A Design Flow for 12.8 GBit/s Triple DES using Dynamic Logic and Standard Synthesis Tools

F. Grassert, S. Flügel, M. Grothmann, M. Haase,
P. Nimsch, H. Ploog, A. Wassatsch, D. Timmermann

University of Rostock (Germany)
Dep. Electrical Engineering and Information Technology
Institute of Applied Microelectronics and CS

Purpose

- Wanted: Fast Triple DES processor
- Wanted: Integration of dynamic logic in standard synthesis

➢ Development of design flow for TSPC Logic

➢ Application: Triple DES

Outline

- Introduction
- Basics of dynamic logic and TSPC logic
- Design flow for TSPC
- Realization of Triple DES
- Summary

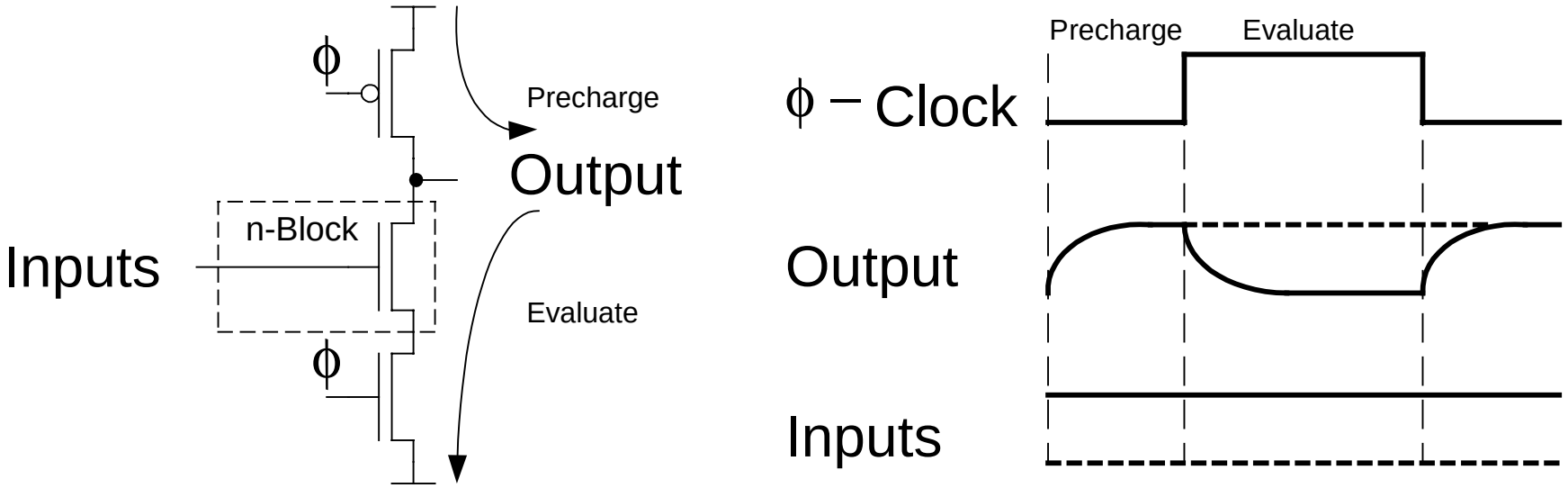
Dynamic Logic

- Application
  - High-end chips

    i.e. Posluszny et al „Design methodology for a 1.0 GHz Microprocessor“, ICCD 1998
  - Ultra fast logic

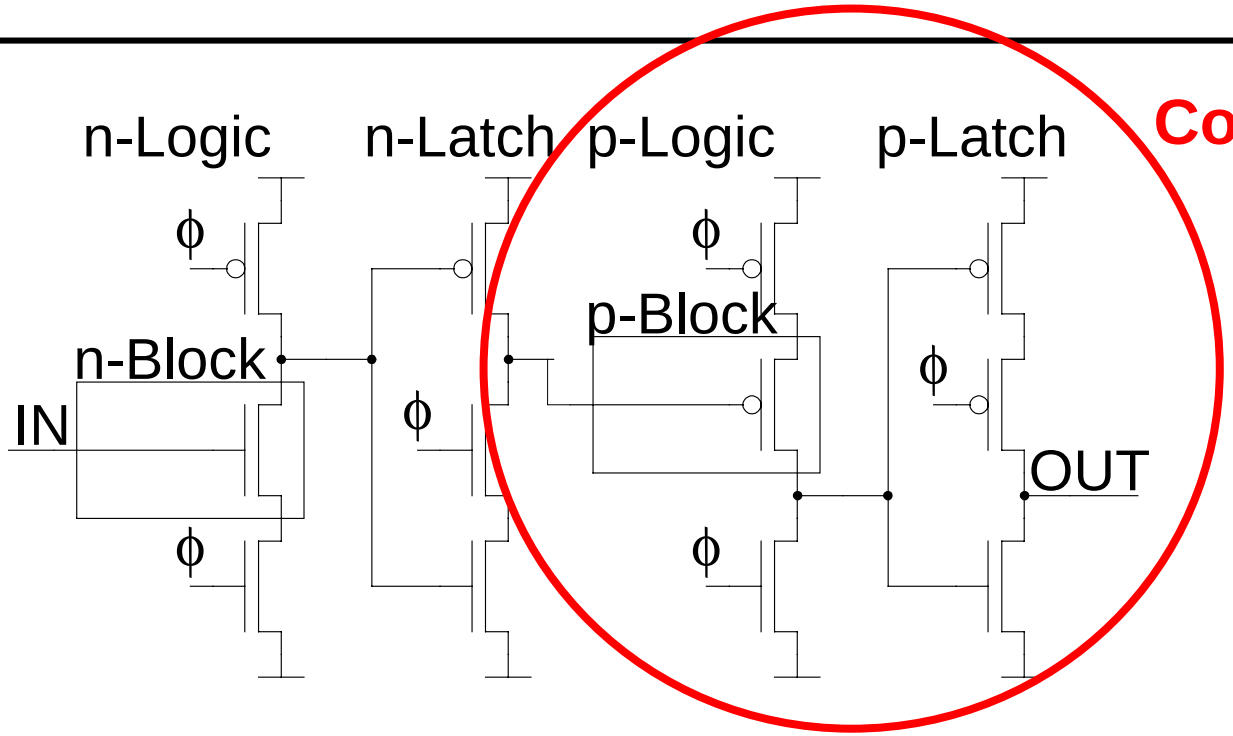
    i.e. Yee, Sechen, „Clock-Delayed Domino for Dynamic Circuit Design“, Trans. On VLSI Systems 2000
- Advantages
  - Very fast
  - Can be small
- Disadvantages
  - Difficult to design
  - Not supported by synthesis tools
  - Power consumption
  - Expensive clock-tree design

Dynamic Logic - Function



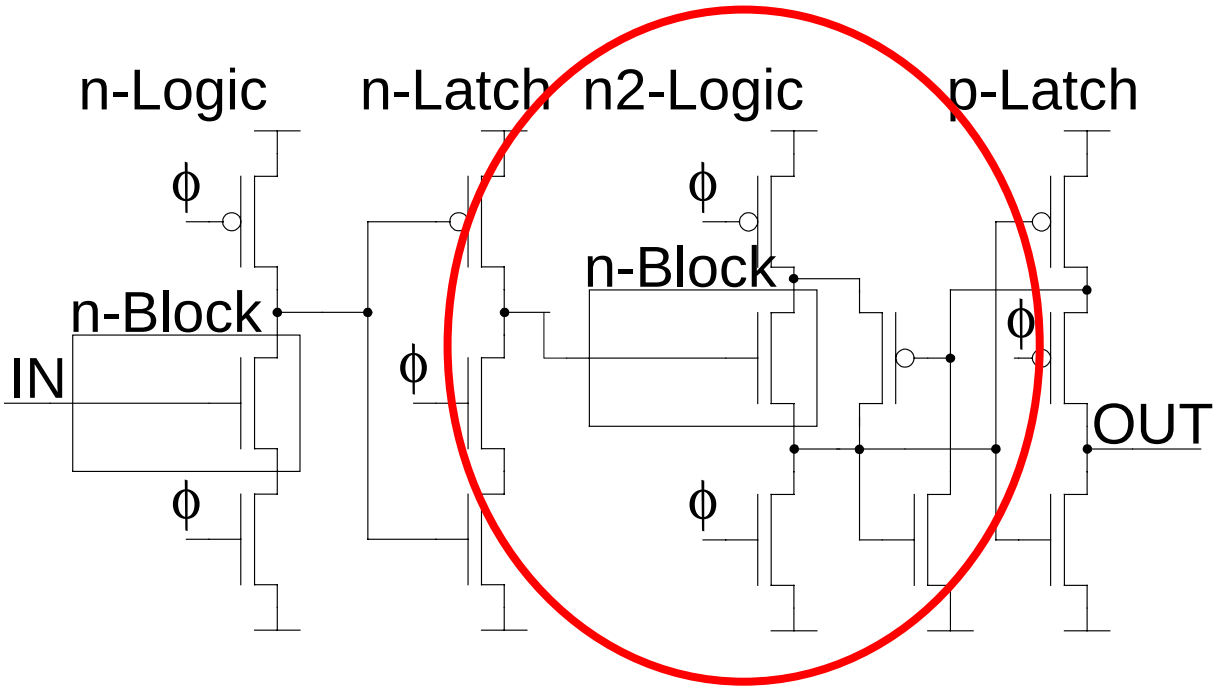
- Works only with two phases
- Logic function using n-transistors (“n-block”)
  - fast and small
- No direct interconnect of outputs and inputs possible

True Single Phase Clock (TSPC) Logic (1)



- True Single Phase Clock
- Realizes register function → combined register and logic
- Only non-inverting logic functions
- P-block: slow, large area

True Single Phase Clock (TSPC) Logic (2)

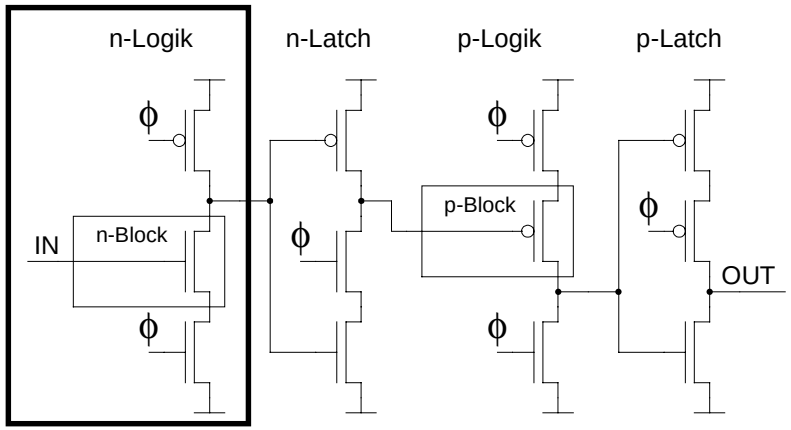


- Second TSPC realization: N-N2 logic
- Inverting logic functions only

True Single Phase Clock (TSPC) Logic (3)

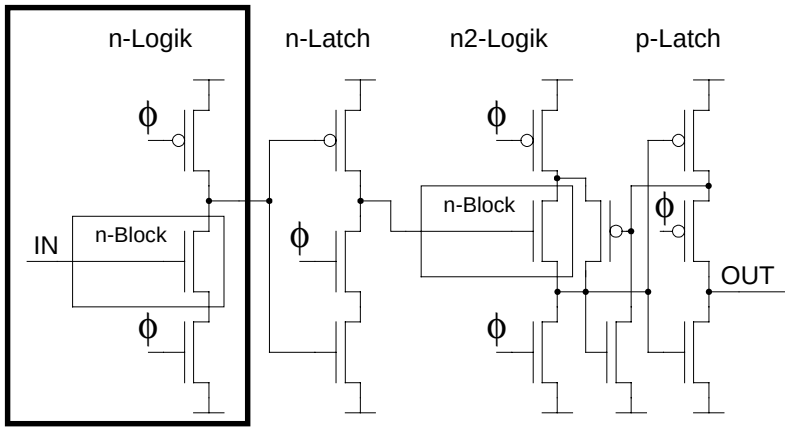
Non-inverting functions

Used for logic



Inverting functions

Used for logic



- Result: non-inverting and inverting logic functions
- No use of second logic block, but possible
- Robust and fast cells
- Extreme pipelining – extreme clock load
- Problem: clock distribution

Synthesis of TSPC Logic

- **Generating the library**
- Generating a combinational netlist
- Generating the pipeline
- Implementing the pipeline in the design

Building a Library

- Cell layout
- Verifying the cells
- Simulation
- Compiling the library

- Combinational function is the main point
- Timing behavior not interesting
- Register function not important

Synthesis of TSPC Logic

- Compiling the library
- **Generating a combinational netlist**
- Generating the pipeline
- Implementing the pipeline in the design

Generating a Combinational Netlist

- Standard design flow
  - VHDL description, analyzing, elaboration
- Mapping (using the library with TSPC gates)

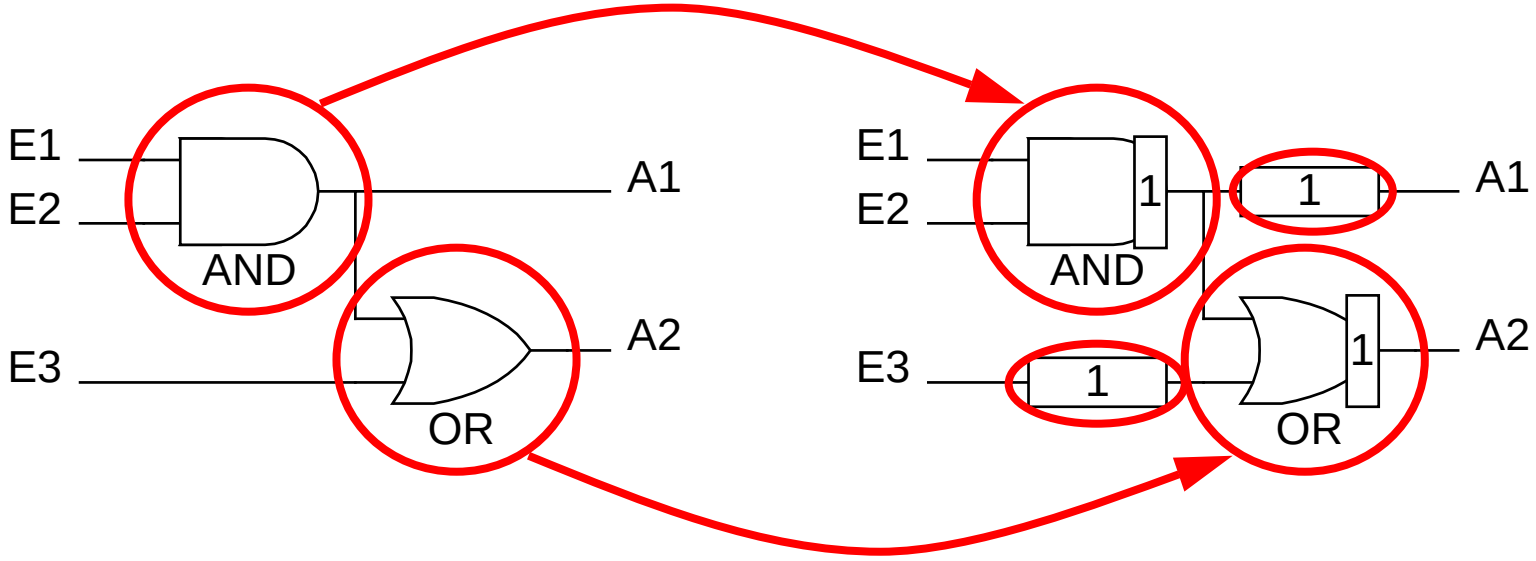
- No feedbacks allowed – only straightforward
  - Otherwise splitting in shorter combinational parts or hand design

Synthesis of TSPC Logic

- Compiling the library
- Generating a combinational netlist
- **Generating the pipeline**
- Implementing the pipeline in the design

Generating the Pipeline

- Interpreting all cells as registers (pipeline stages)
- Building the pipeline and integrating buffers

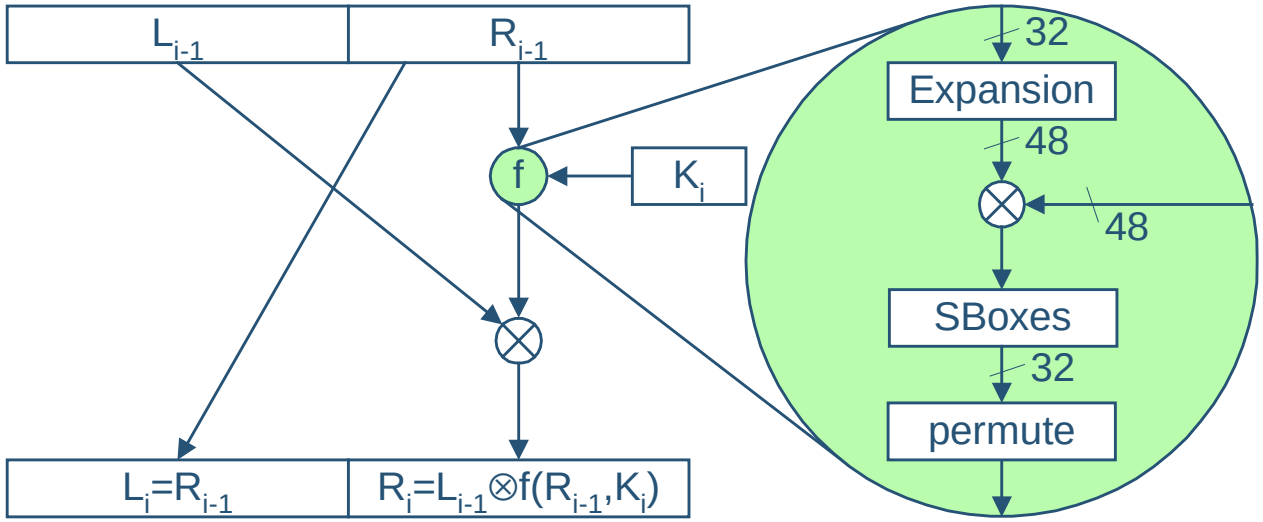


Synthesis of TSPC Logic

- Compiling the library
- Generating a combinational netlist
- Generating the pipeline
- **Implementing the pipeline in the design**

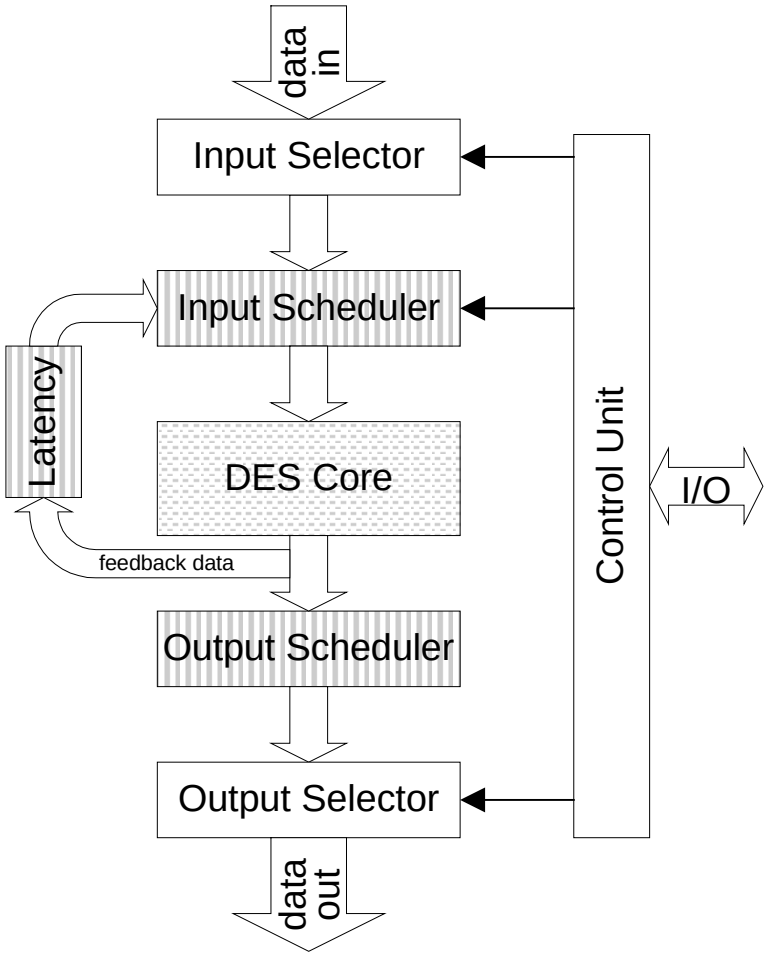
DES Core as an Example

- Data Encryption Standard (DES) – symmetric encryption
- 64 bit message with 56 bit key to 64 bit cipher text
- 16 rounds per data word
- Loop-unrolling ideal for pipelining



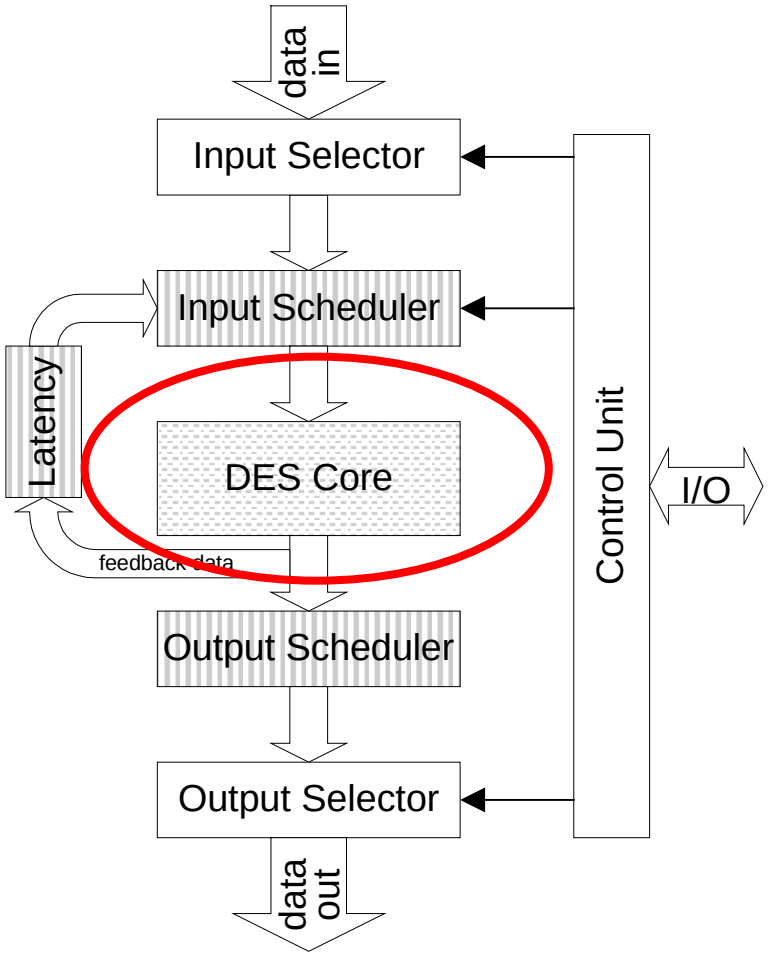
Structure of the DES Chip

- One round – Single DES
- Three rounds – Triple DES
- 4 channels for encryption
- Communication with control unit through parallel and I²C interfaces
- Control part, Input / Output 200MHz, SCMOS
- Core part 800Mhz, TSPC
- Built In Self Test (BIST)



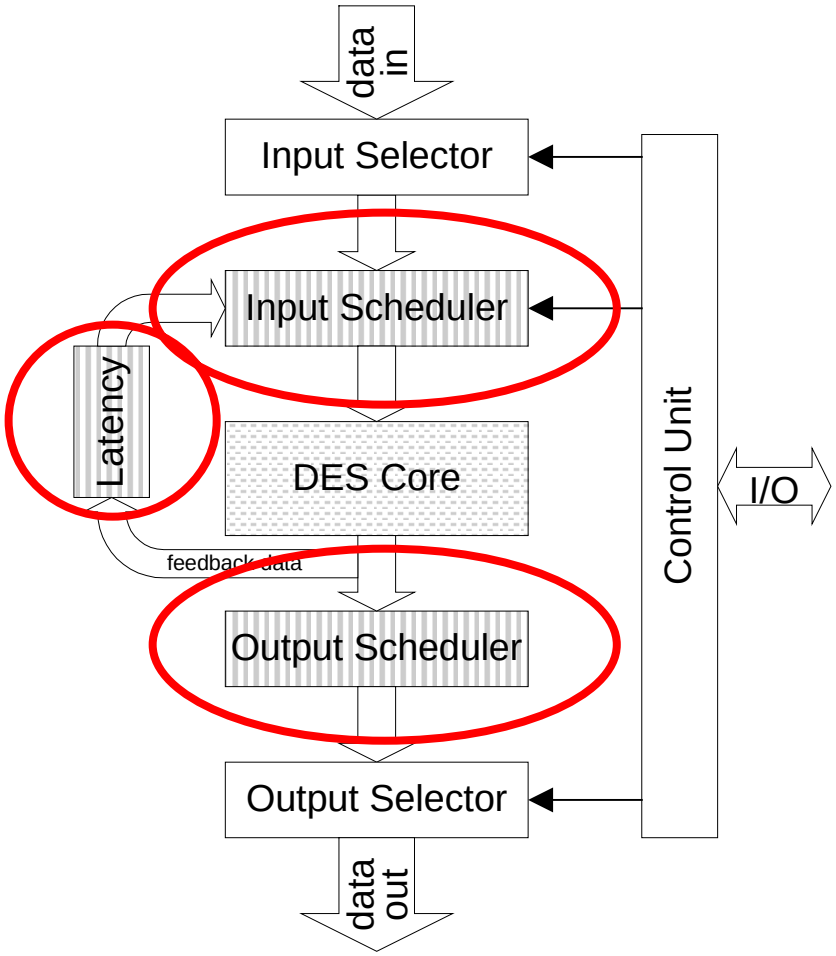
Realization DES Chip

- DES - Core completely realized with automatic synthesis
- Black box verification between VHDL description and C-program via CLI
- Compiling VHDL to combinational netlist with TSPC library information
- Micro Pipeline Reorganization (MPR) step using developed tool
- Verification steps



Realization DES Chip

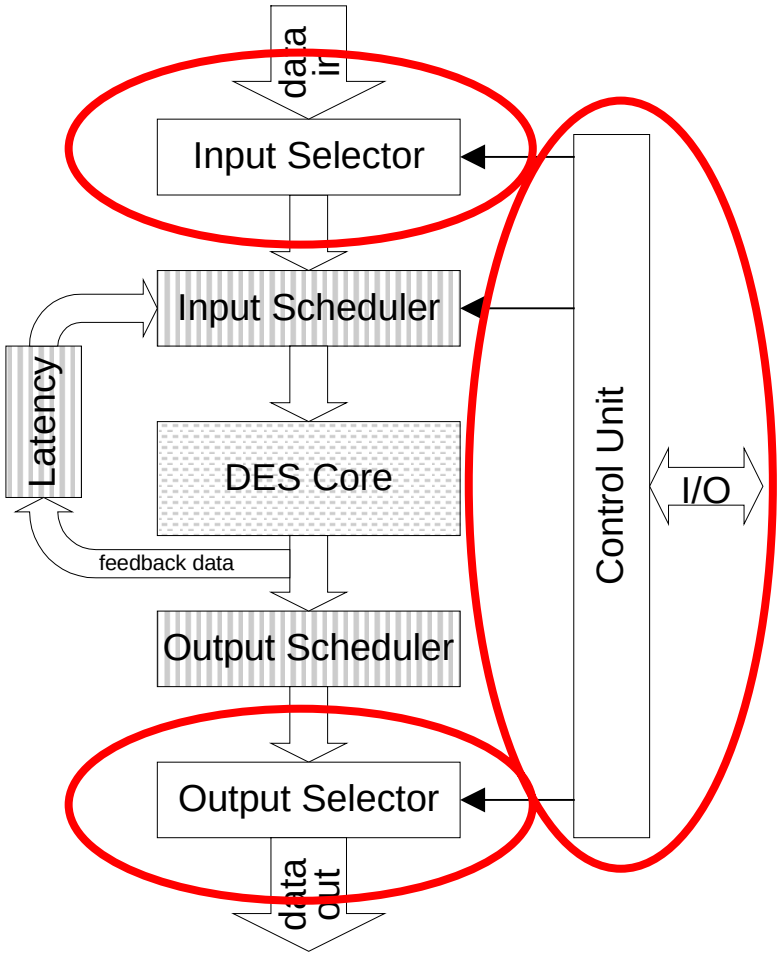
- Scheduler – TSPC handmade
- VHDL description needs register information
- Combining with DES core
- Verification



Realization DES Chip

- Control parts with standard synthesis
- VHDL description compiled to standard library

- Complete chip:
  Combination with TSPC parts
- Verification of behavior
- Verification of cycles



Discussion

- 12.8 GBit Triple DES chip (64 Bit @ 200 MHz)
- Three separated parts during synthesis
- Speed-up of the calculation intensive parts through TSPC
- All parts work to capacity – no bottleneck

- Very long TSPC pipeline (ca. 250 stages)
- Large area (no optimizations yet)

Summary

- Automatic design of dynamic logic with standard synthesis tools
- Example: GBit DES
- Disadvantages: very large area and high power consumption
- Demonstrates the possibility to speed up designs through extreme pipelining and using dynamic logic
- Compared with other realizations: large area, but high speed, standard synthesis