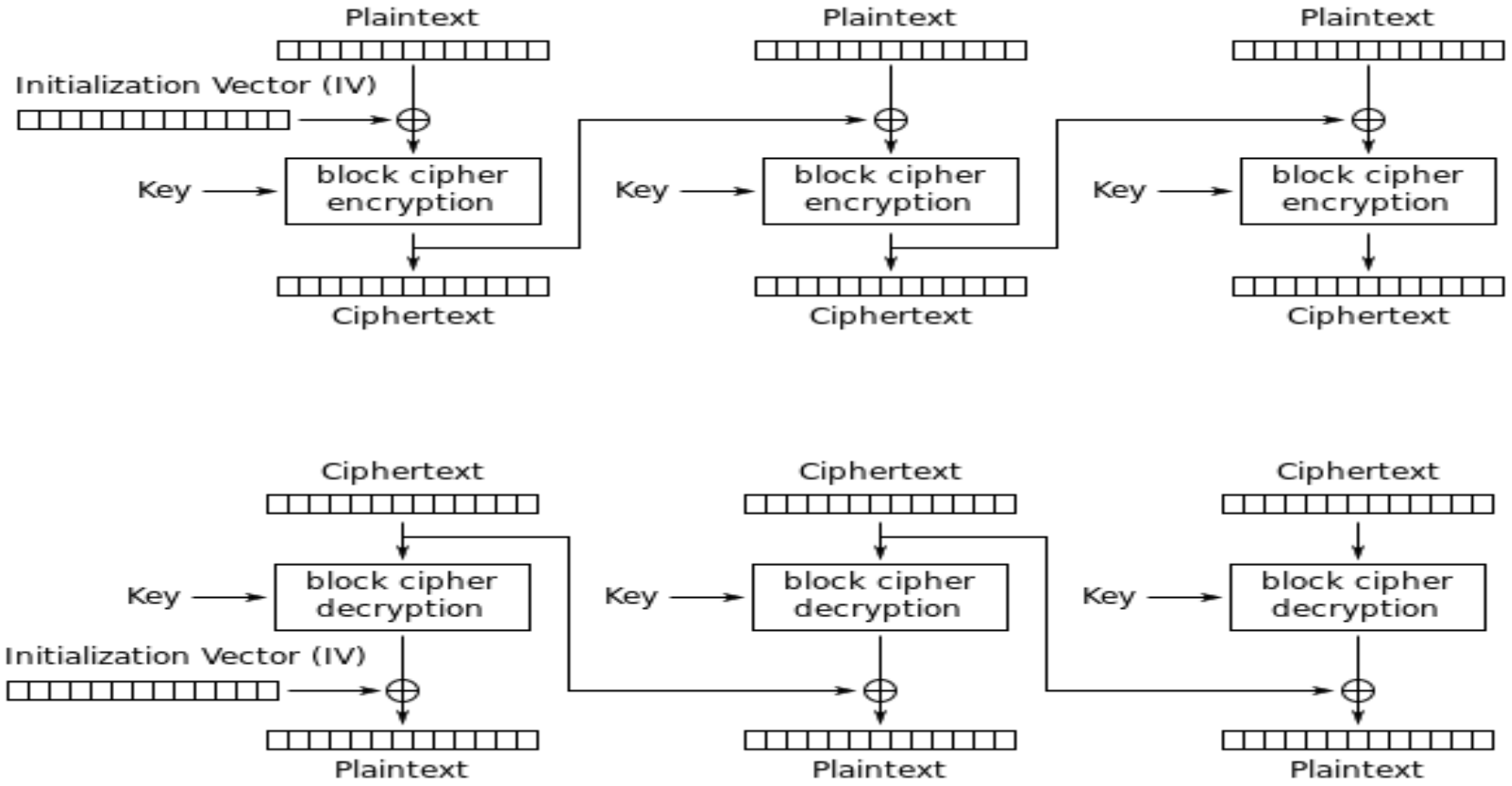
BASIC OPERATION OF GOST STANDARD



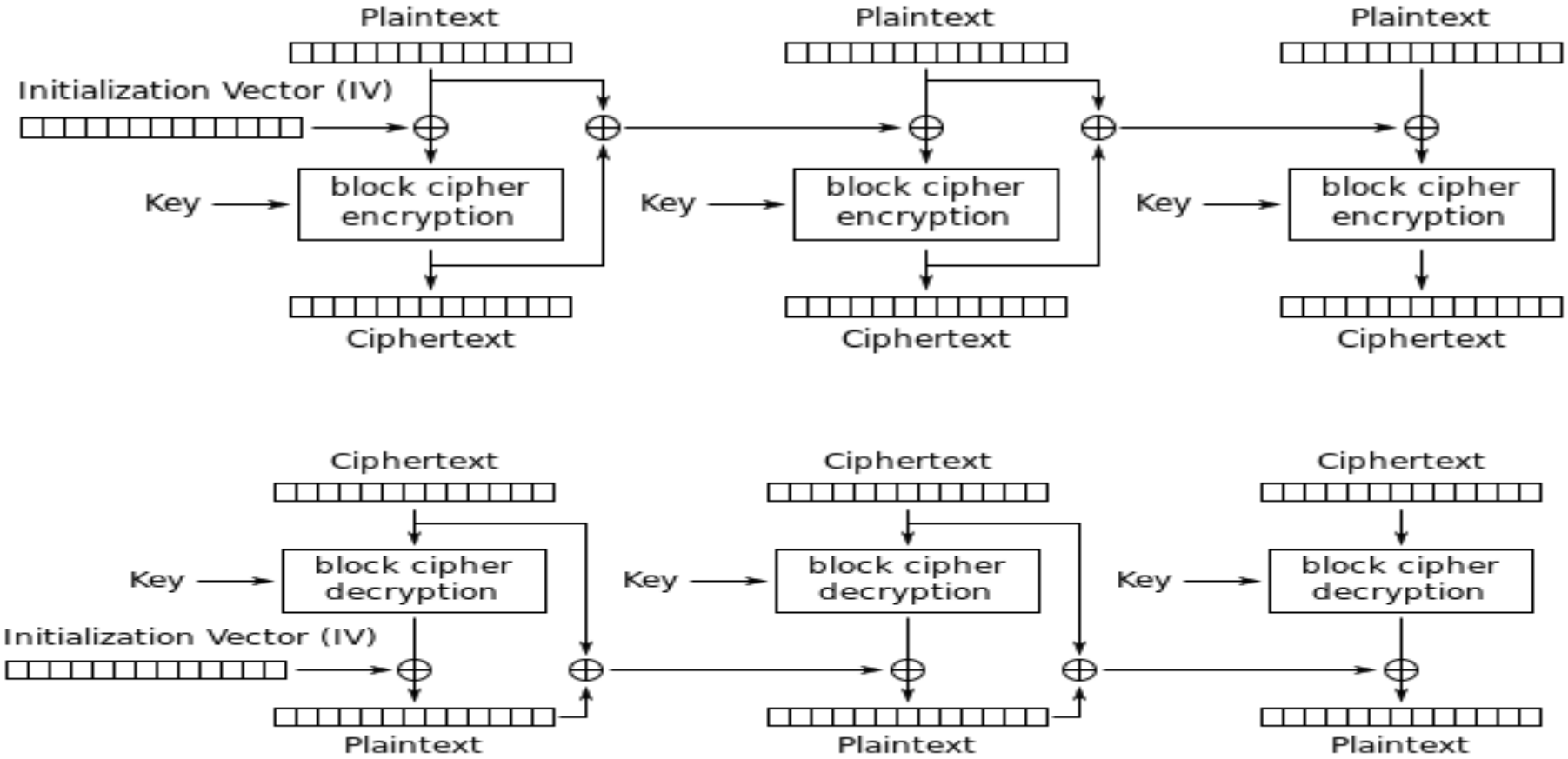
KEY FEATURES

- ROUND : 32 Bit Sub key modulo 2^{32}
- S_BOX : Obscure relation between key and ciphertext

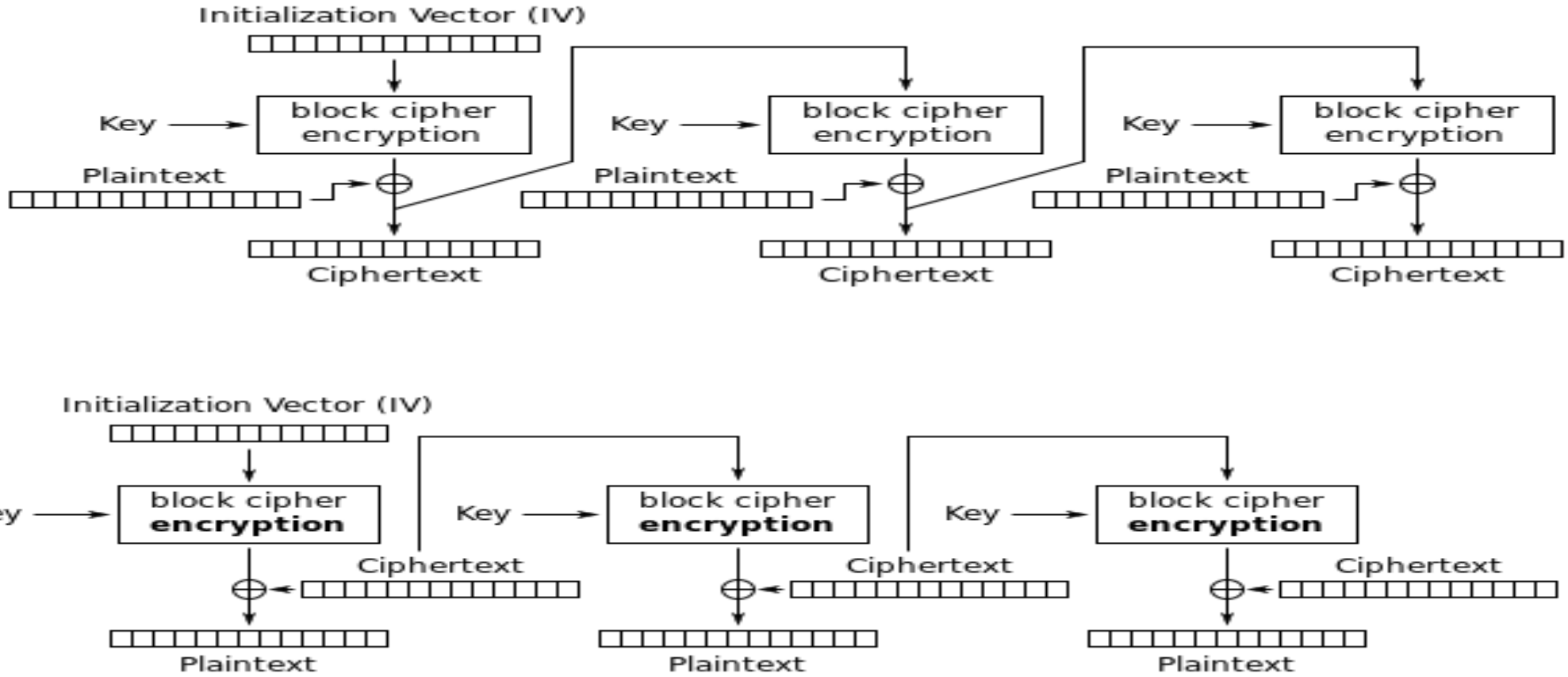
ECB ENCRYPTION & DECRYPTION



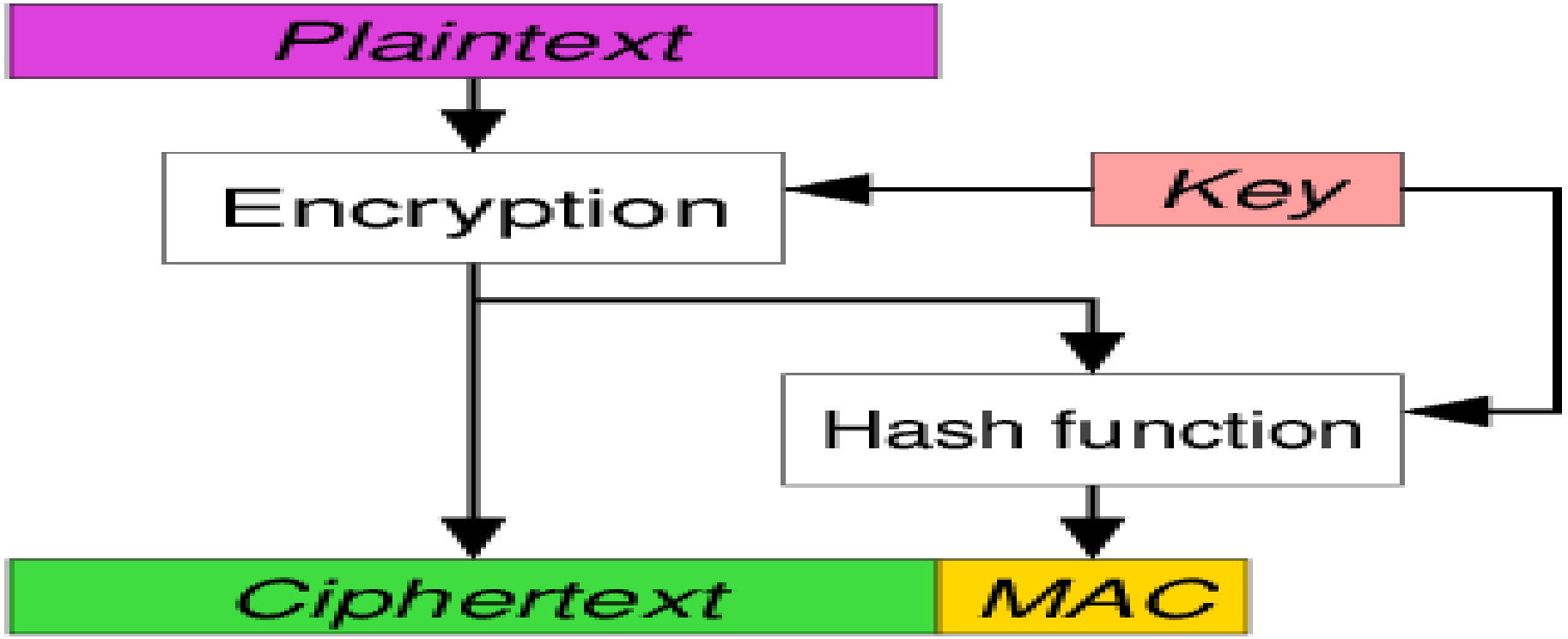
ECB WITH PIPELINE ENCRYPTION & DECRYPTION



CFB ENCRYPTION AND DECRYPTION

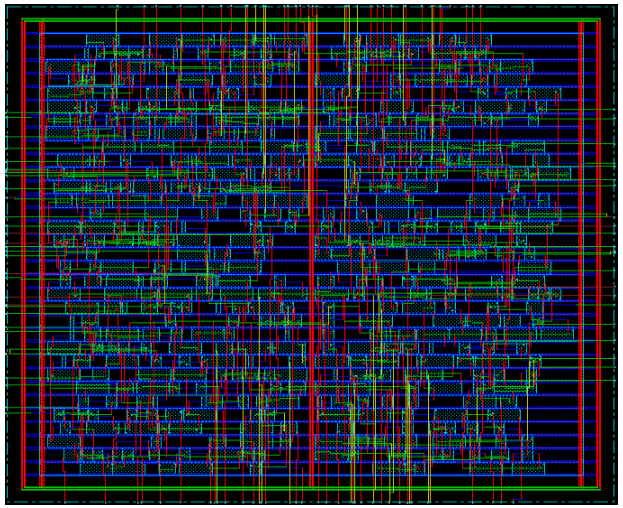


Message Authentication Code

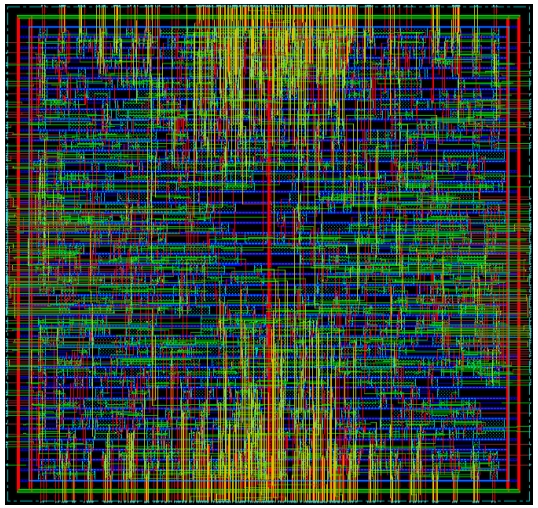


TOOLS USED

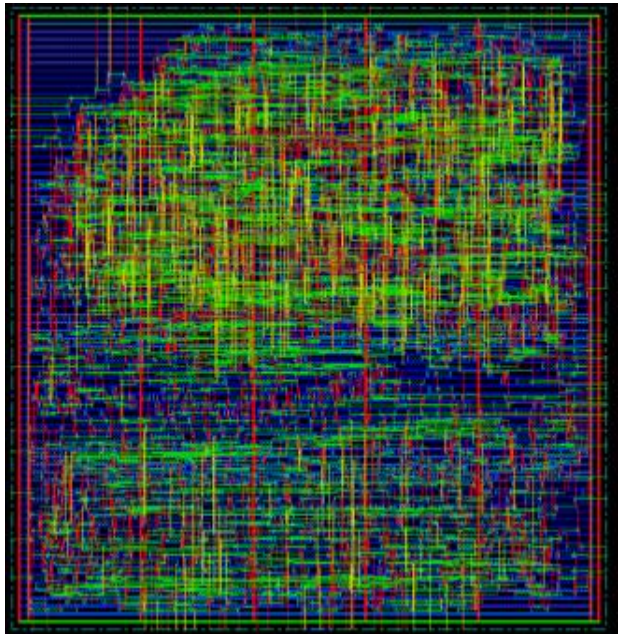
- VIVADO 2015 for Verilog Compilation , RTL Design & Simulations output Waveforms
- Cadence Encounter for Chip Layout and Gate Counts
- Synopsys Design Vision for Power, Area and Slack Data



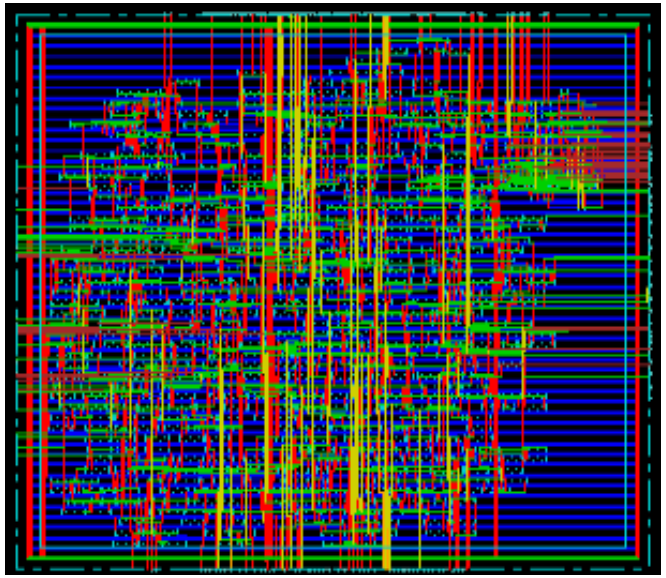
ECB



Pipelined ECB

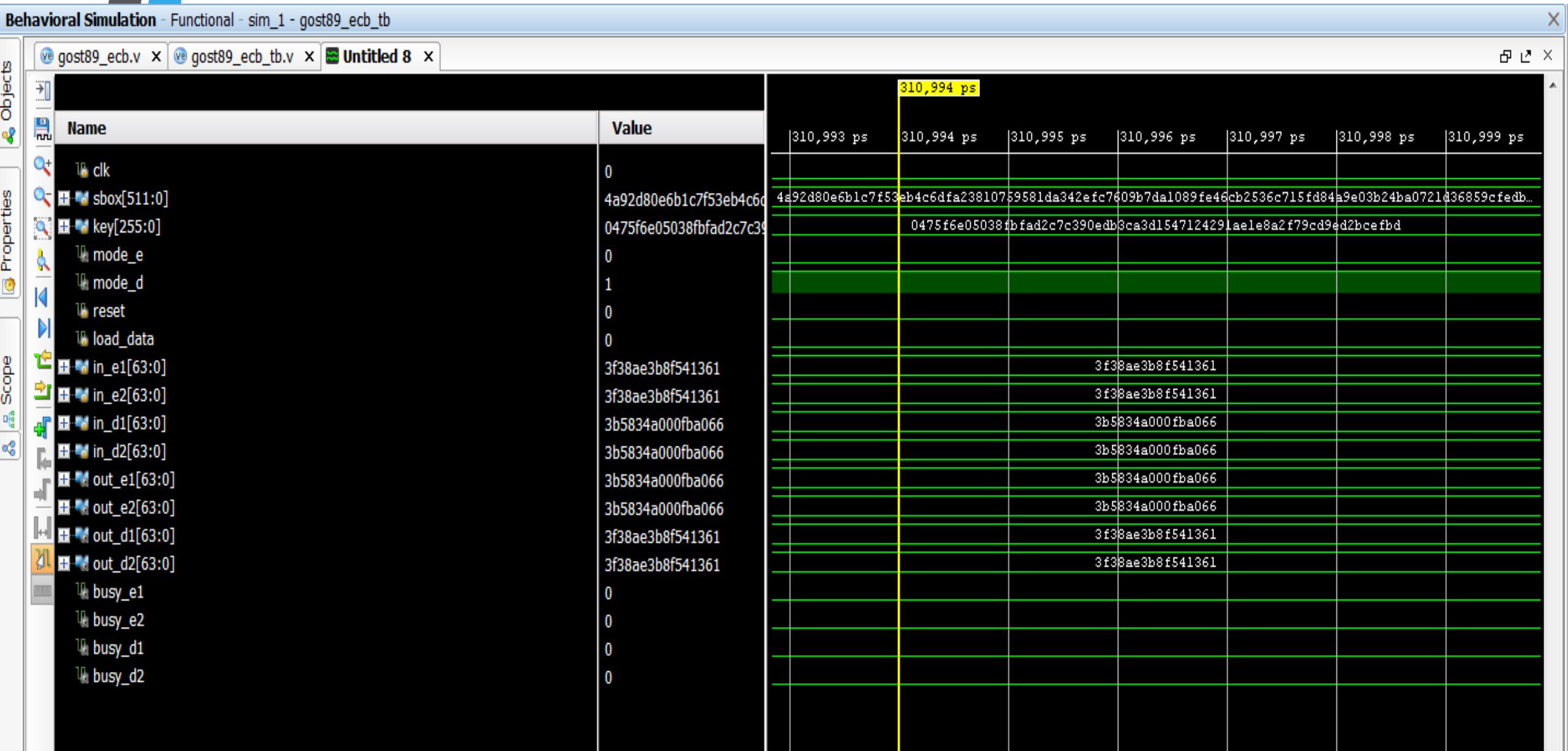


CFB

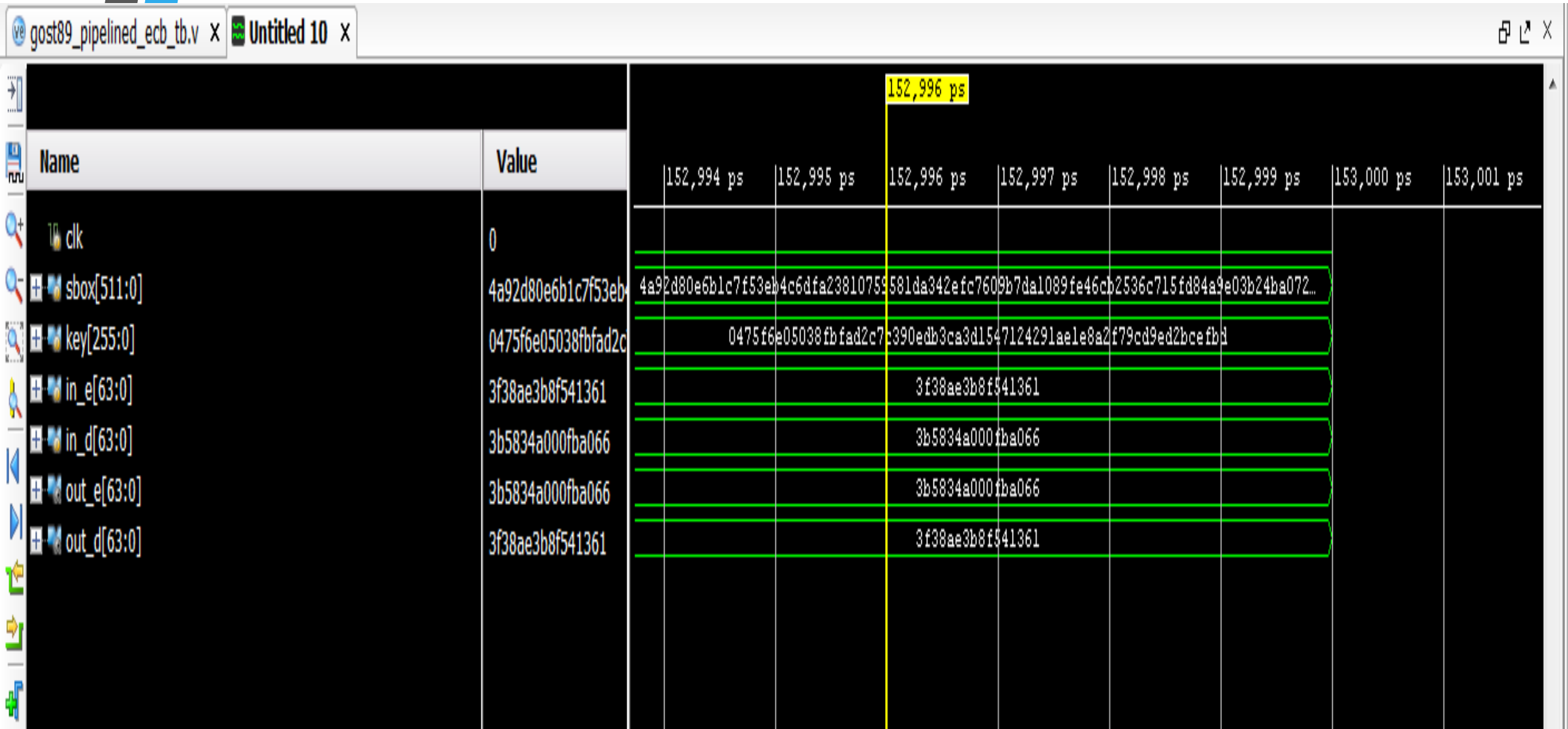


MAC

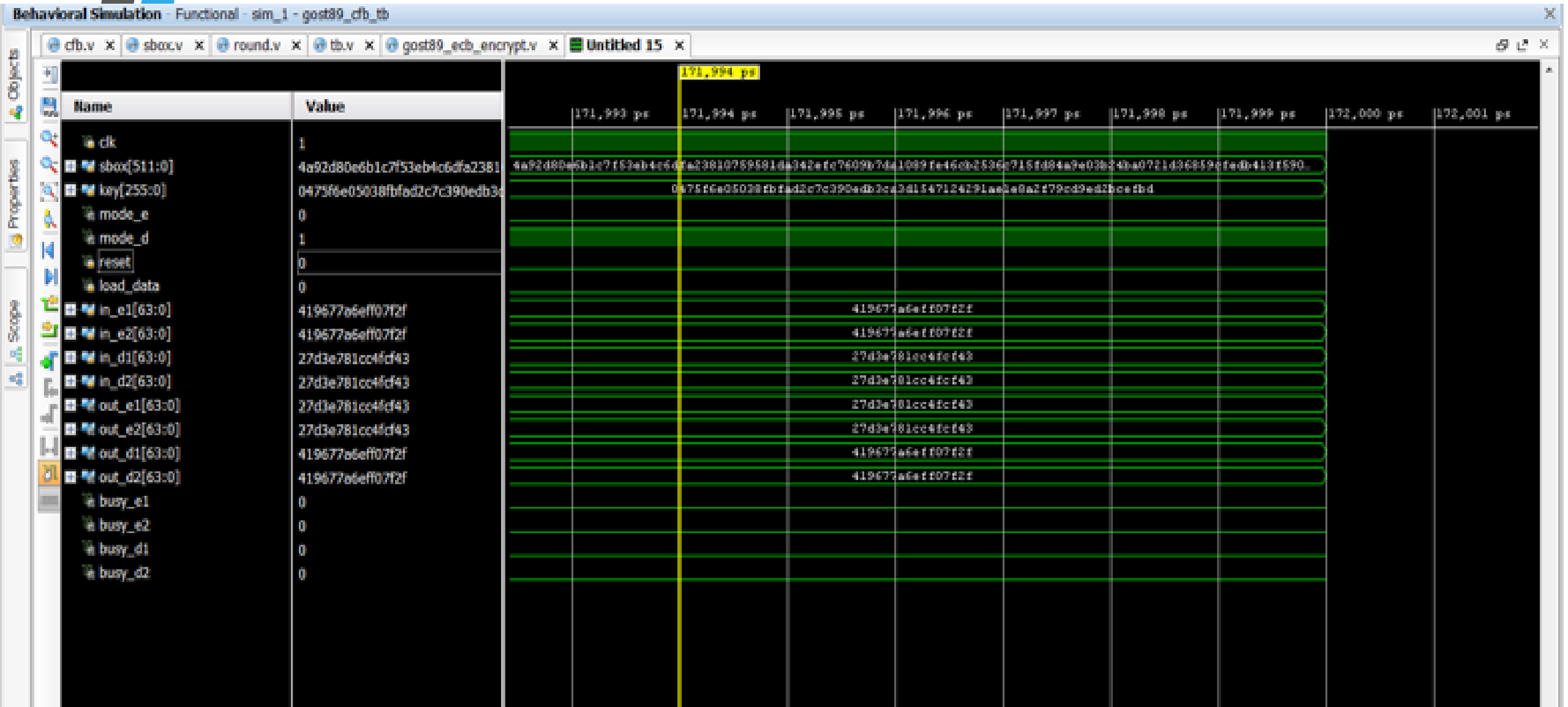
ECB OUTPUT WAVEFORMS



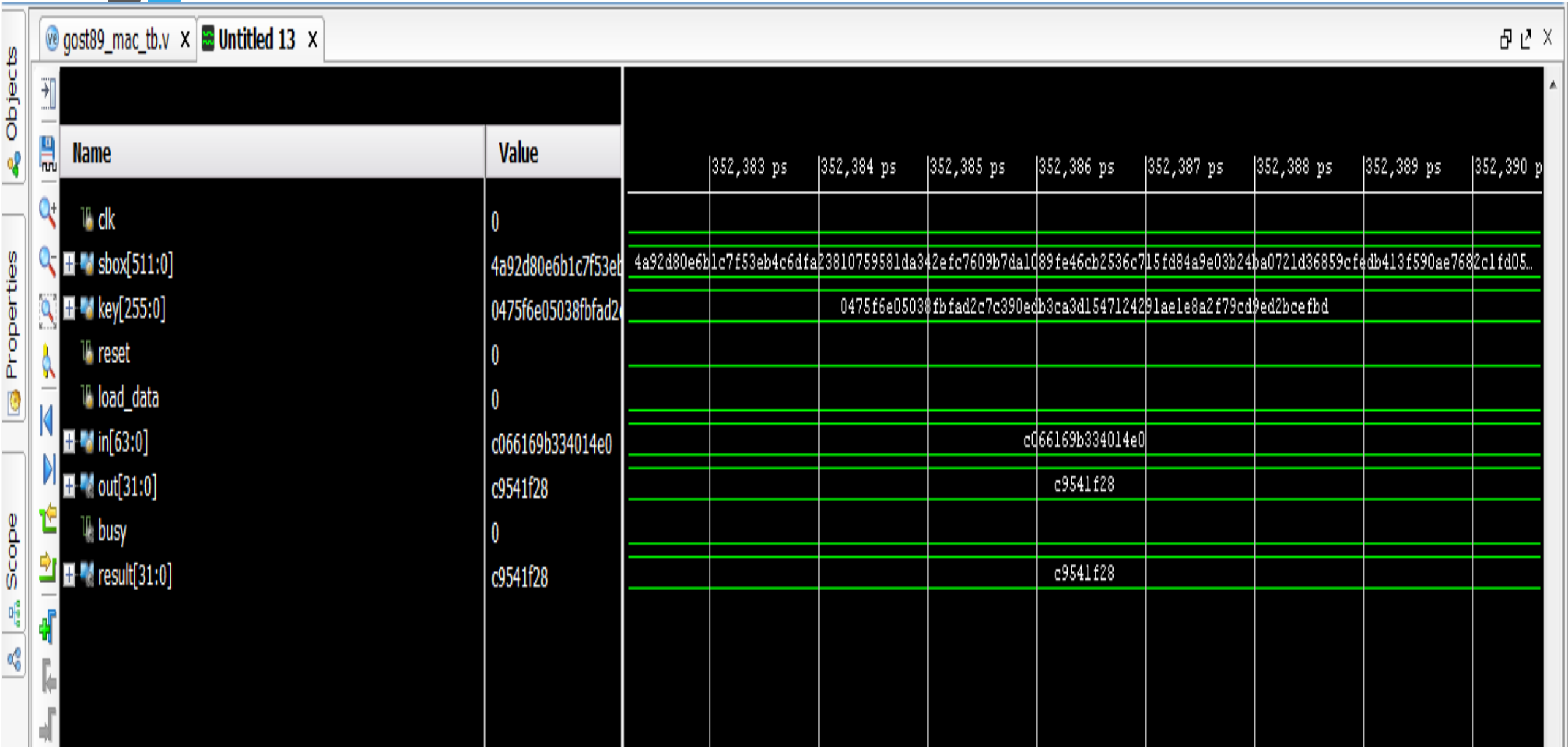
ECB PIPELINE OUTPUT WAVEFORMS



CFB OUTPUT WAVEFORMS



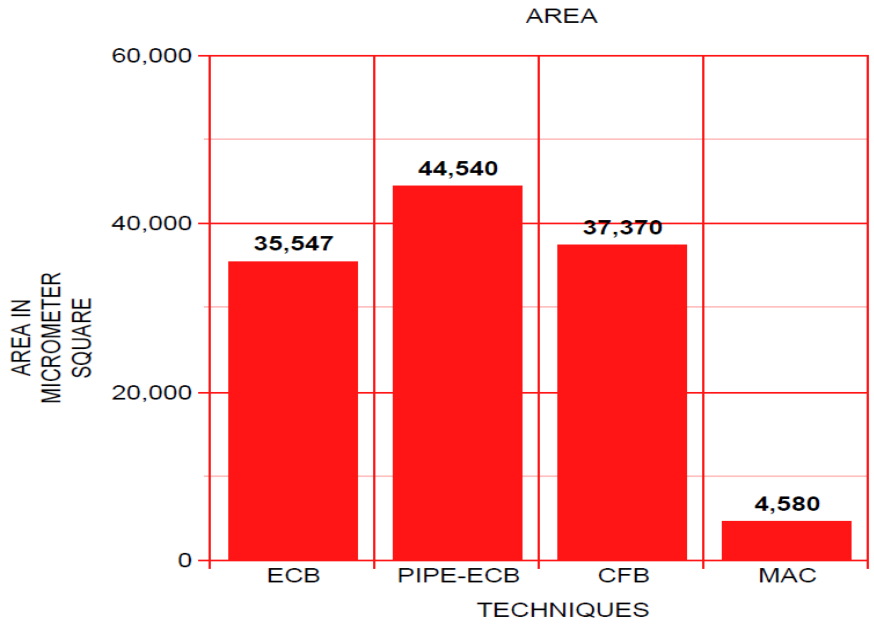
MAC OUTPUT WAVEFORMS

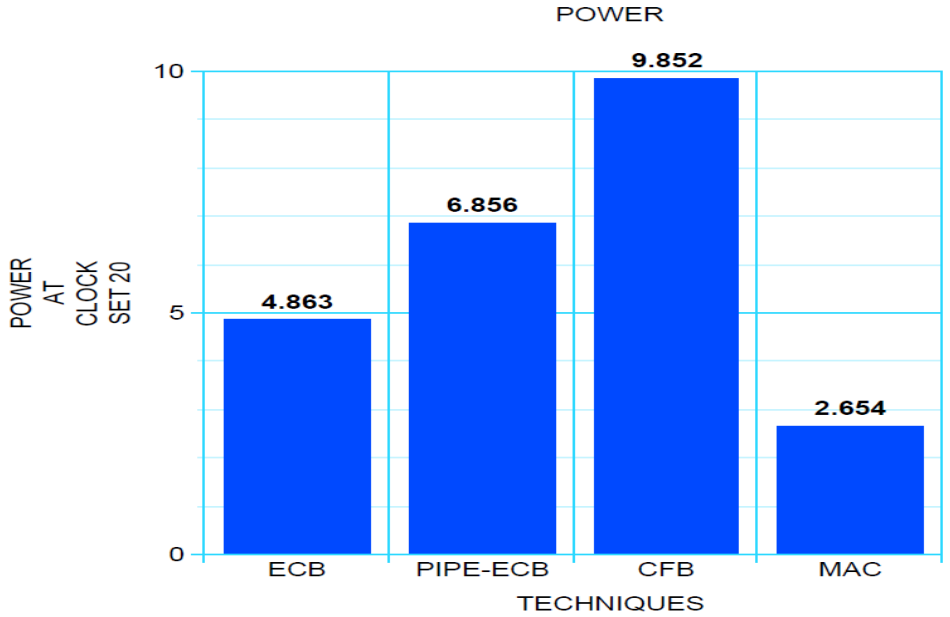


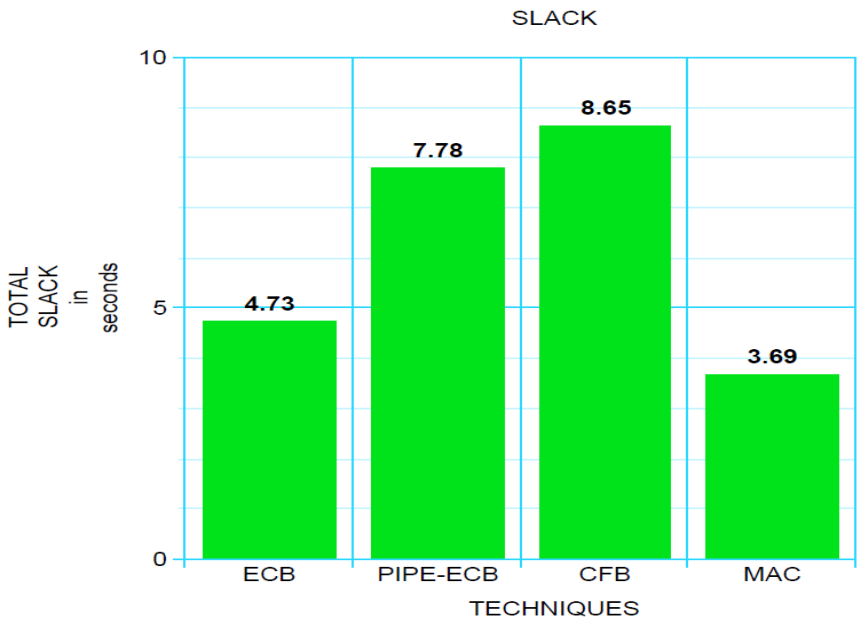
AREA, POWER, GATE COUNT AND SLACK ANALYSIS

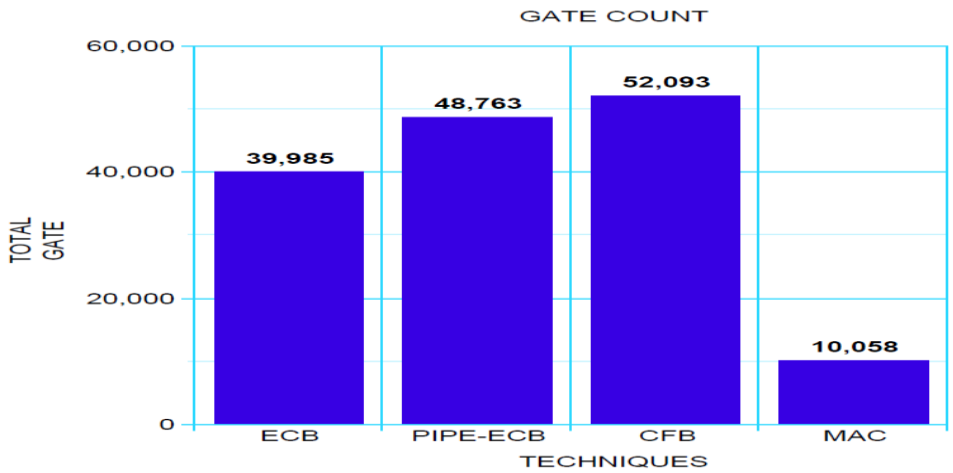
	AREA (micrometers quare)	POWER (mW)	GATE COUNT	SLACK (seconds)
ECB	35547	4.863	39985	4.73
PIPELINED ECB	44540	6.856	48763	7.78
CFB	37370	9.852	52093	8.65
MAC	4580	2.654	10058	3.69

GRAPHICAL REPRESENTATION OF AREA,POWER,SLACK AND GATE COUNT









Conclusion

Based on application and suitable Area, Power and Slack values the proper cryptographic model engine must be selected.

Future Work

1. Based on Data Mining conclusions and thus based on threat severity the appropriate model can be selected.
2. Addition of MAC module before any mode gives enhanced security.
3. Simple Interface like USB or NIC connection with Server can provide small scale industrial security of their information

THANK YOU