Kris Gaj and Pawel Chodowiec

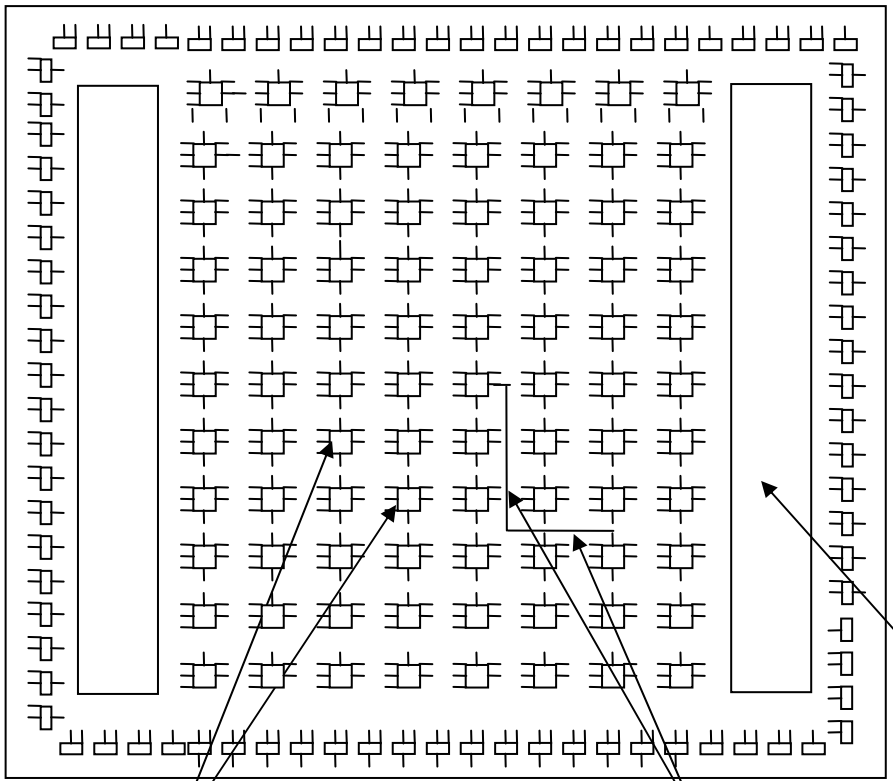
George Mason University

Comparison of the hardware performance of the AES candidates using reconfigurable hardware

http://ece.gmu.edu/crypto-text.htm

Target FPGA devices: High Performance

Virtex - XCV 1000



- 0.22 μm CMOS process
- 12 288 CLB slices
- 1 mln equivalent logic gates
- Up to 200 MHz clock

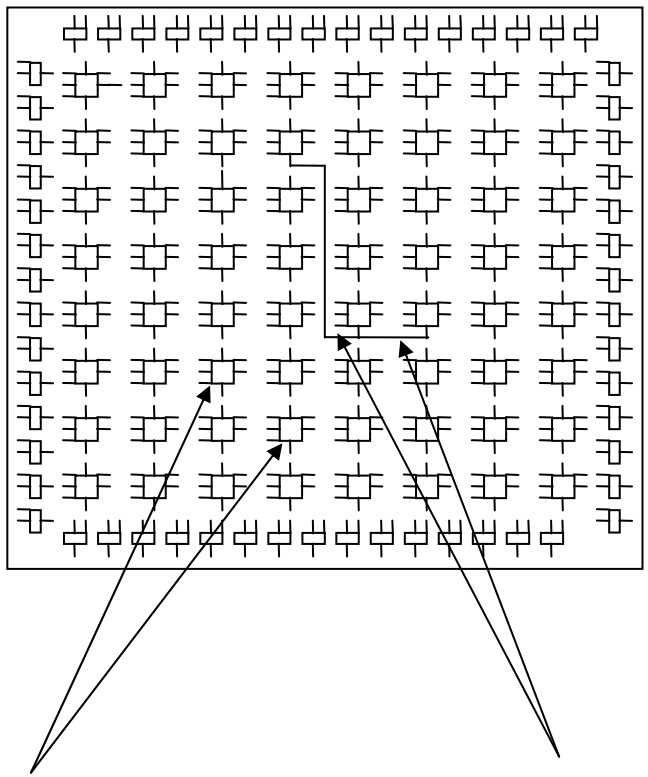
Block RAMs

Configurable Logic Block slices (CLB slices)

Programmable Interconnects

Target FPGA devices: Low Cost

XC4000XL - XC4085XL



Configurable Logic Blocks (CLBs)

Programmable Interconnects

- 0.35 μm CMOS process
- 3136 CLBs
- 180,000 equivalent logic gates
- Up to 80 MHz clock

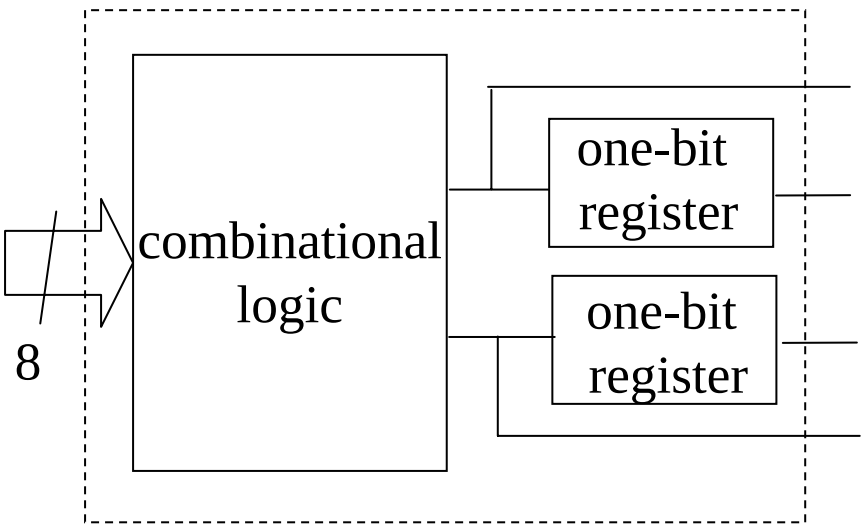
Basic building blocks of FPGA devices

Virtex **XC4000XL**

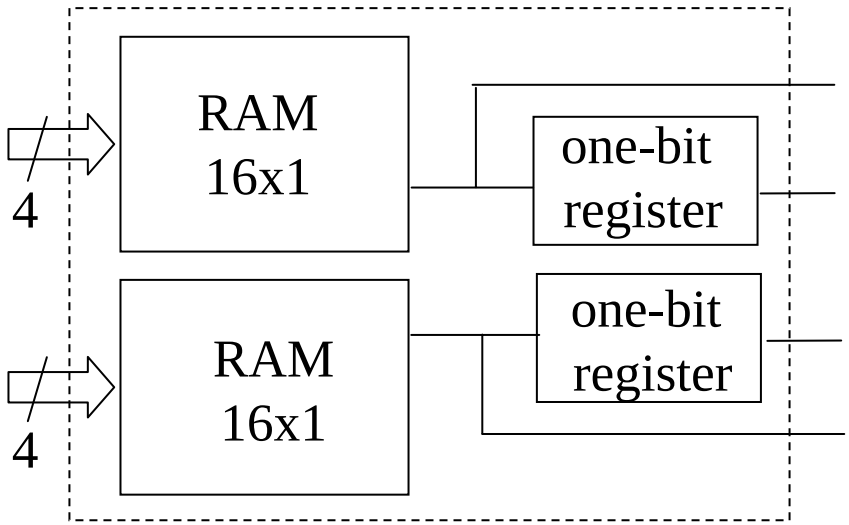
CLB slice ≡ **CLB**

CLB - Configurable Logic Block

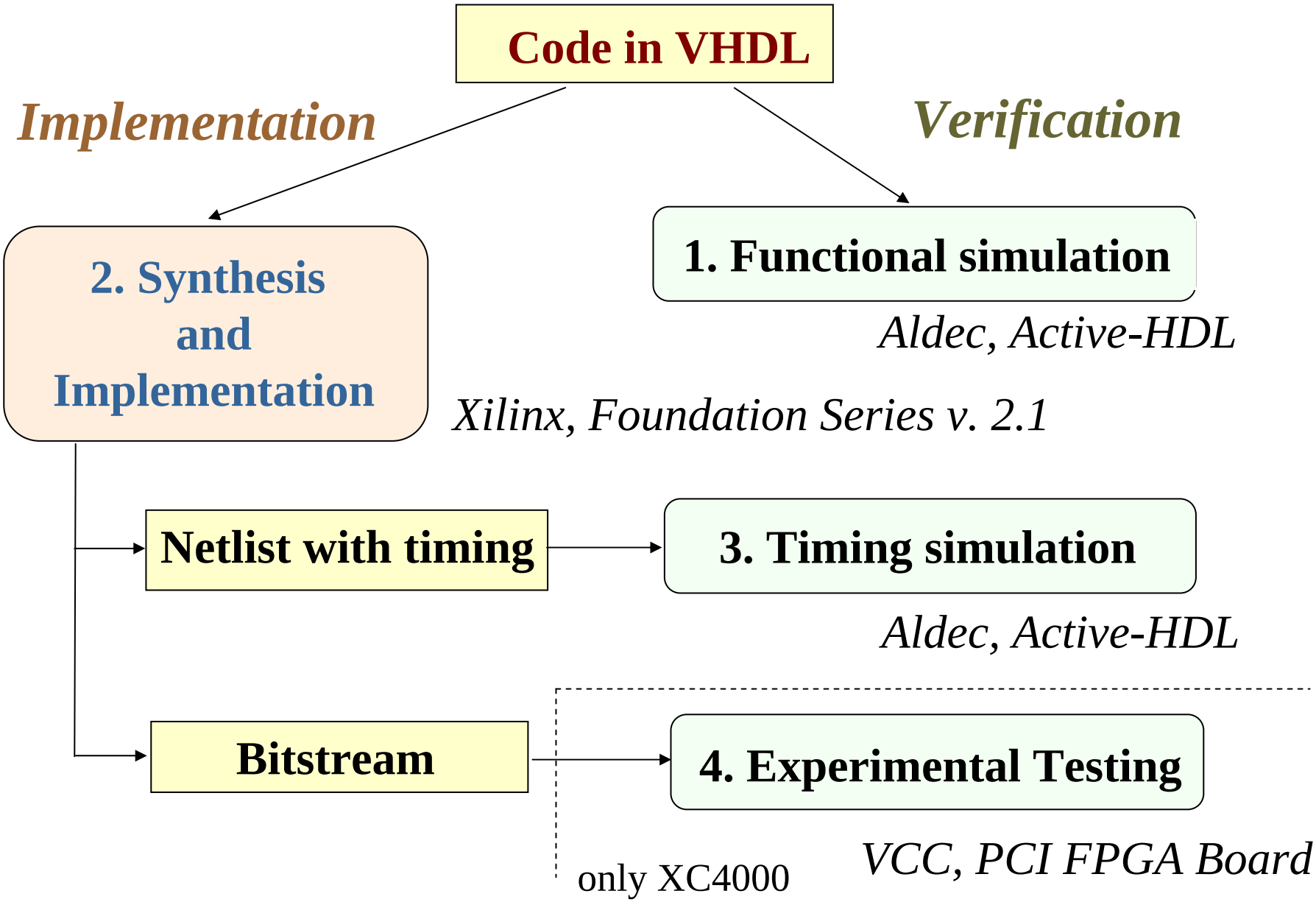
Logic mode



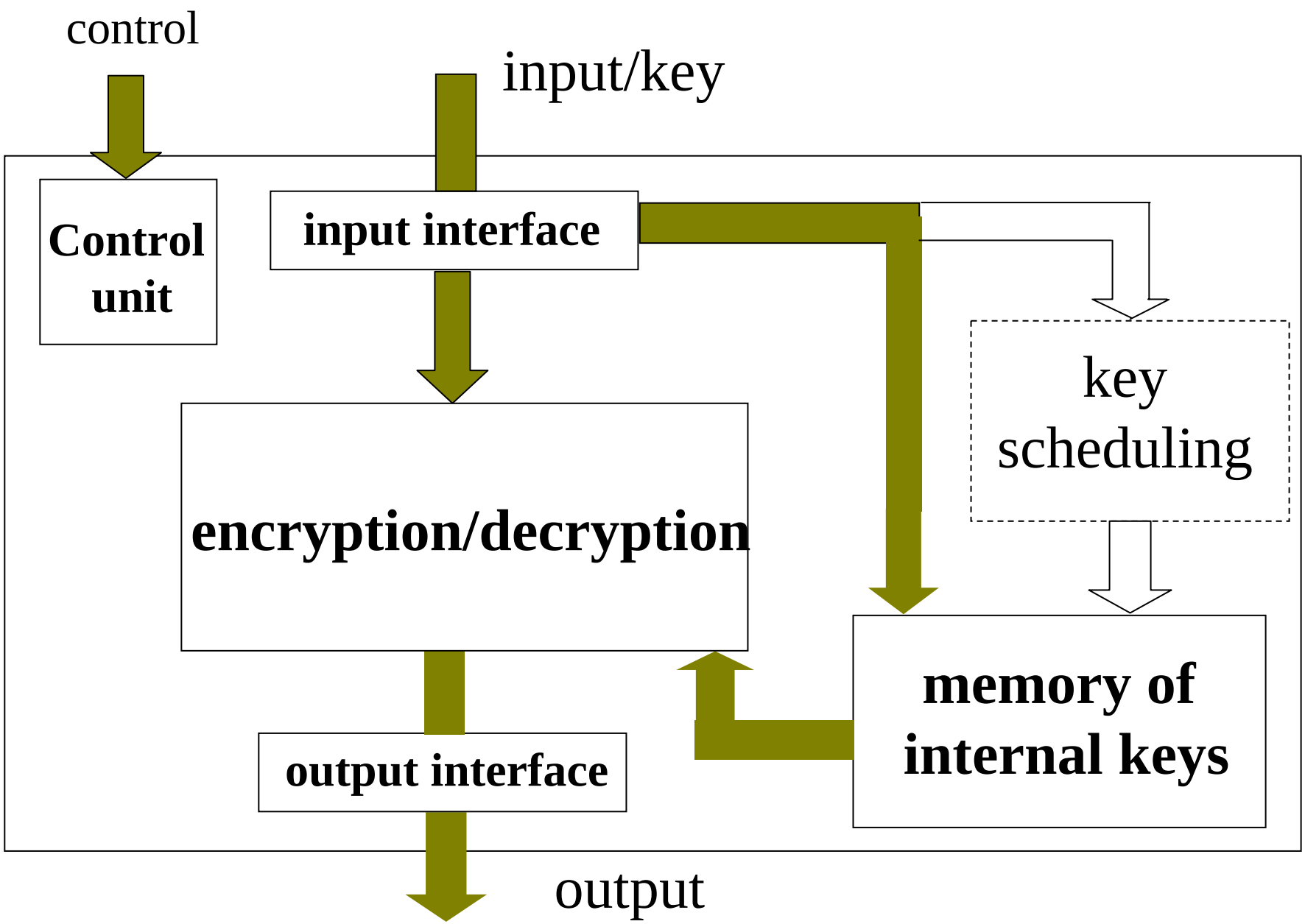
Memory mode



Methodology and Tools

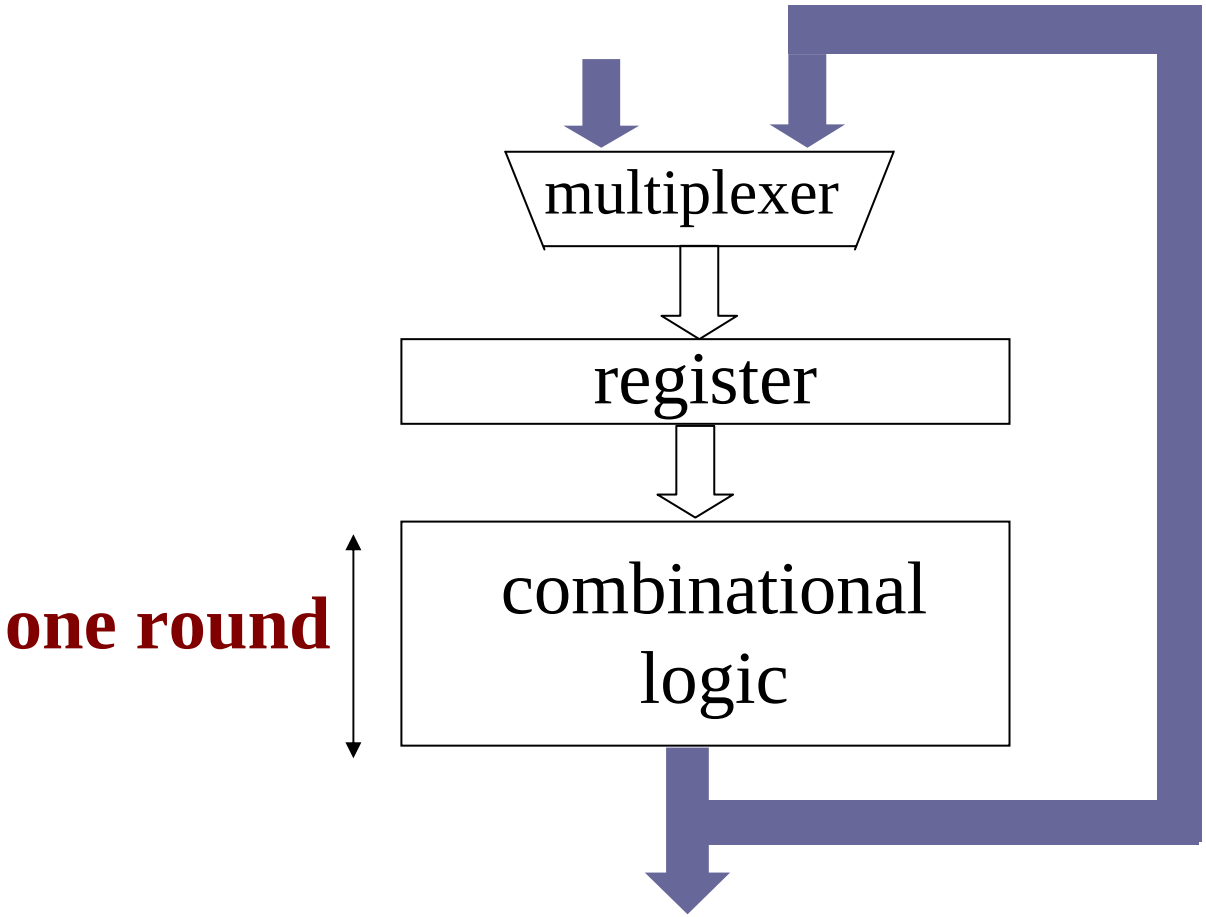


Top level block diagram

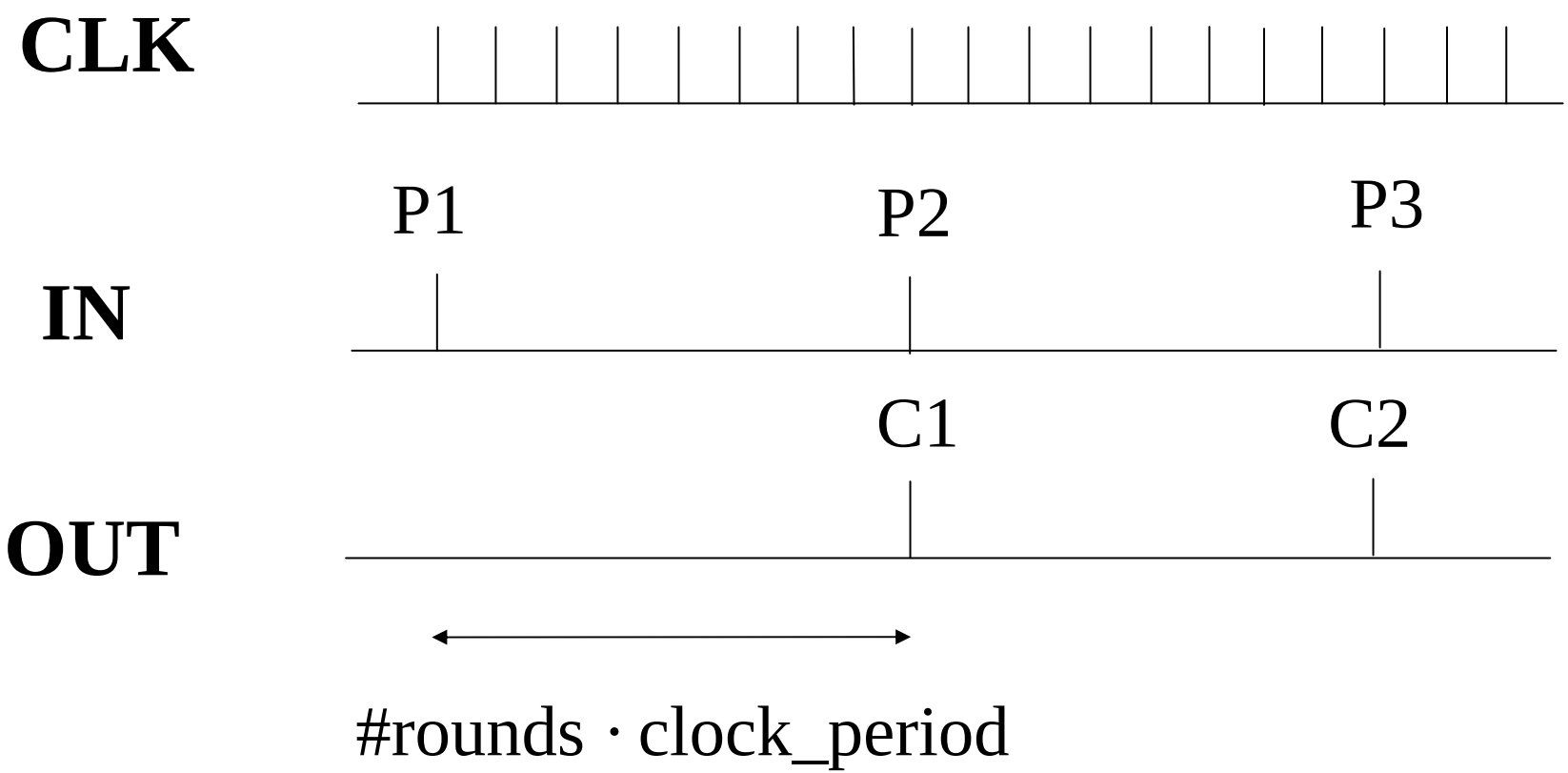


Basic architecture

WPI: Iterative Looping, LU-1 **NSA:** Iterative Architecture
USC: Single-Round Based

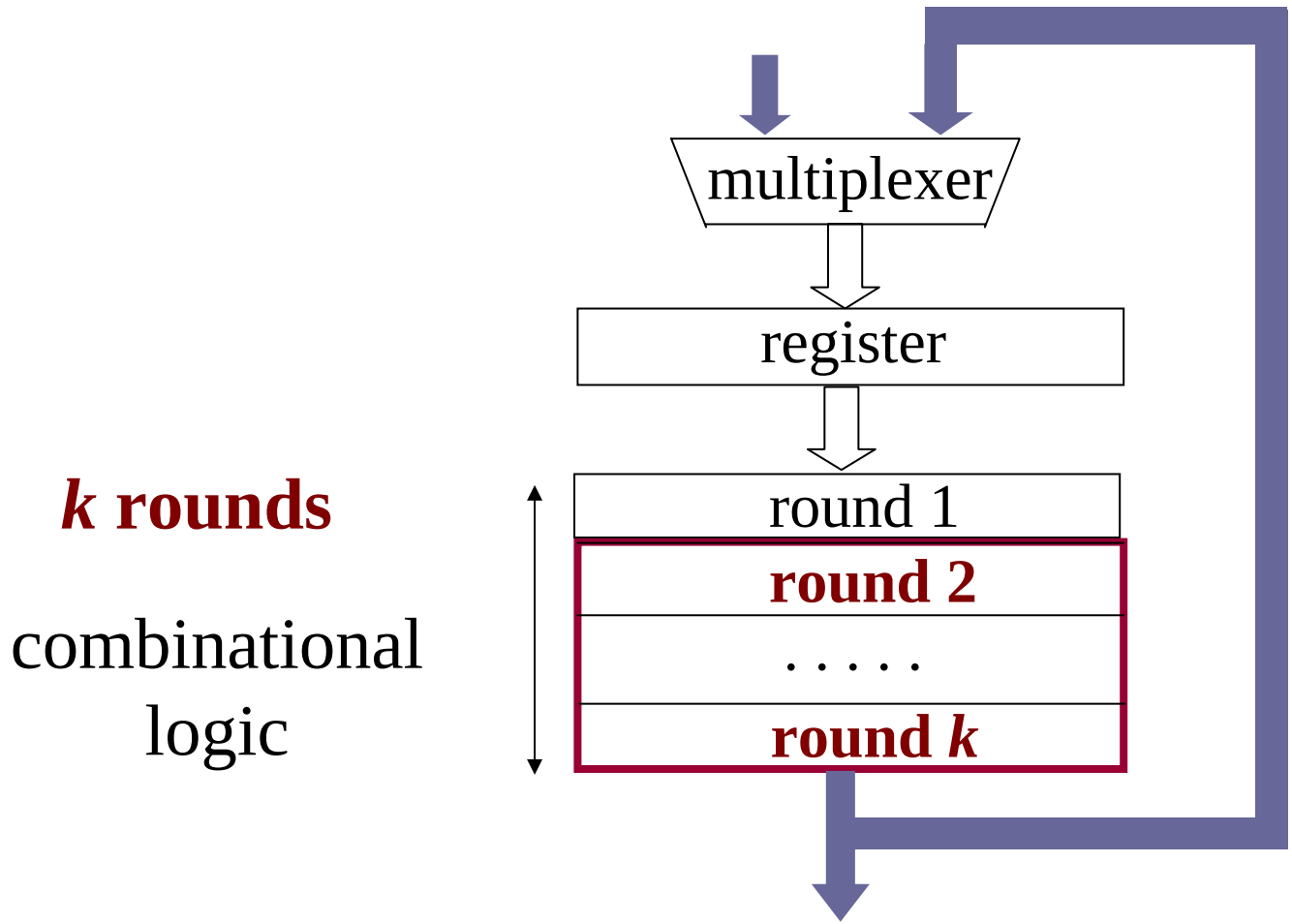


Basic architecture: Timing

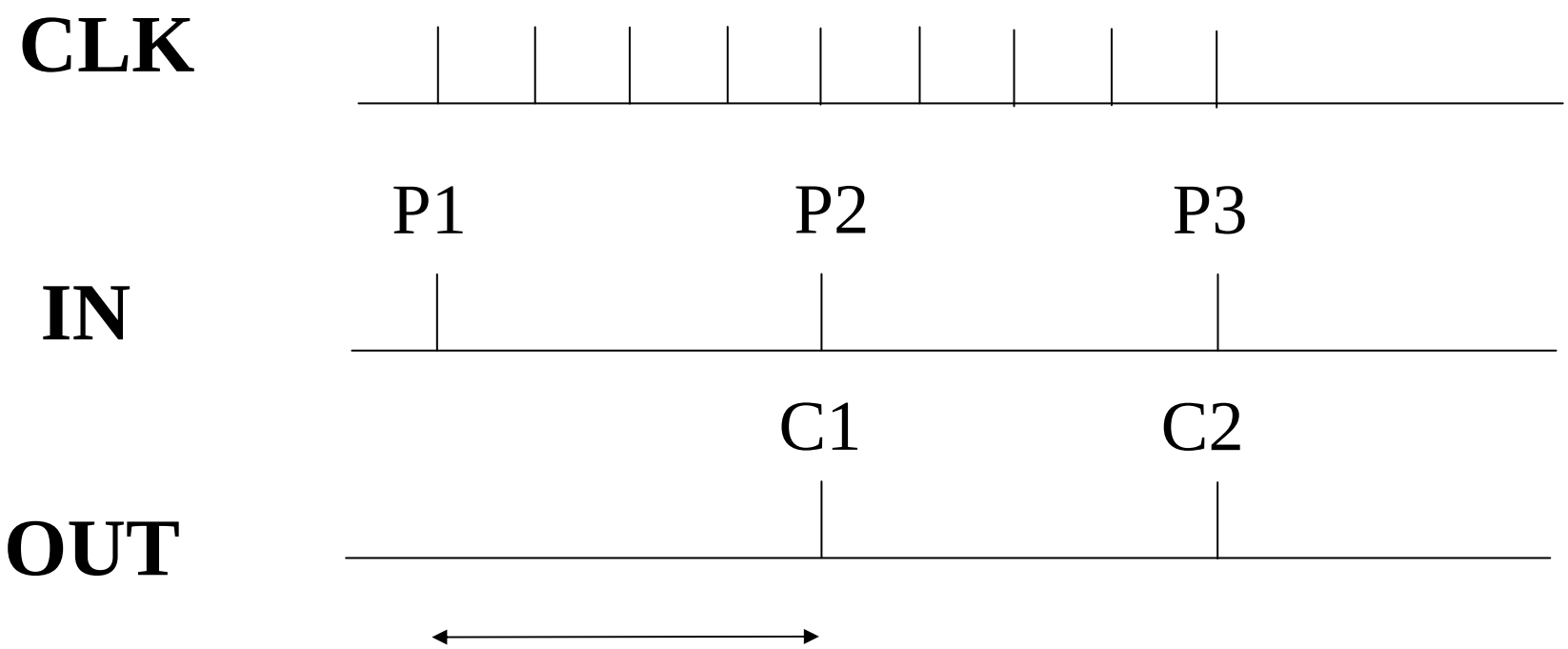


k-rounds Loop Unrolling

WPI: Loop Unrolling, LU-*k*

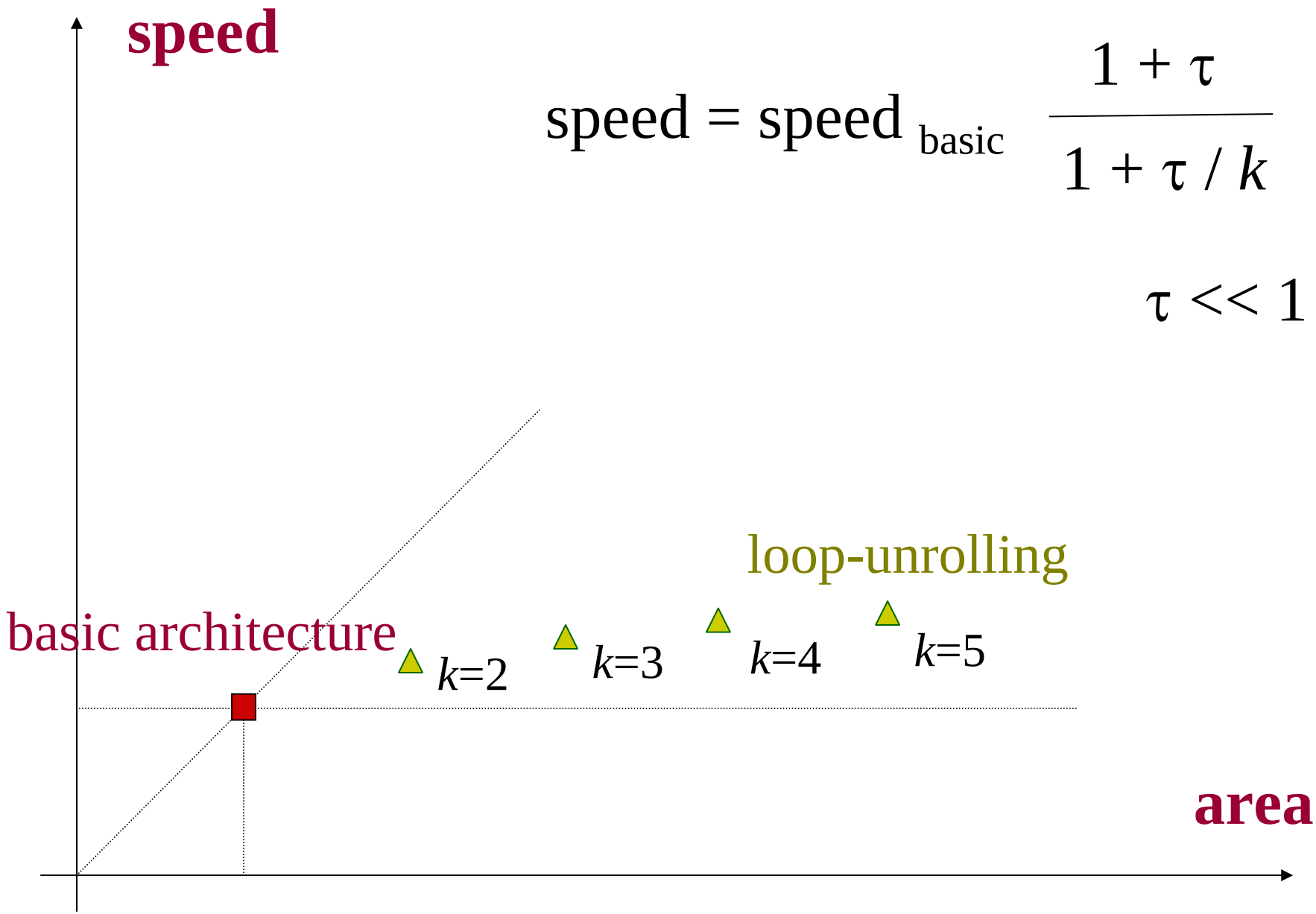


Loop Unrolling: Timing



#rounds/k · extended_clock_period

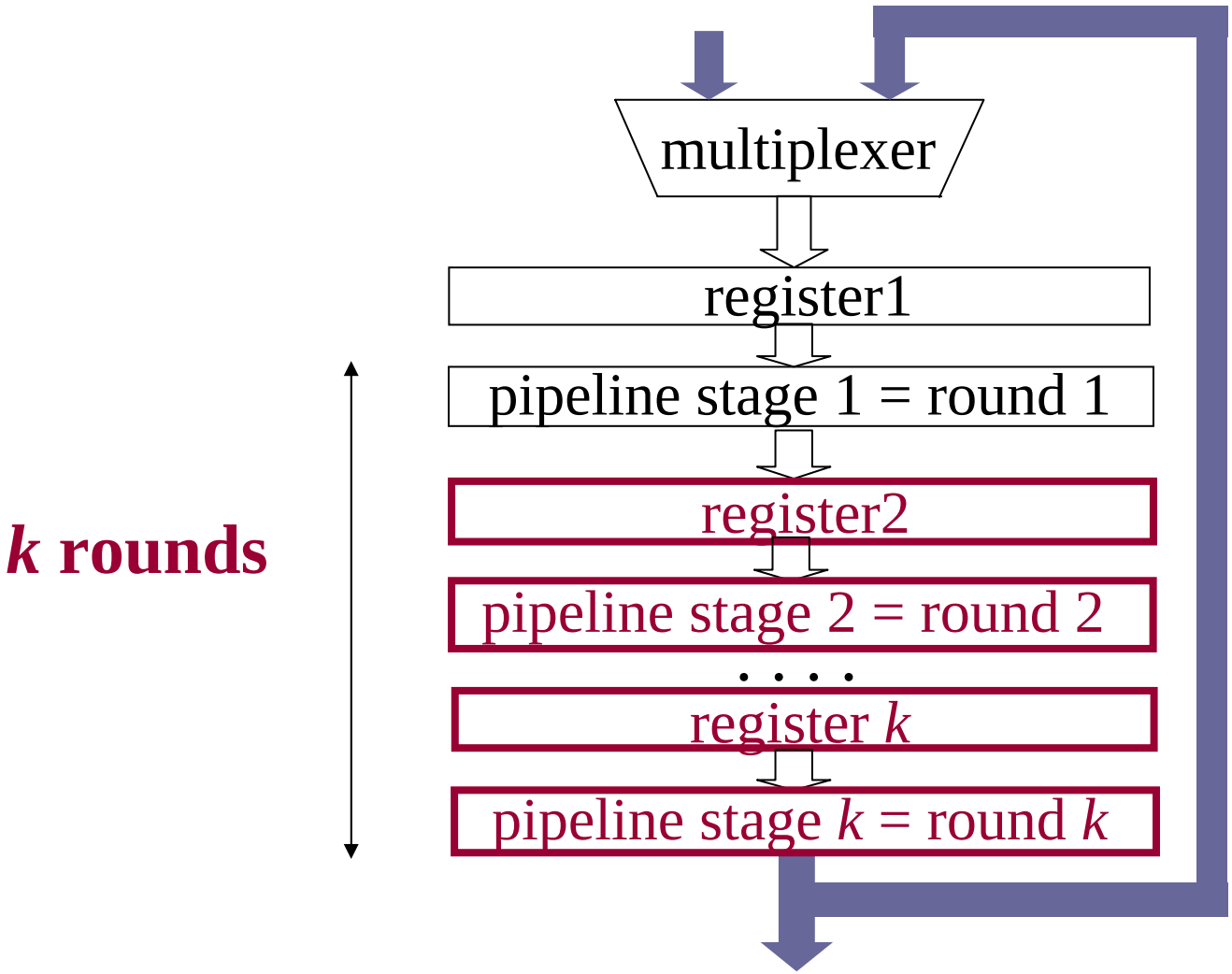
Loop Unrolling: Speed vs. Area



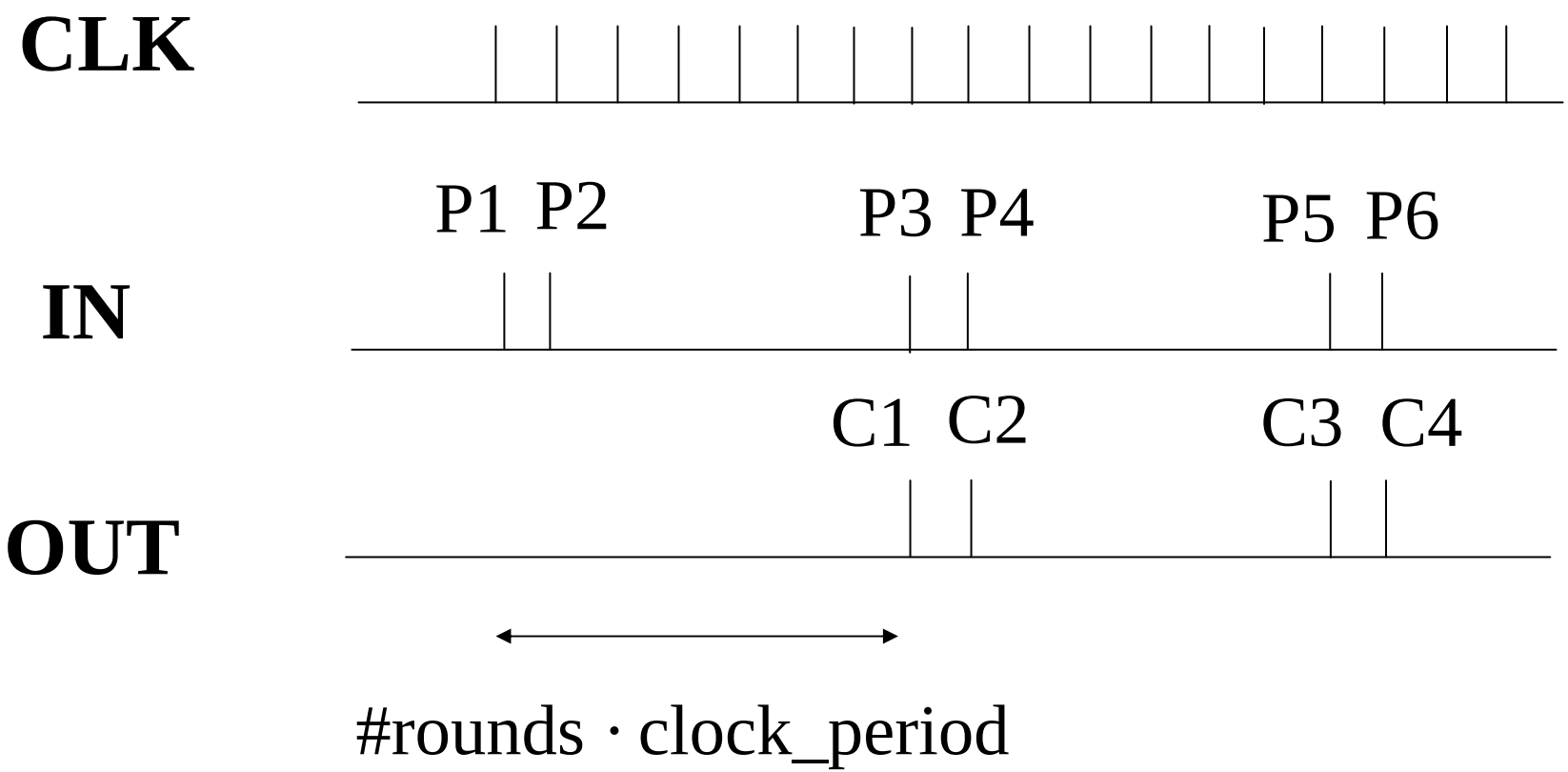
k-stage Outer-Round Pipelining

WPI: Partial Pipelining, PP-*k* **NSA:** Pipelined Architecture

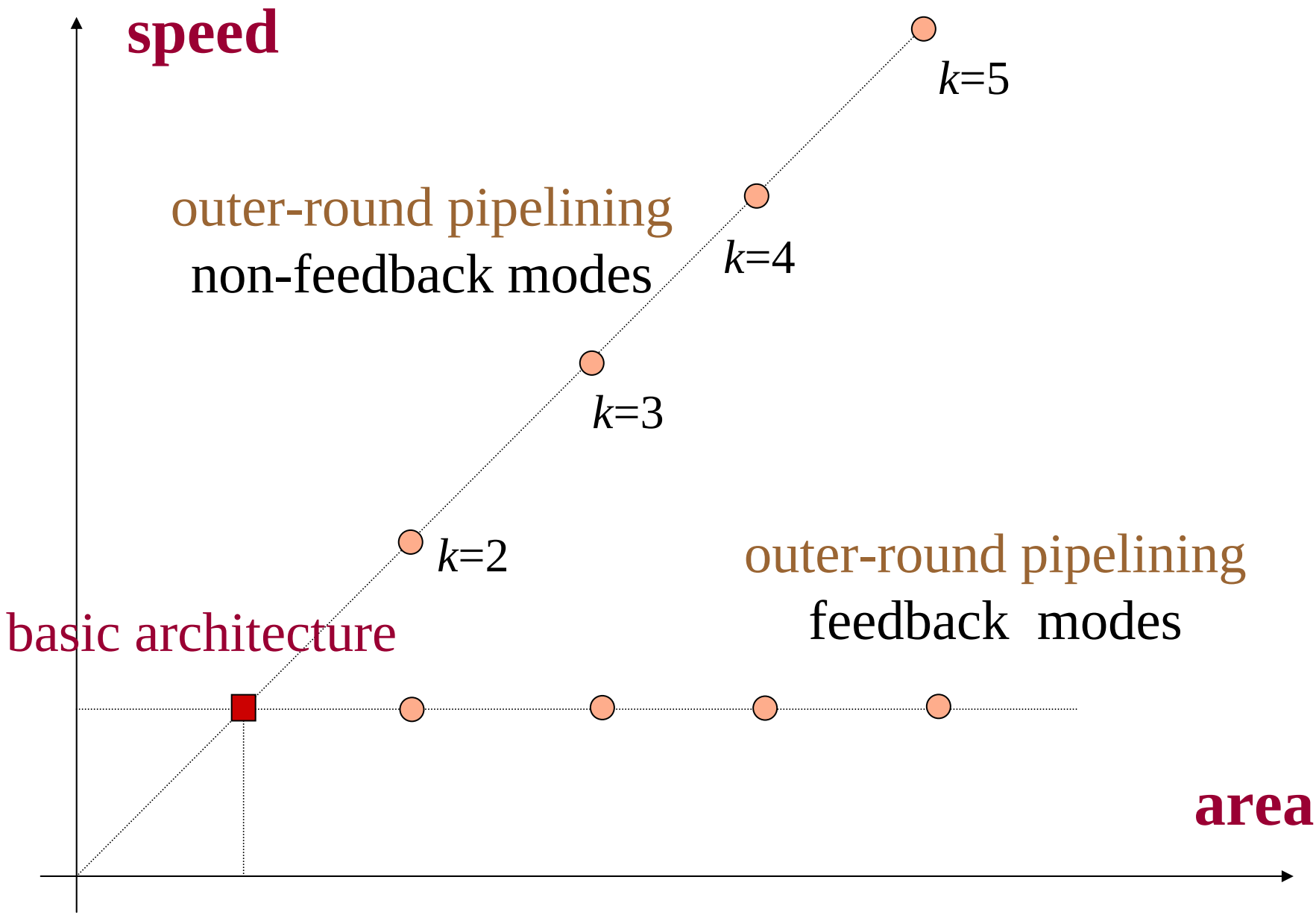
UC Berkeley: Unrolled Pipeline



Outer-Round Pipelining: Timing



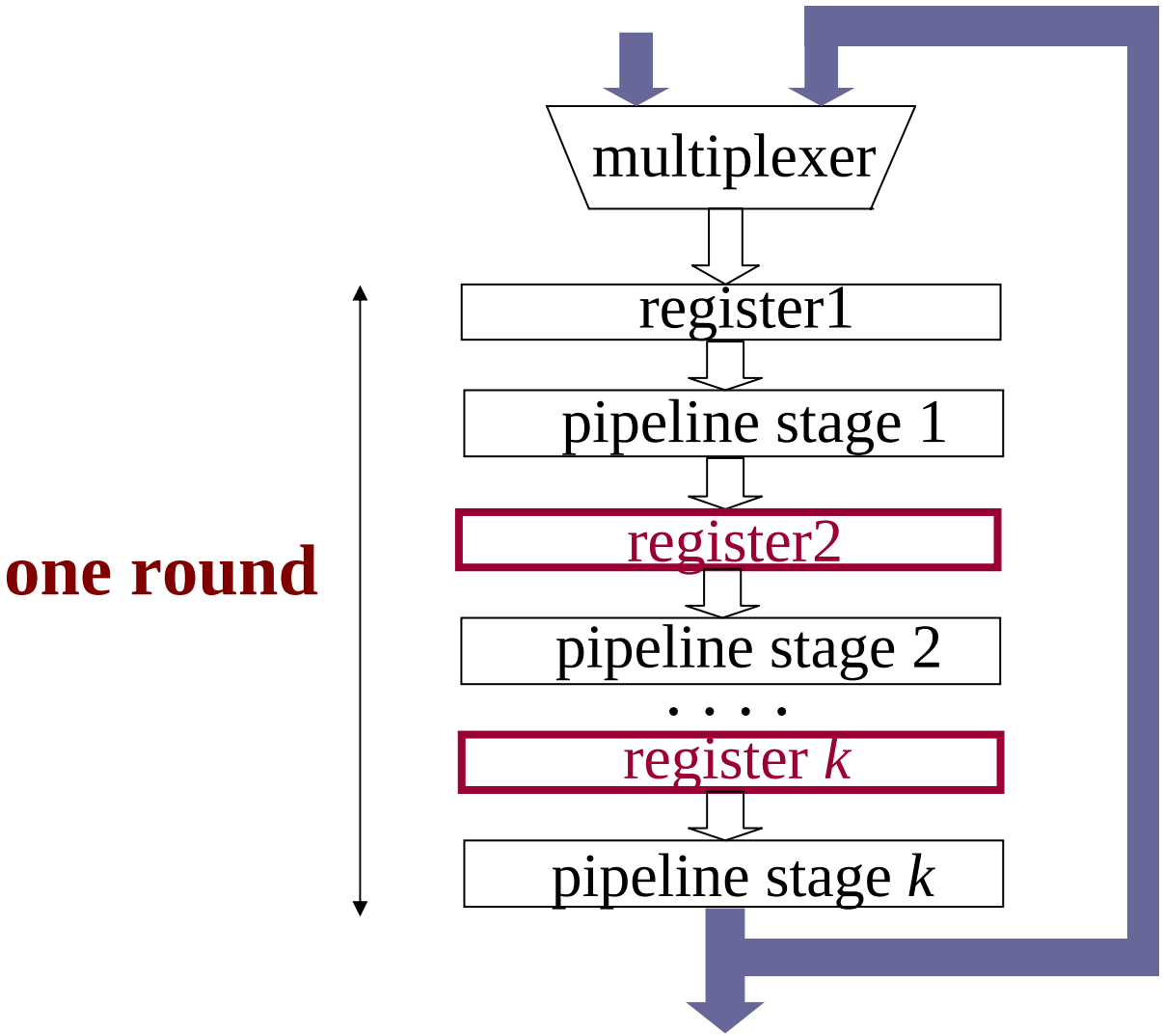
Outer-Round Pipelining: Speed vs. Area



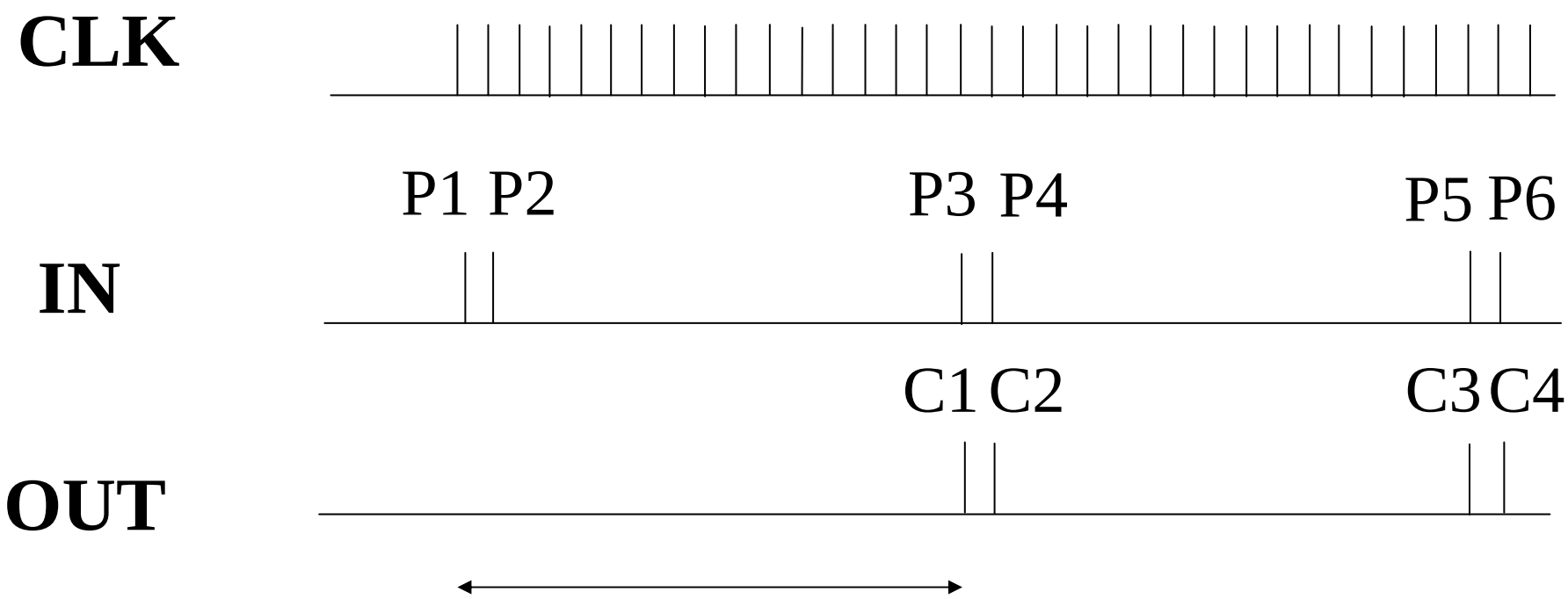
k-stage Inner-Round Pipelining

UC Berkeley: *C*-Slow single round datapath (*C*=*k*)

WPI: Sub-Pipelining, SP-1-*y* (*y*=*k*-1)

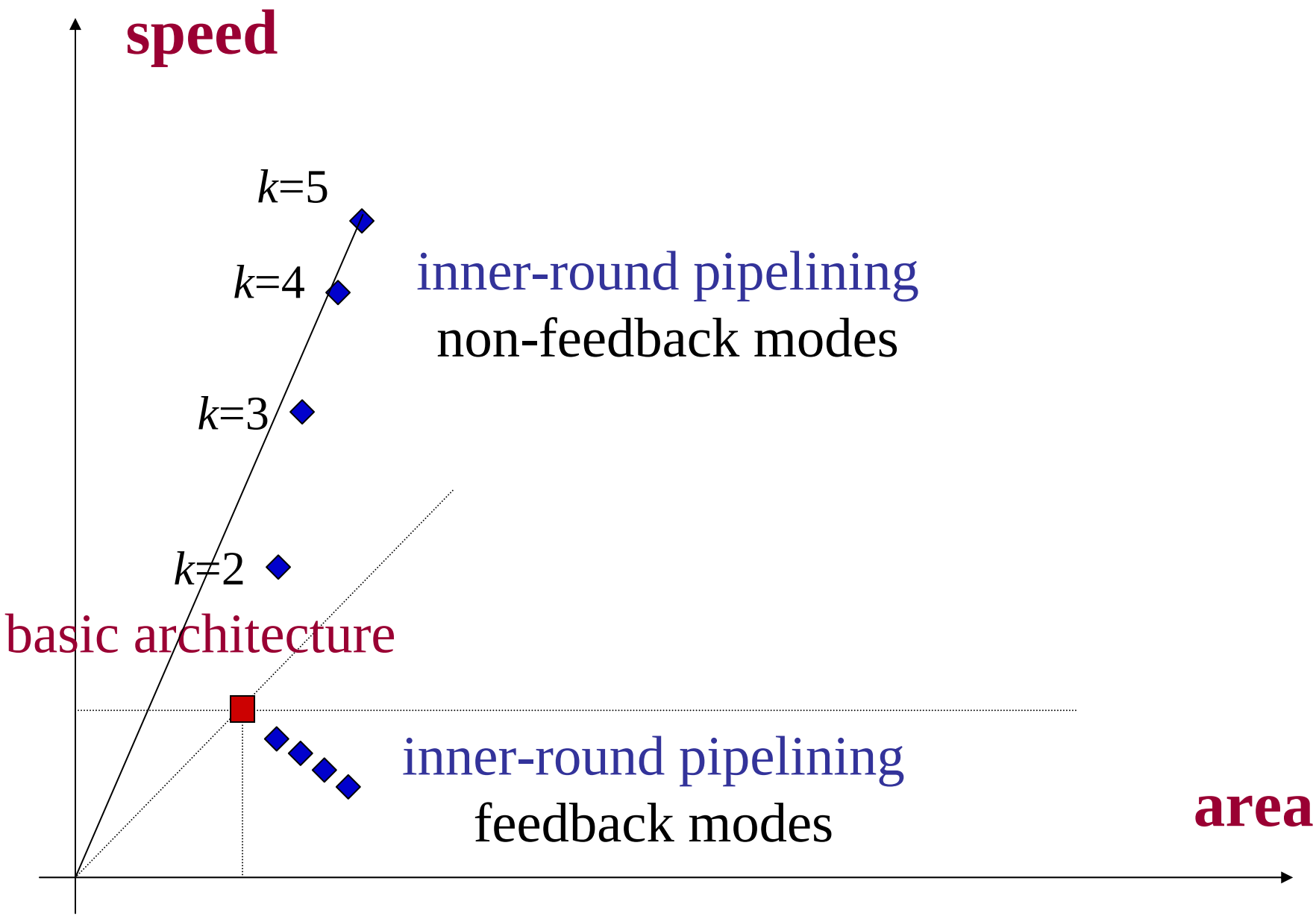


Inner-Round Pipelining: Timing



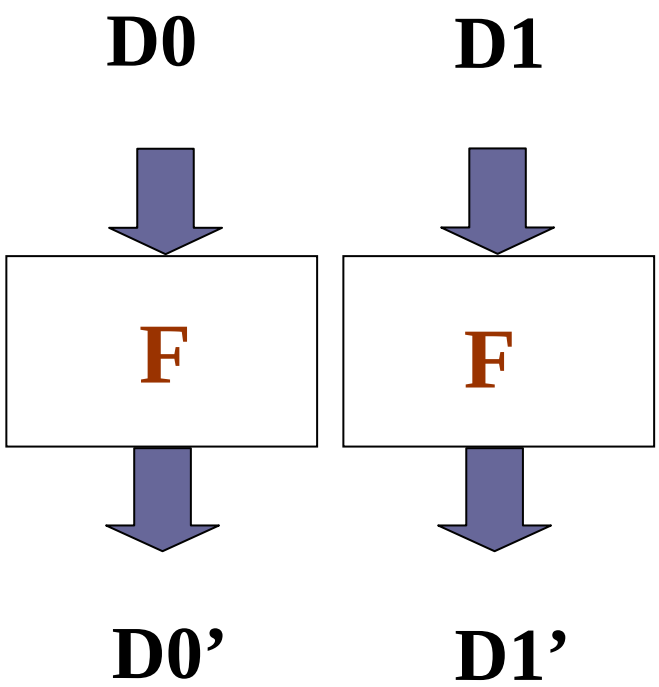
#rounds · (*k* · reduced_clock_period)

Inner-Round Pipelining: Speed vs. Area

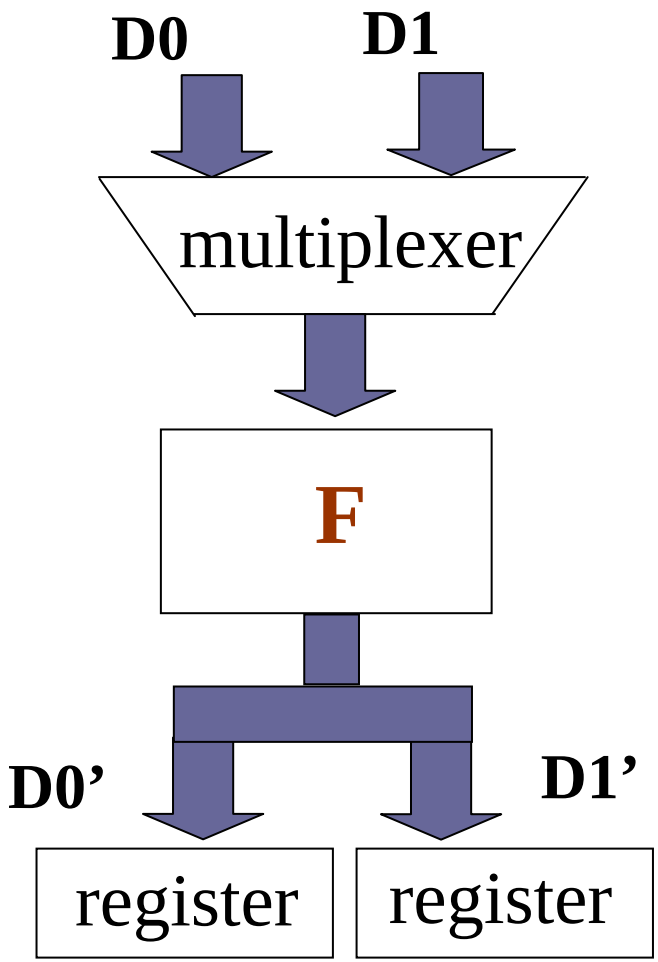


Resource Sharing

Before



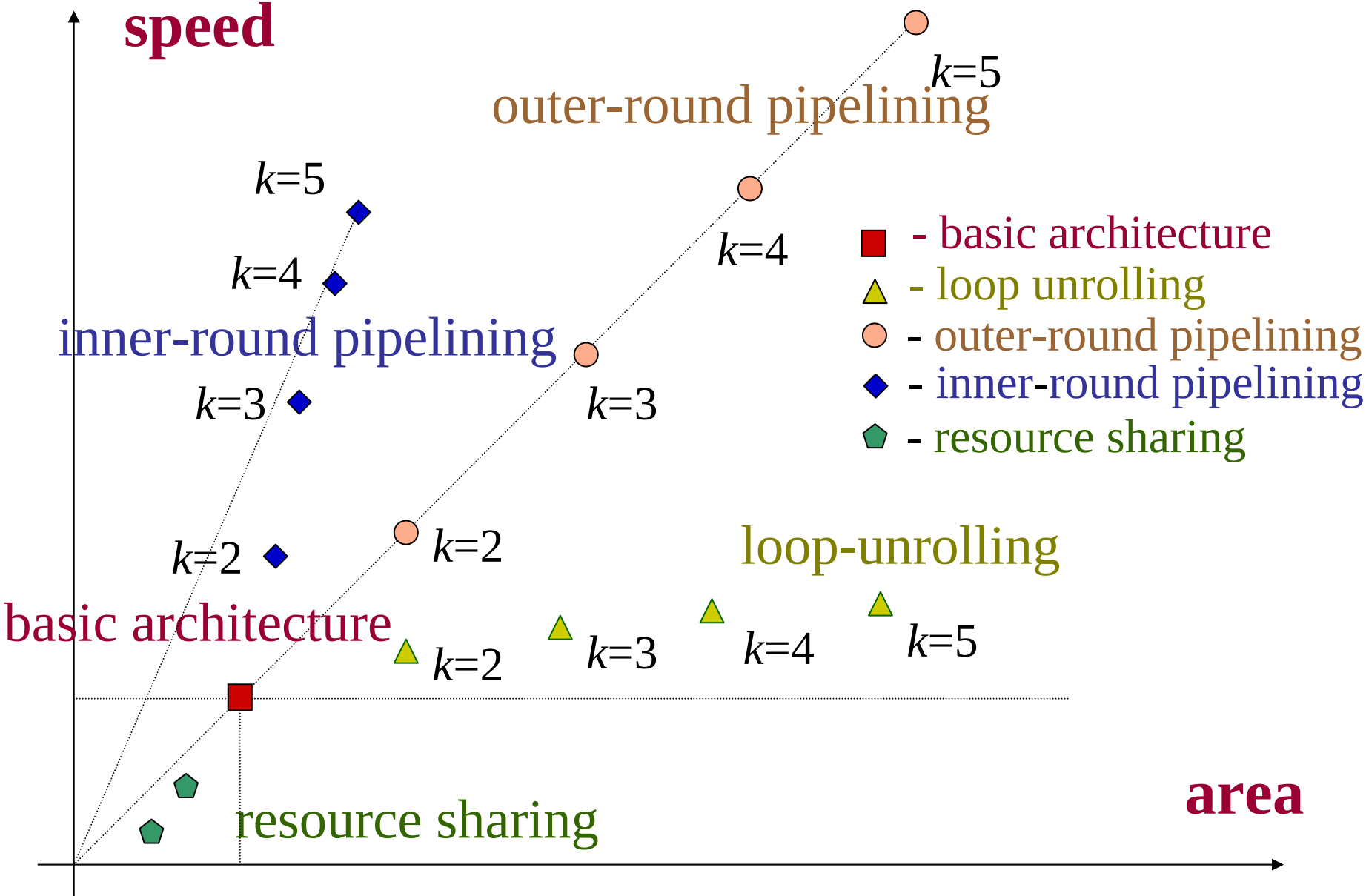
After



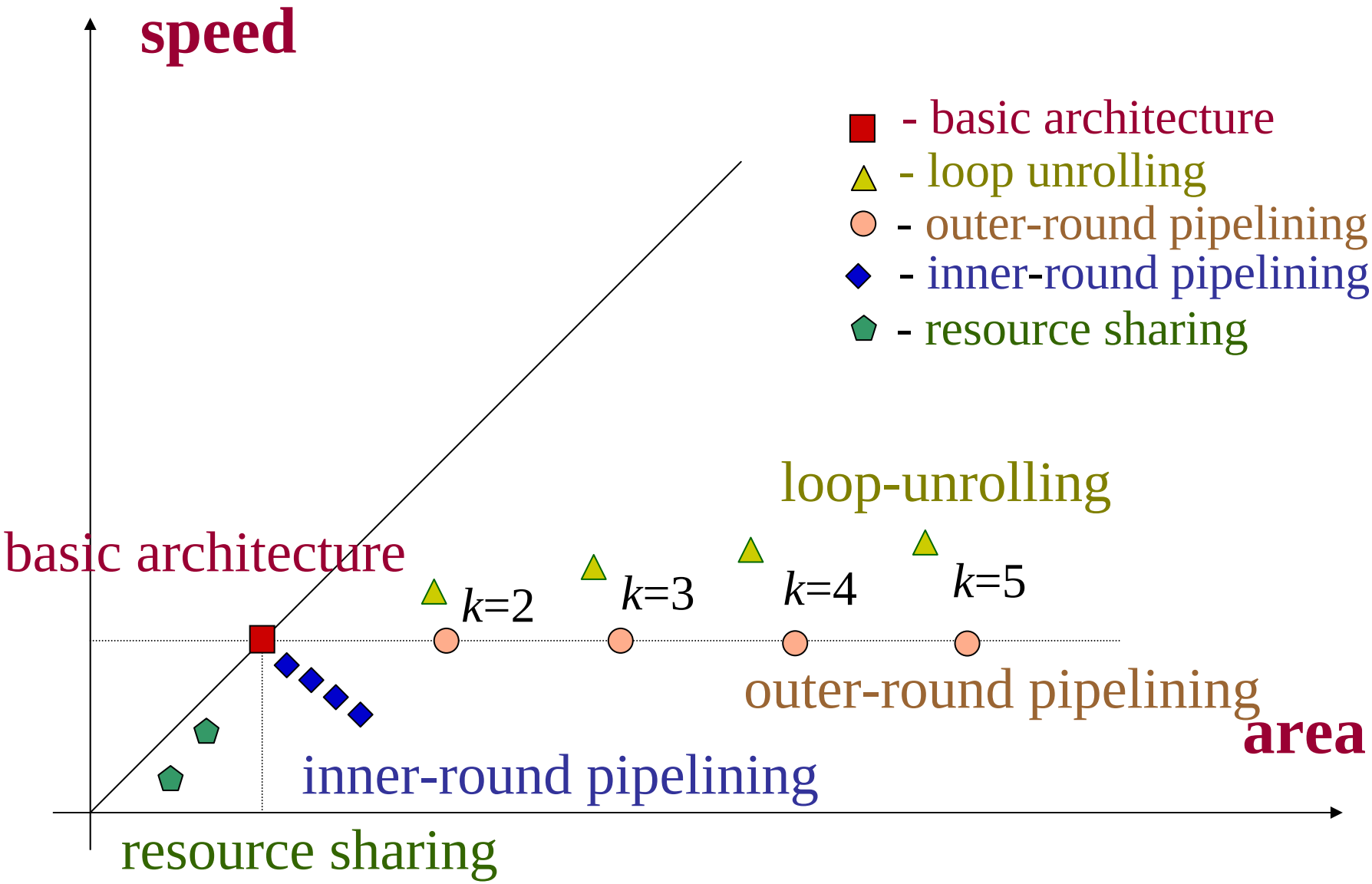
Examples of functions F that can be shared

Twofish:	h-function
RC6:	half-round
Mars:	S-boxes S0, S1 8x32, partial products reduction tree in the multiplier
Serpent:	16 S-boxes 4x4
Rijndael:	8 S-boxes 8x8

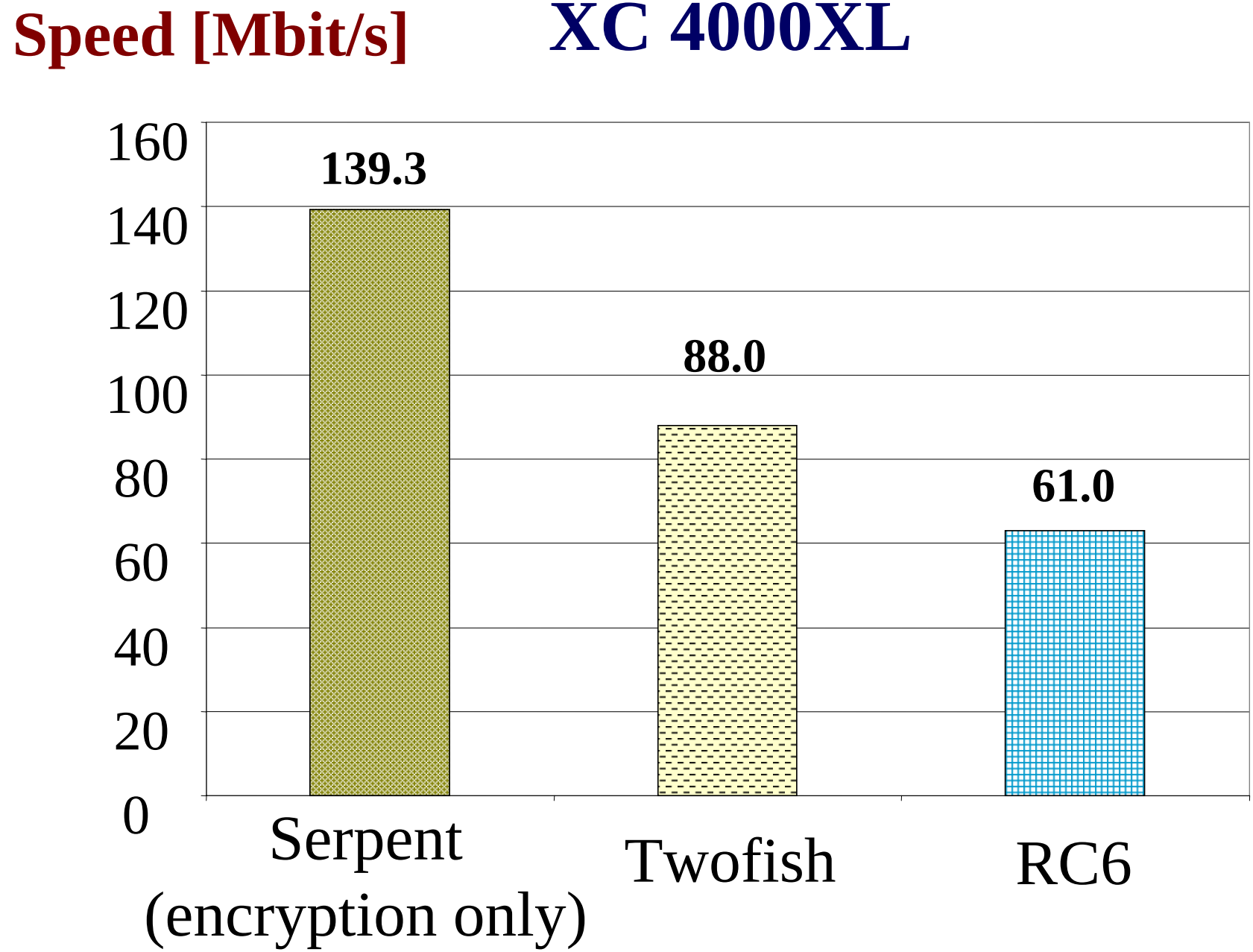
Performance of alternative architectures: in non-feedback cipher modes (ECB, counter)



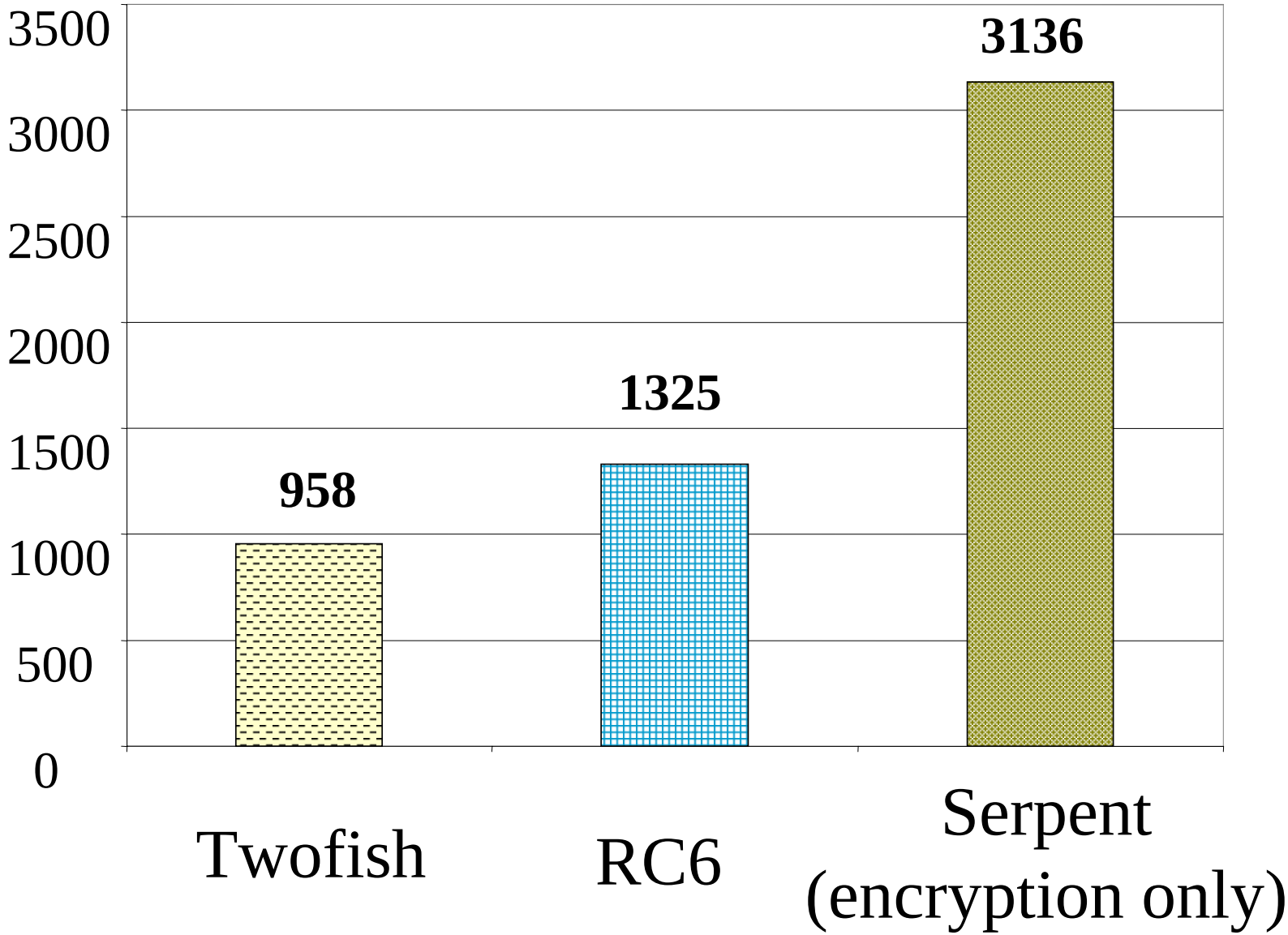
Performance of alternative architectures: in feedback cipher modes (CBC, CFB, OFB)



Basic architecture: Speed
XC 4000XL

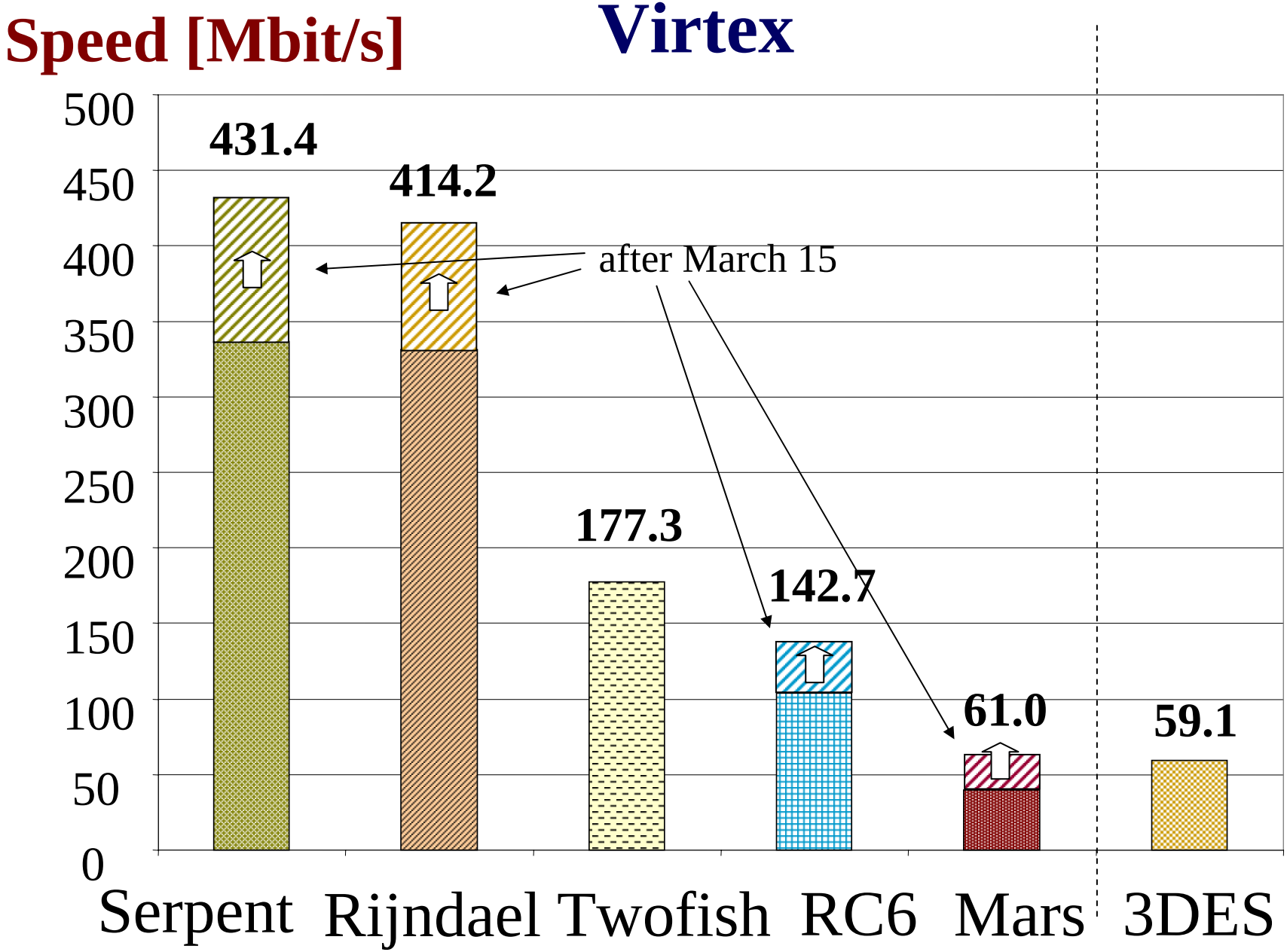


Basic architecture: Area
XC 4000XL



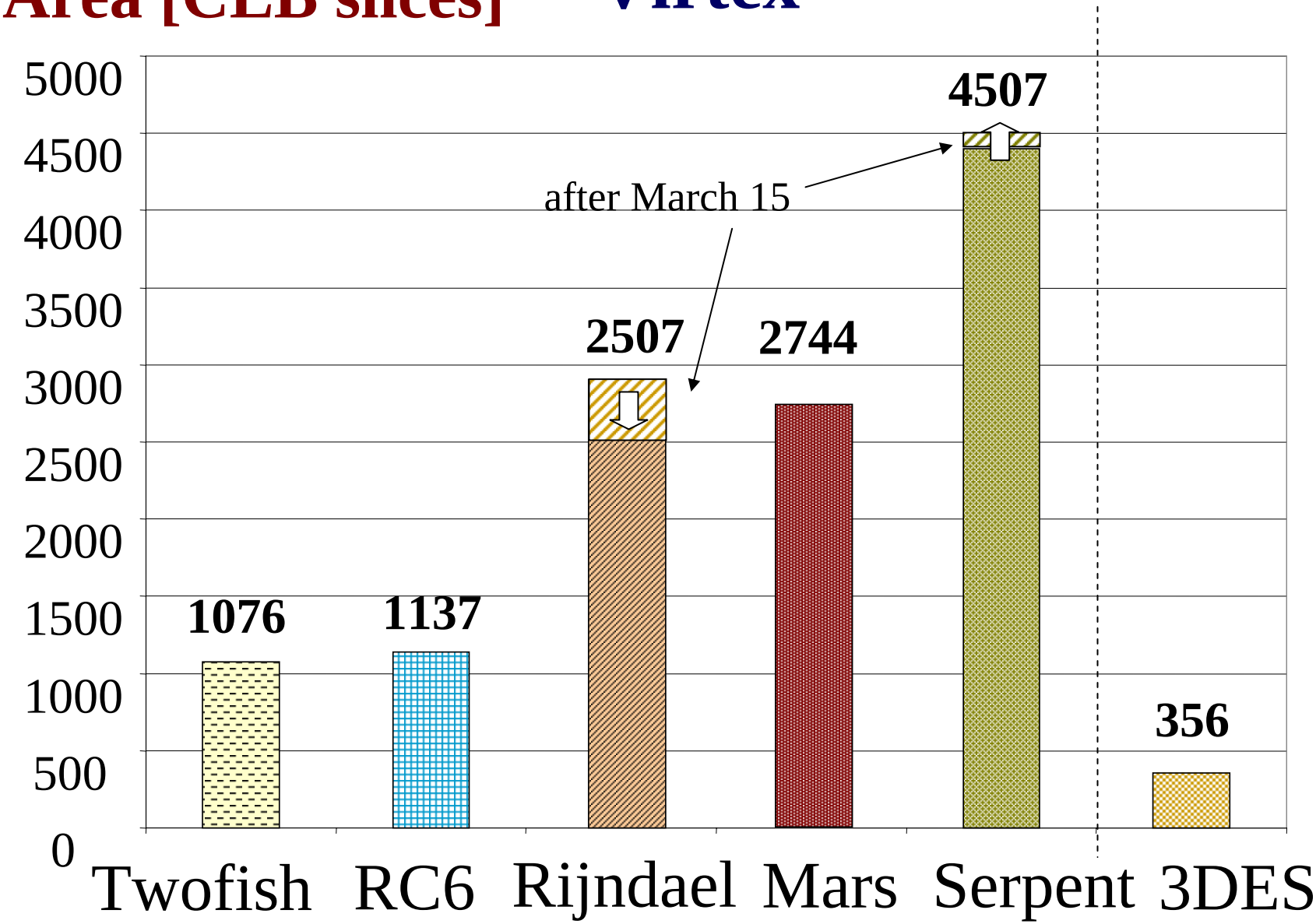
Basic architecture: Speed

Virtex

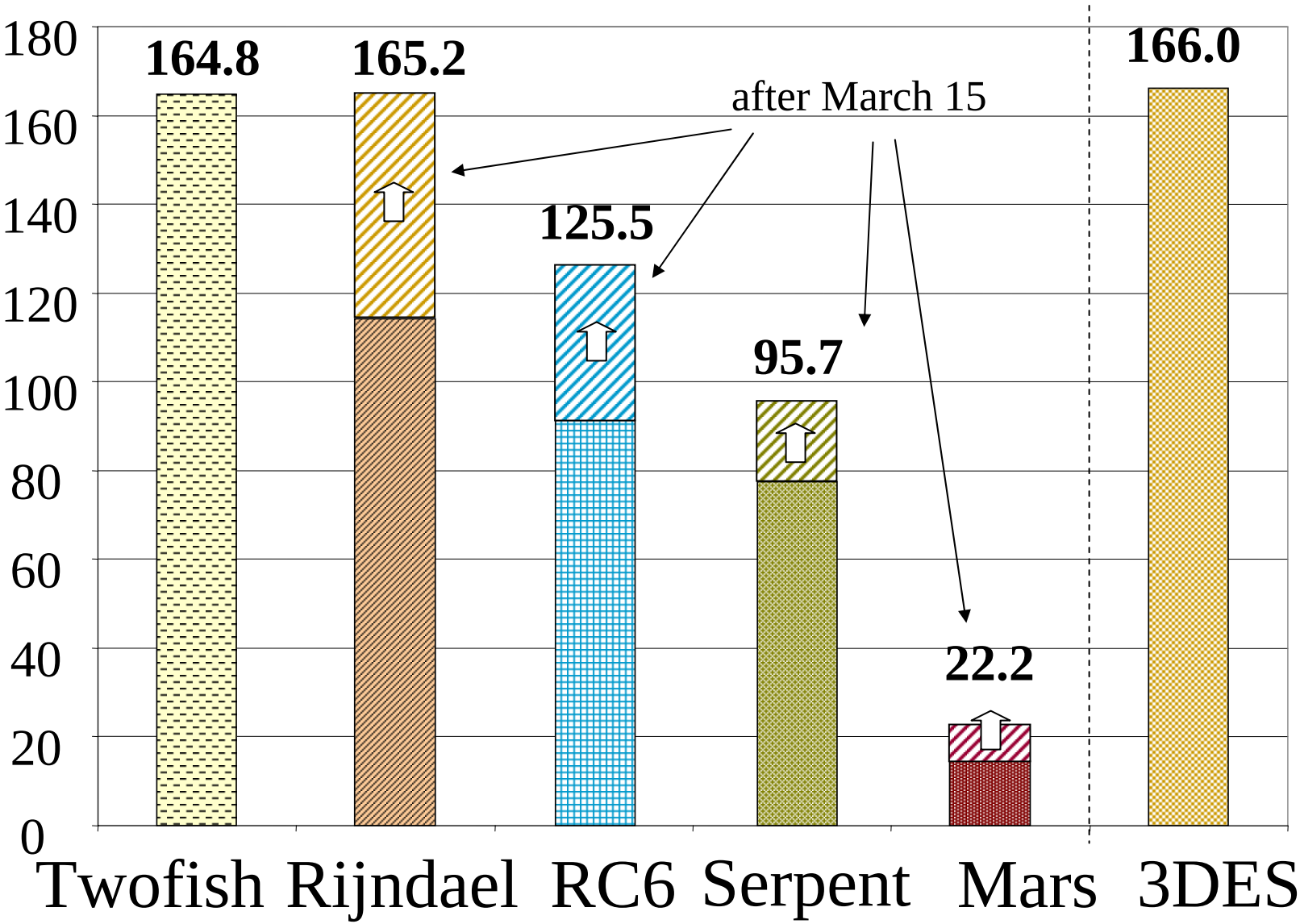


Basic architecture: Area

Virtex

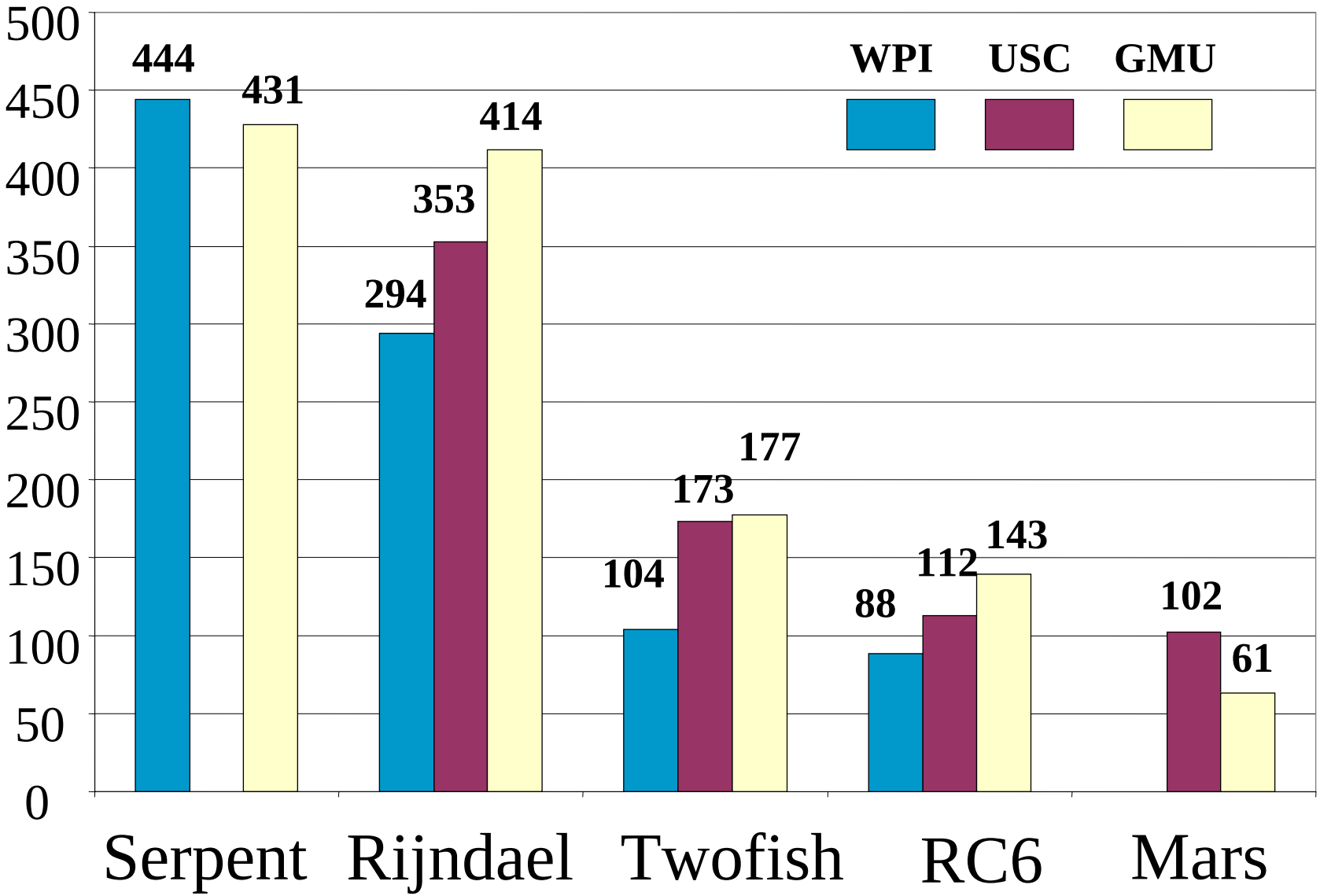


Basic architecture: Speed/Area



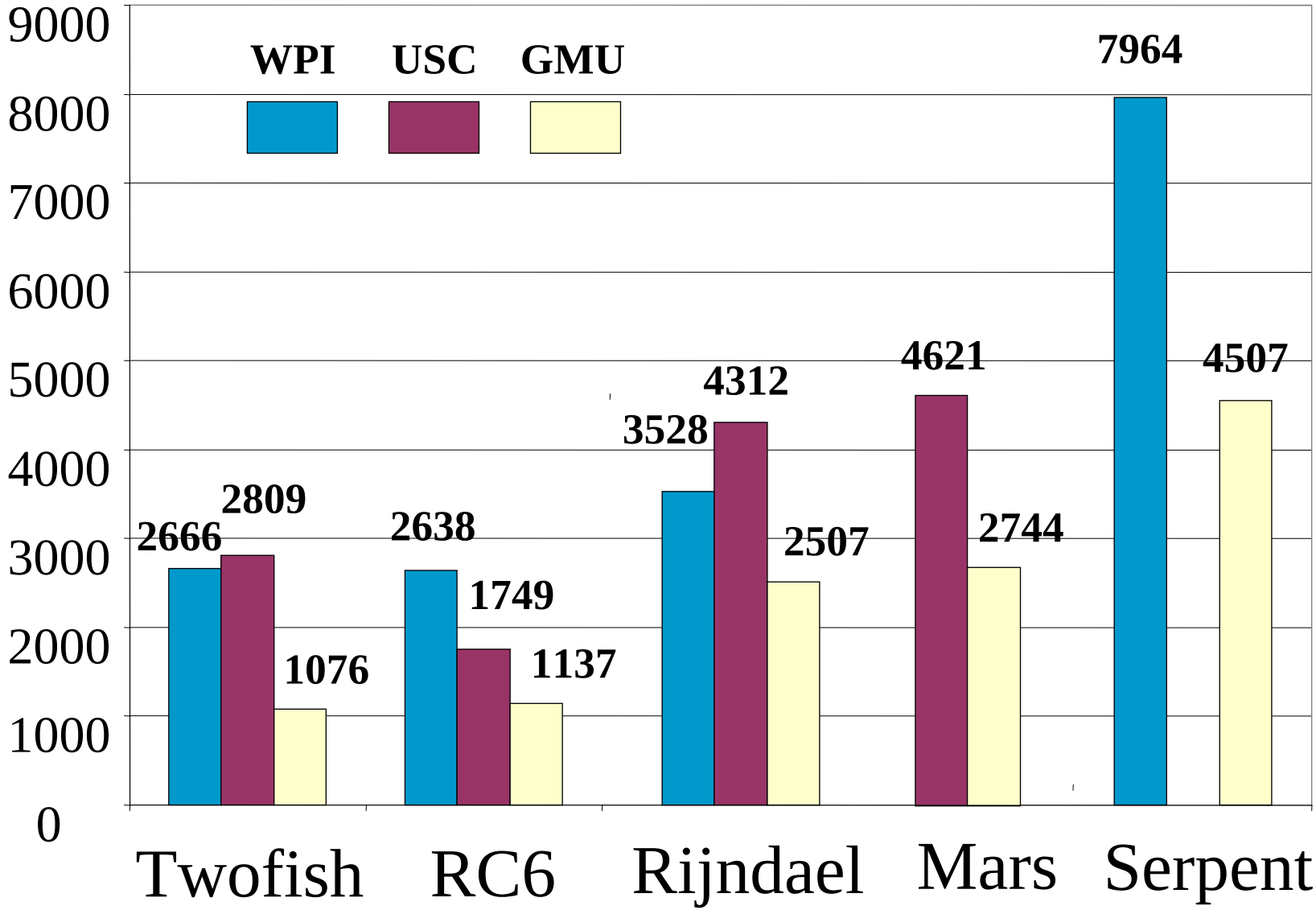
Comparison with results of other groups: Speed

Speed [Mbit/s]

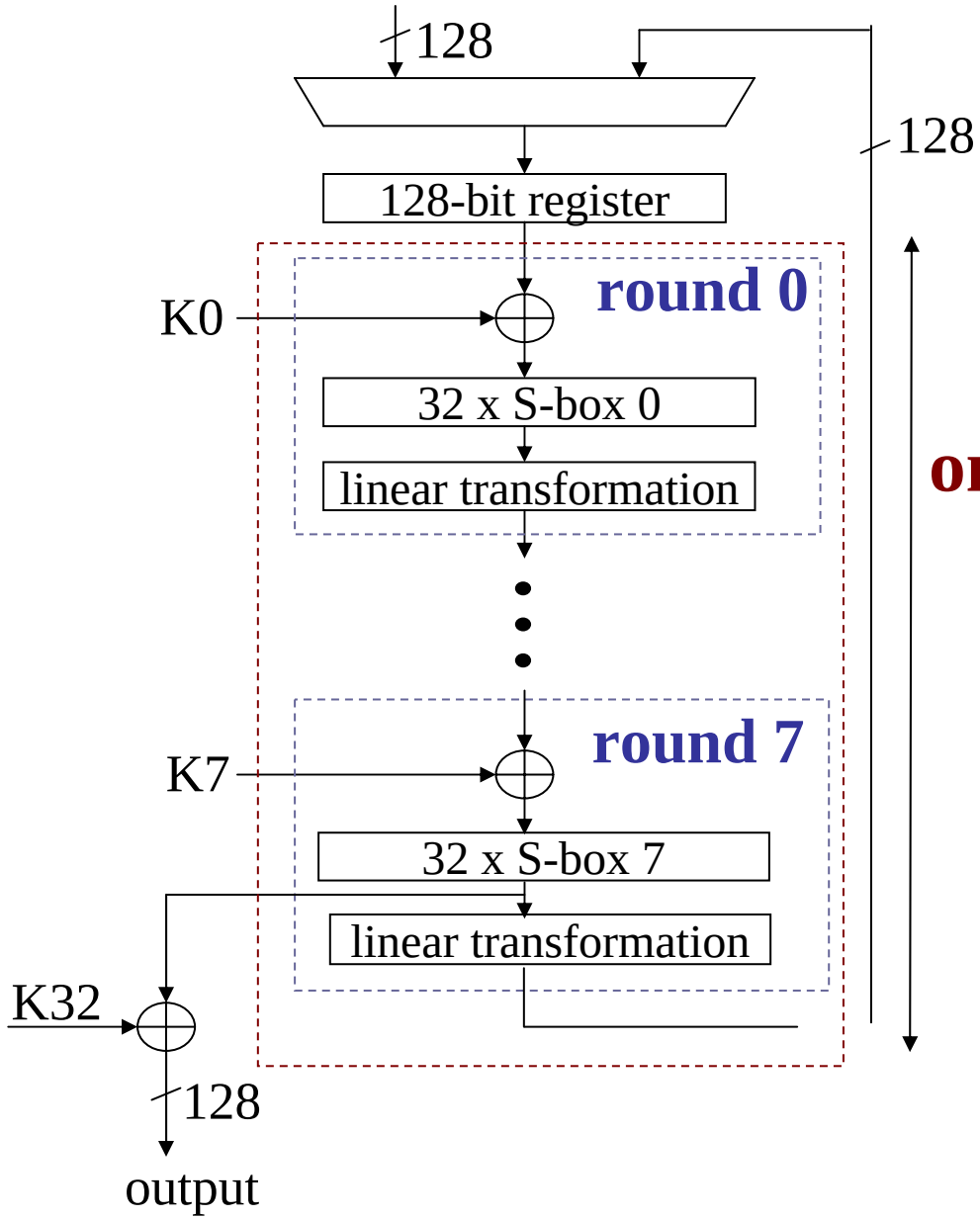


Comparison with results of other groups: Area

Area [CLB slices]



Basic architecture of Serpent (encryption)

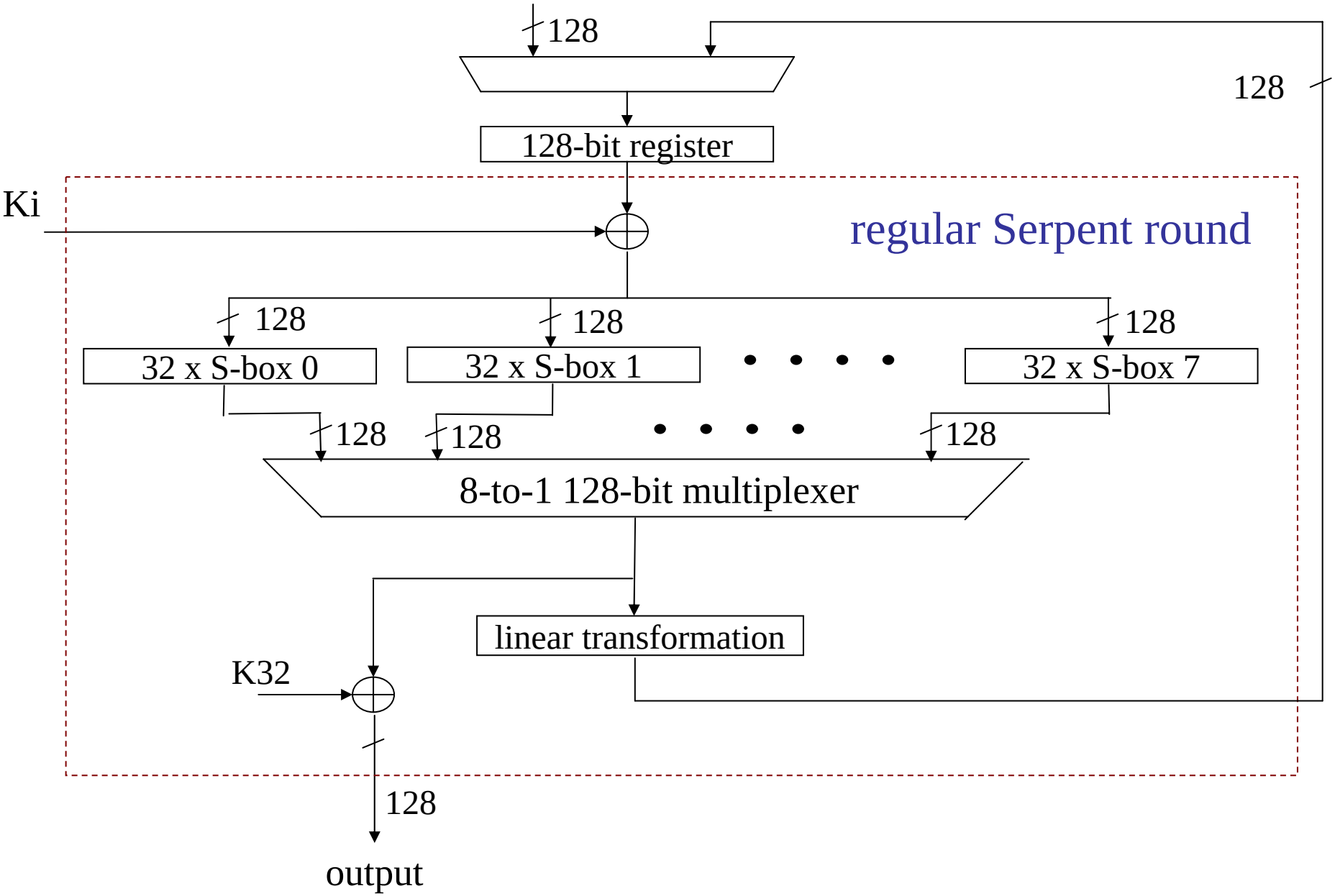


one implementation round of Serpent

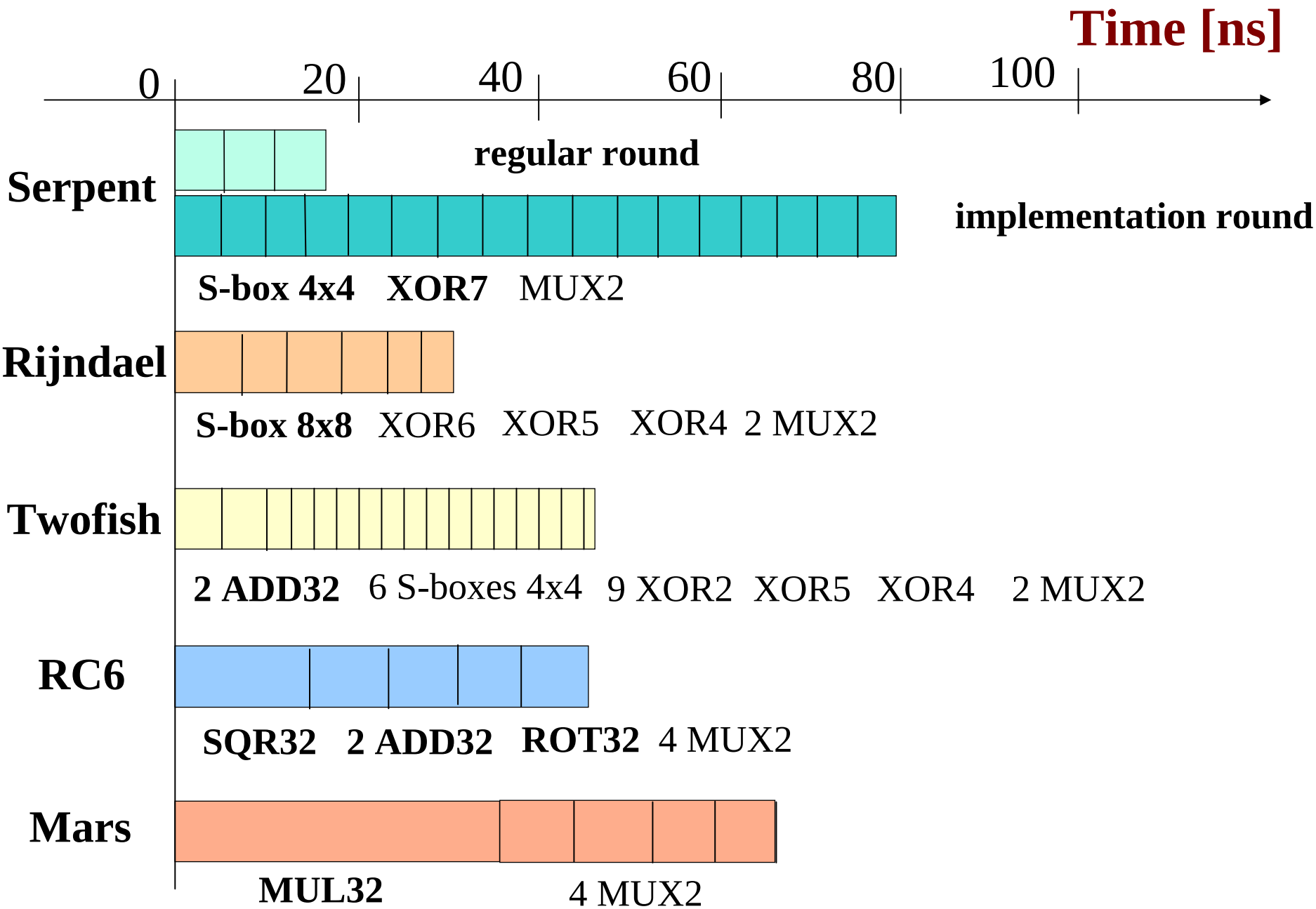
=

8 regular cipher rounds

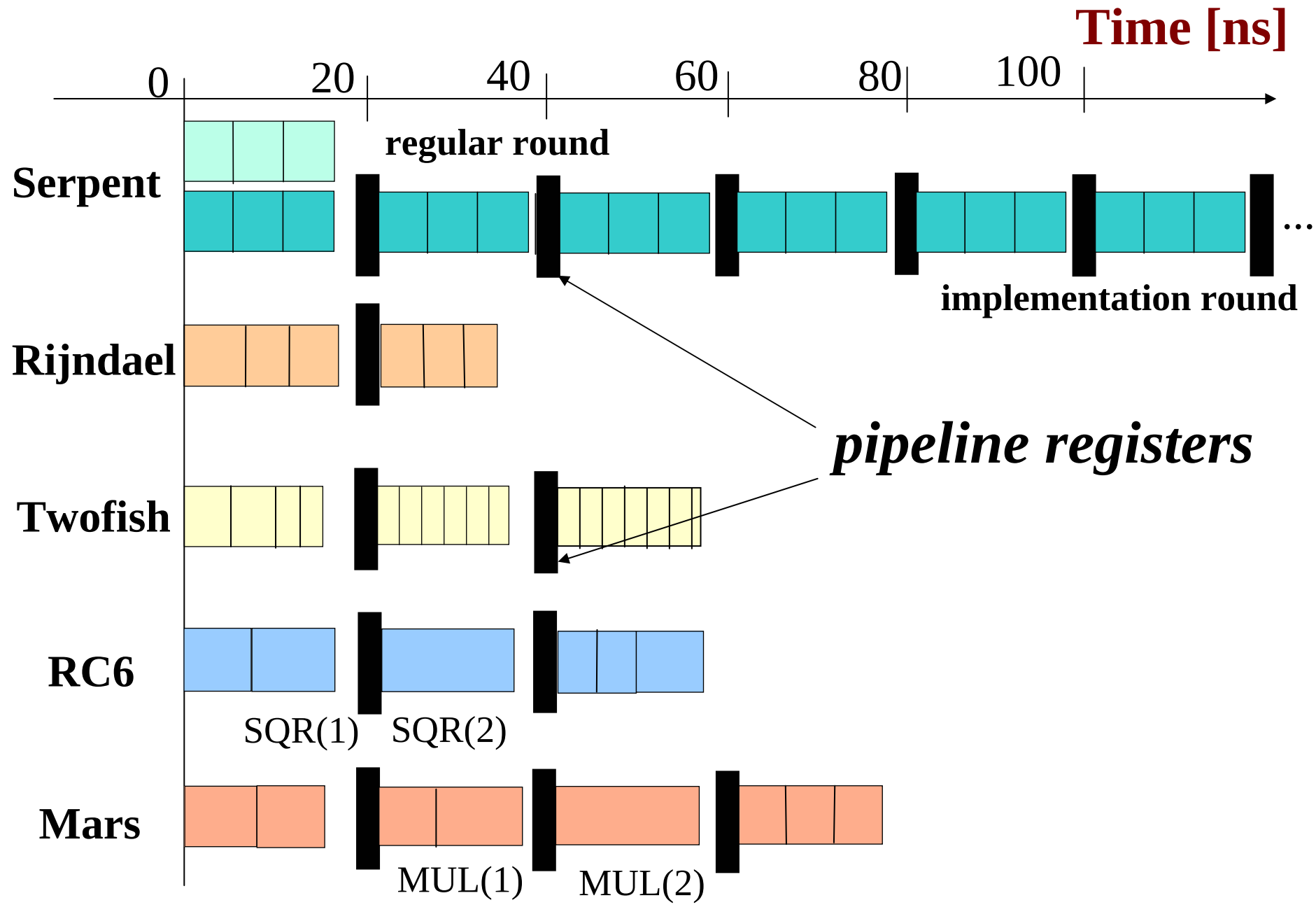
Serpent architecture with resource sharing



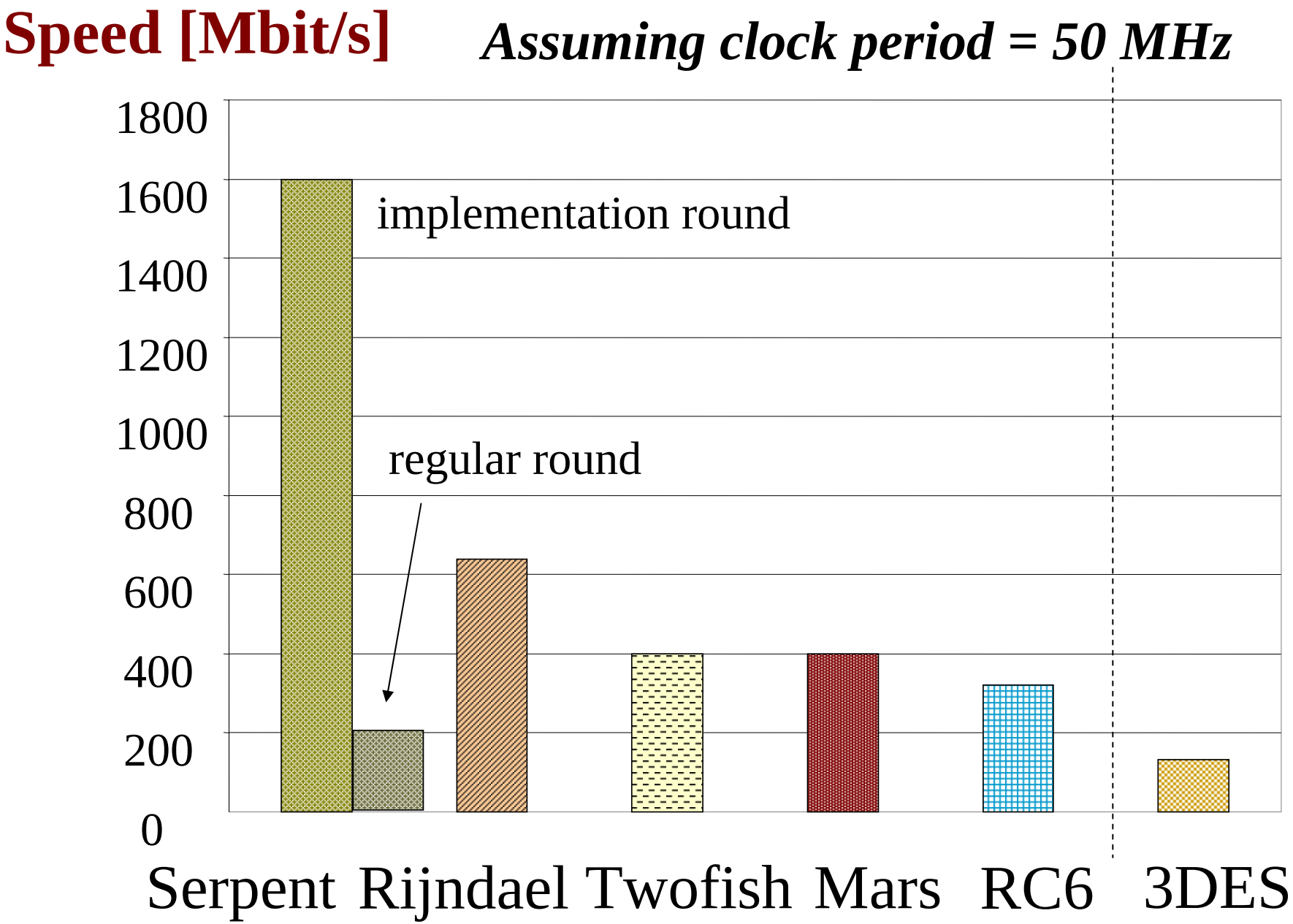
Critical path: Time



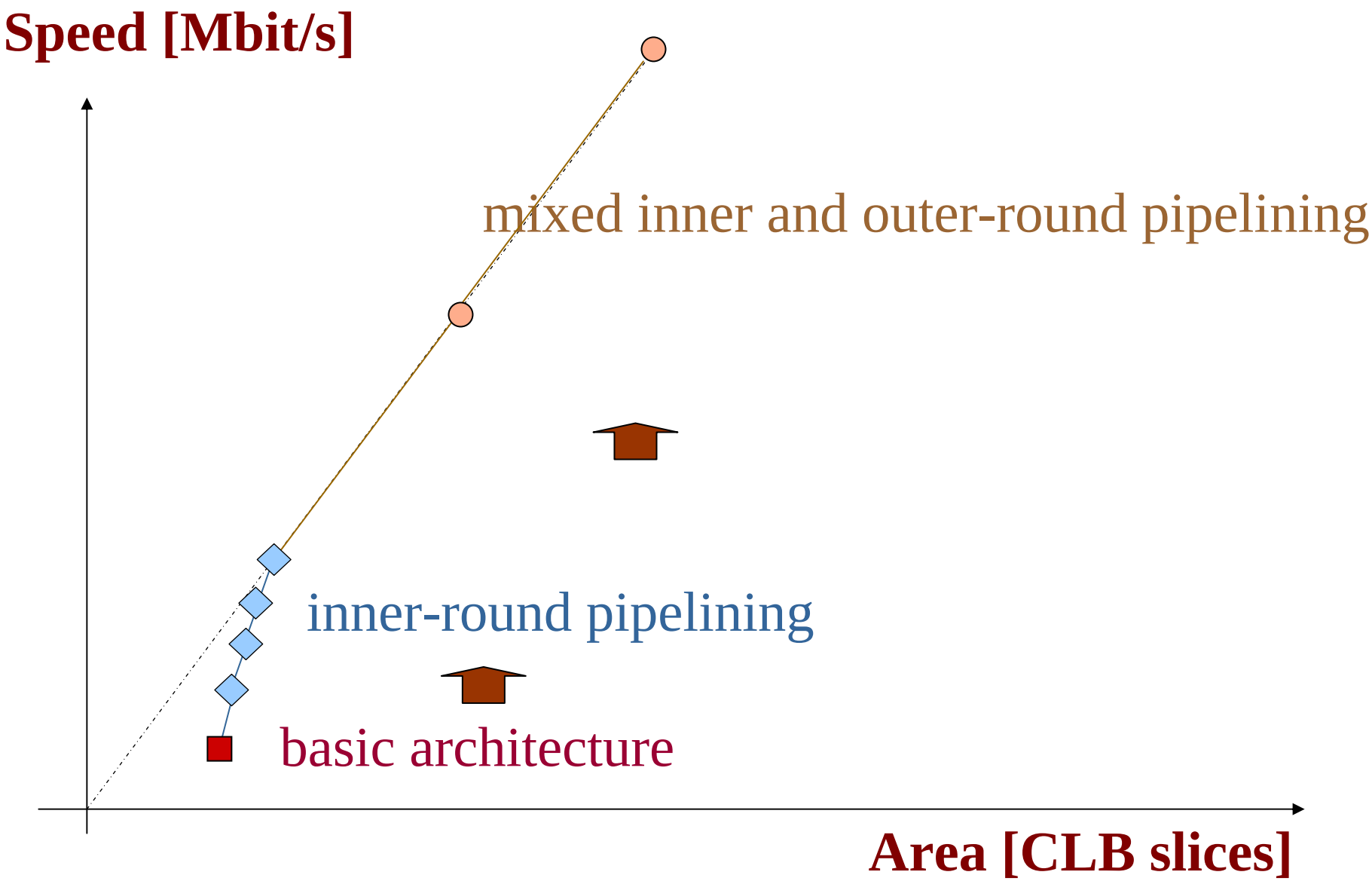
Inner-Round Pipelining



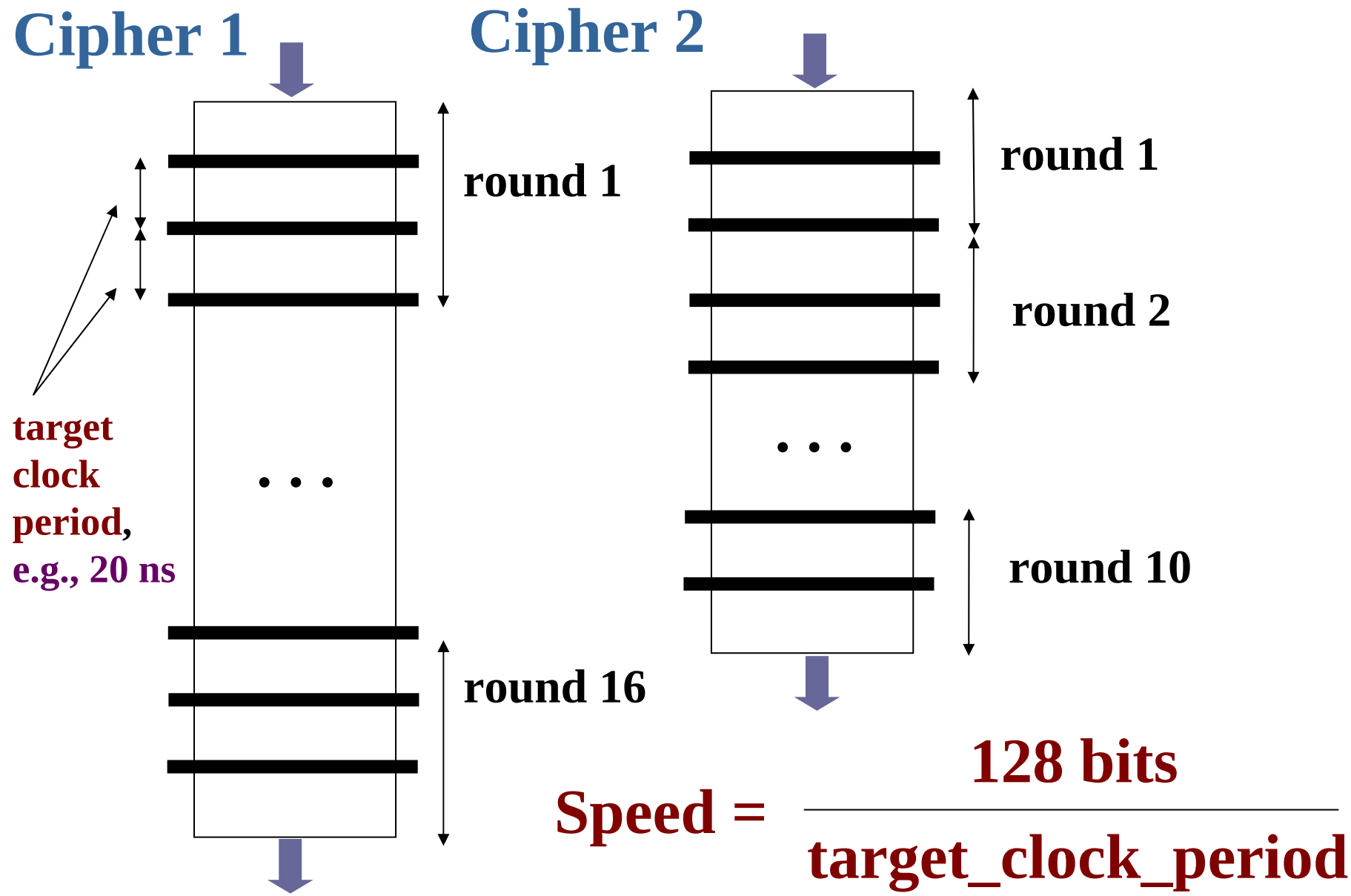
Inner-round pipelining: Speed



Choosing optimum architecture for non-feedback cipher modes

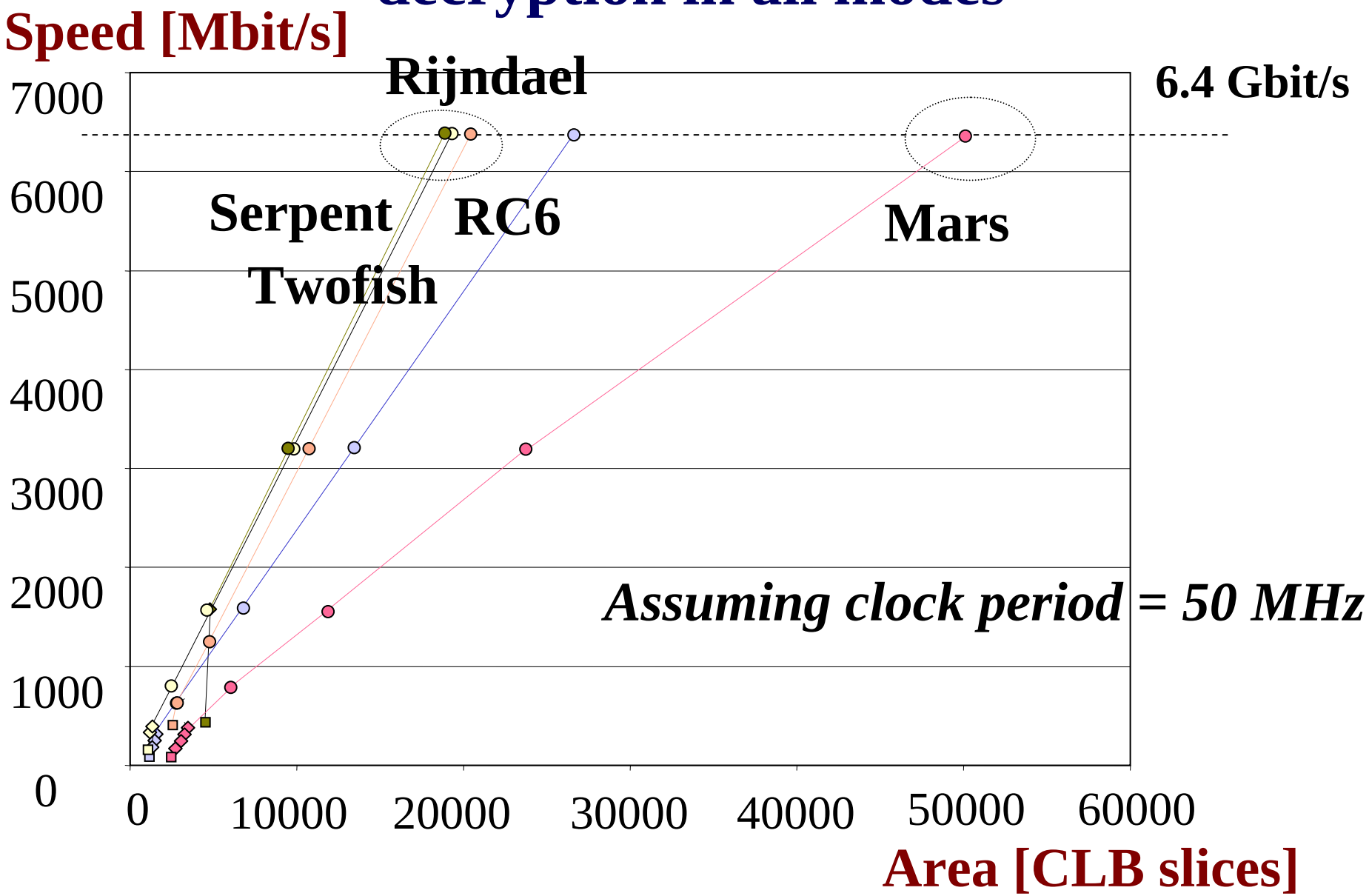


Full Mixed Inner and Outer-Round Pipelining

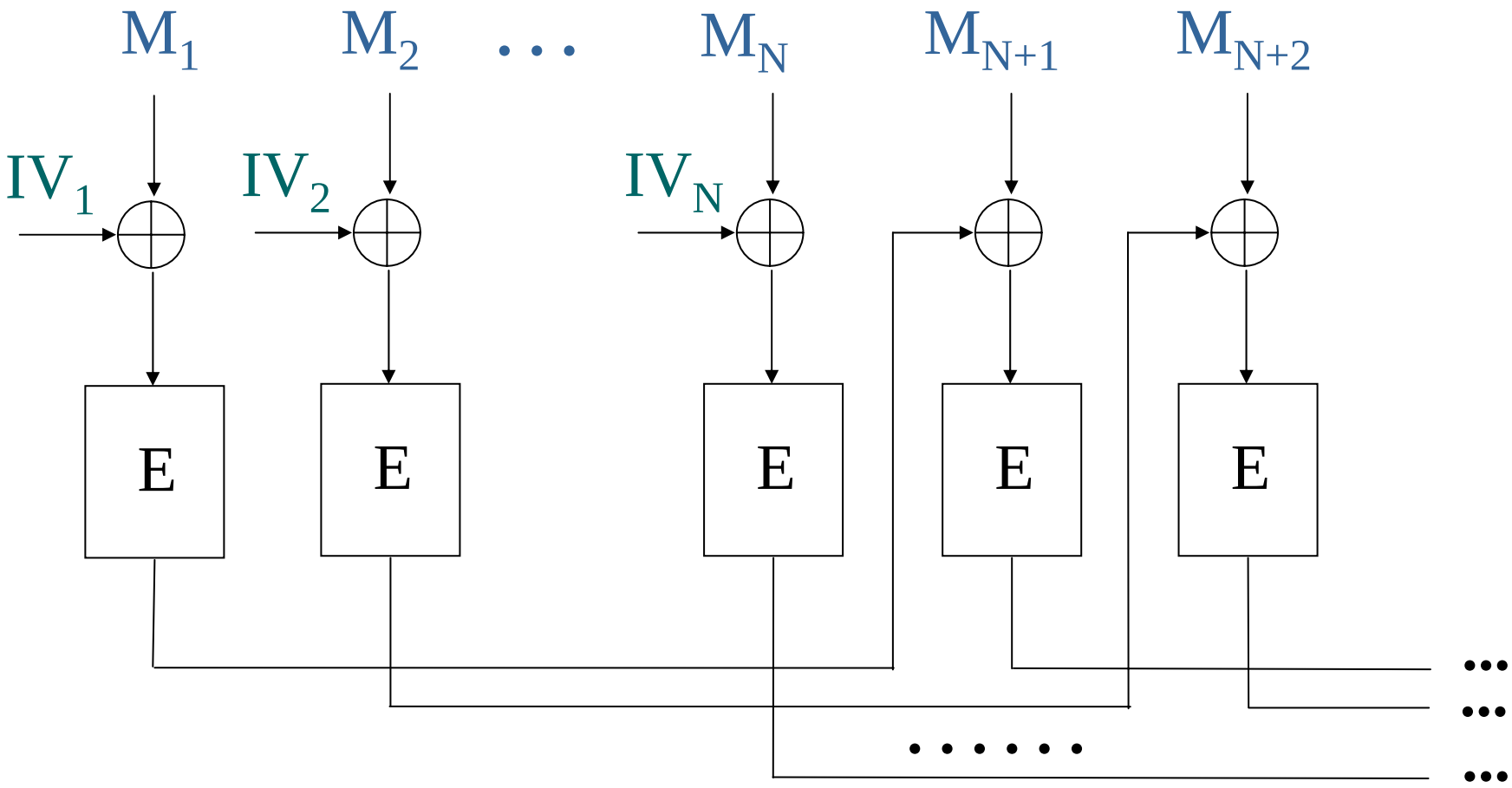


$$\text{Speed} = \frac{128 \text{ bits}}{\text{target\_clock\_period}}$$

Encryption in non-feedback modes (ECB, counter)
decryption in all modes



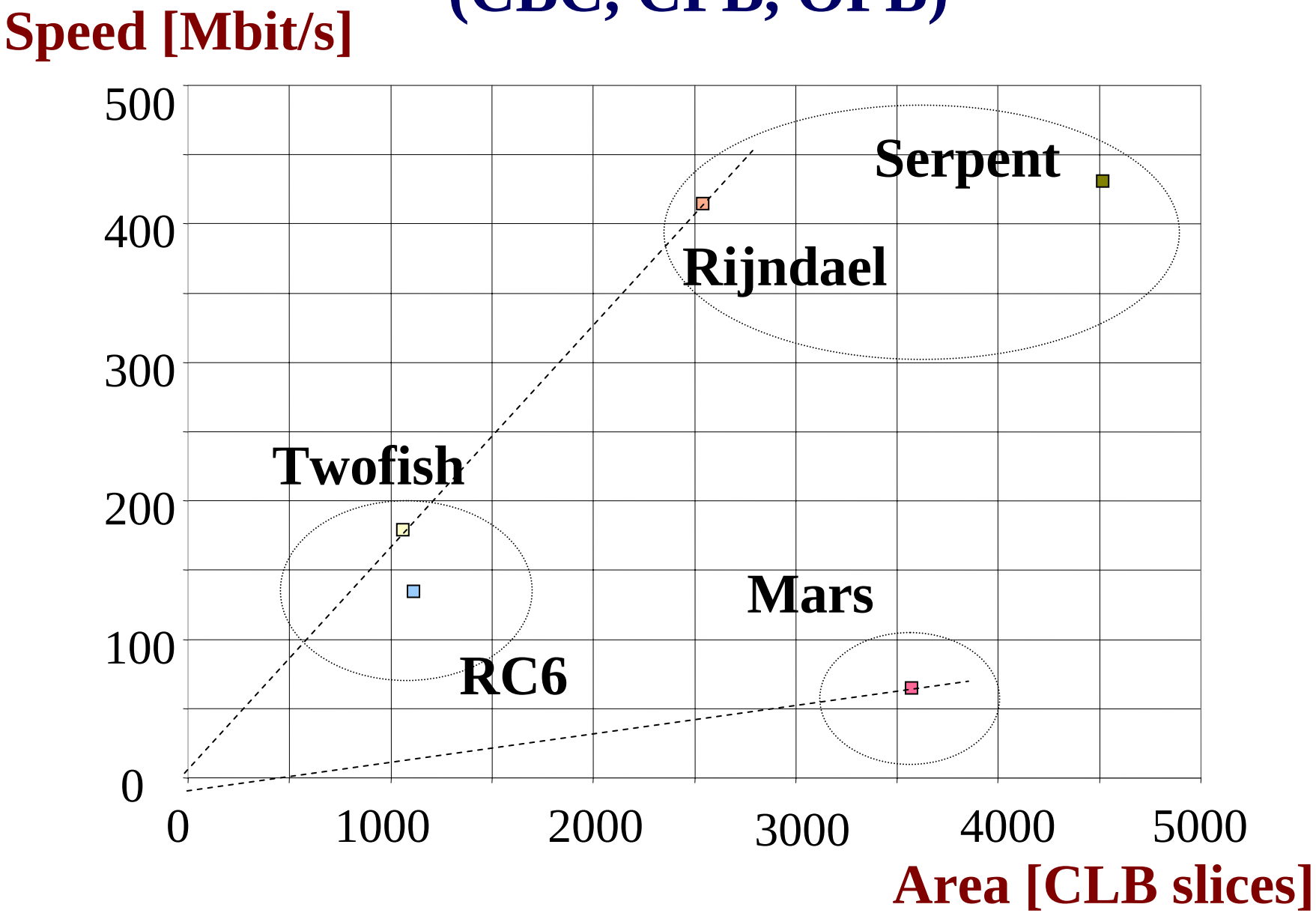
Need for interleaved operating modes



$C_i = \mathrm{AES}(M_i \oplus IV_i)$ for i=1 to N,

$C_i = \mathrm{AES}(M_i \oplus C_{i\text{-}N})$ for i>N

Encryption in cipher feedback modes (CBC, CFB, OFB)



Conclusions (1)

For feedback cipher modes (CBC, CFB, OFB):

- **Speed should be the primary criteria of comparison**
- **Basic (iterative) architecture is the most appropriate for comparison and future implementations**
- **Serpent and Rijndael are over twice as fast as the next best candidate**
- **Results confirmed by three independent groups**

Conclusions (2)

For non-feedback cipher modes (ECB, counter):

- All ciphers can achieve the same speed
  Area should be the primary criteria of comparison.
- Architecture with inner round pipelining combined with full outer round pipelining is the most appropriate for comparison and future implementations
- Serpent, Twofish and Rijndael are the most cost-efficient and take approximately the same amount of area
- No agreement regarding the methodology and architecture used for comparison

More results needed!