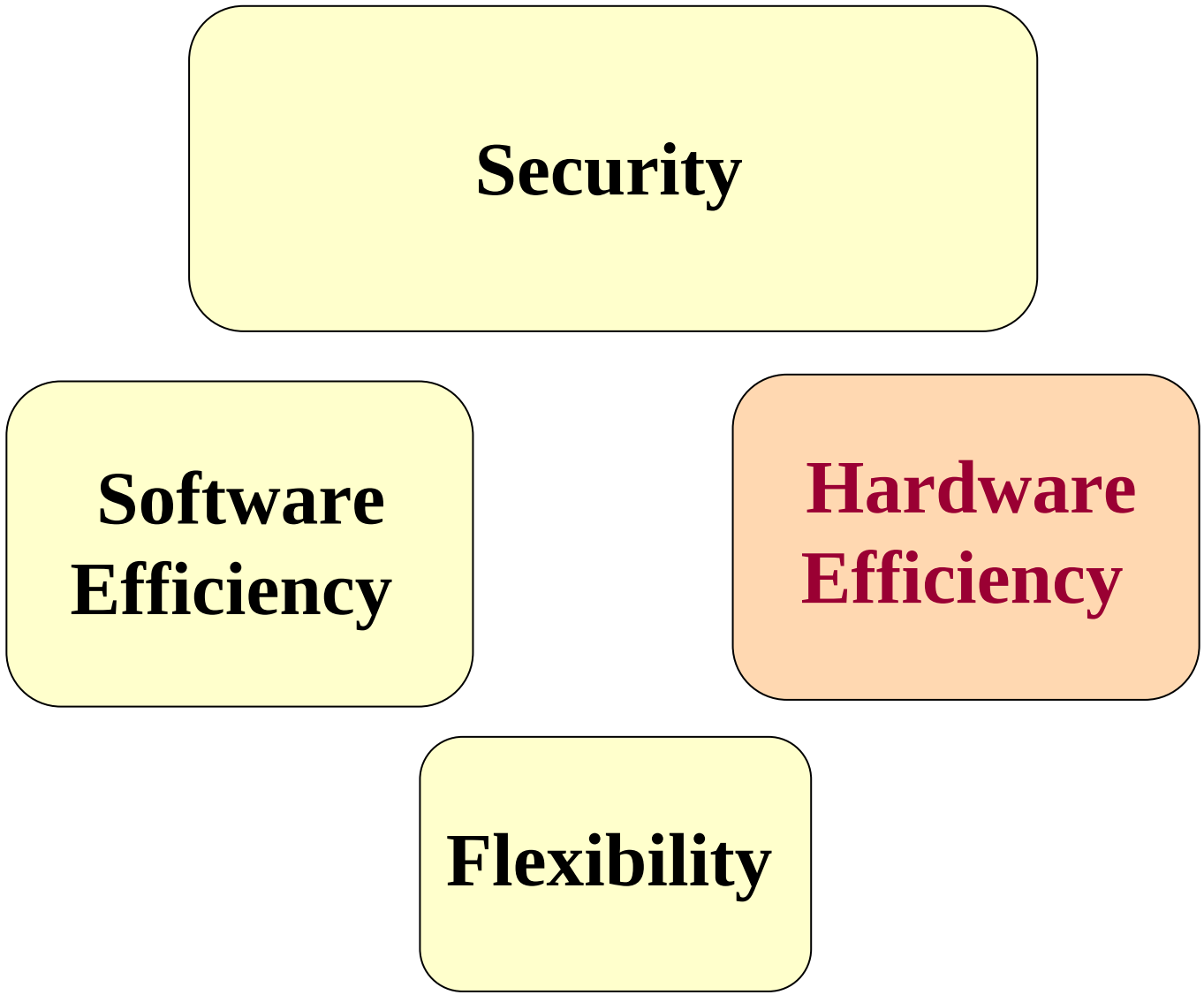
Kris Gaj and Pawel Chodowiec
Electrical and Computer Engineering
George Mason University

Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using Field Programmable Gate Arrays

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

AES Contest - NIST Evaluation Criteria



AES Contest Effort

June 1998

15 Candidates

from USA, Canada, Belgium,
France, Germany, Norway, UK, Isreal,
Korea, Japan, Australia, Costa Rica

Round 1

Security
Software efficiency

August 1999

5 final candidates

Mars, RC6, Rijndael, Serpent, Twofish

Round 2

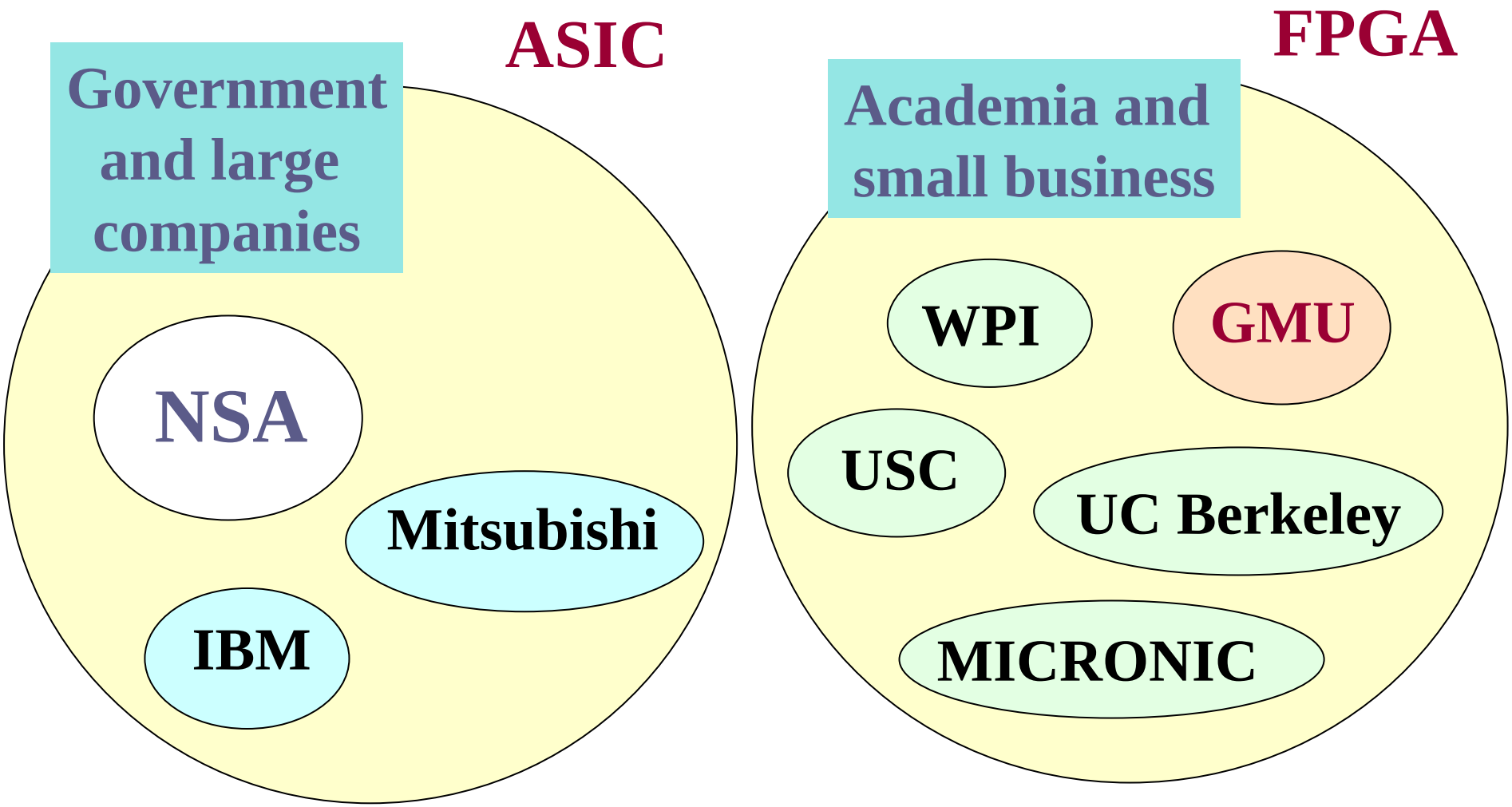
Security
Hardware efficiency

October 2000

1 winner: Rijndael

Belgium

Hardware Efficiency Comparisons



Primary ways of implementing cryptography in hardware

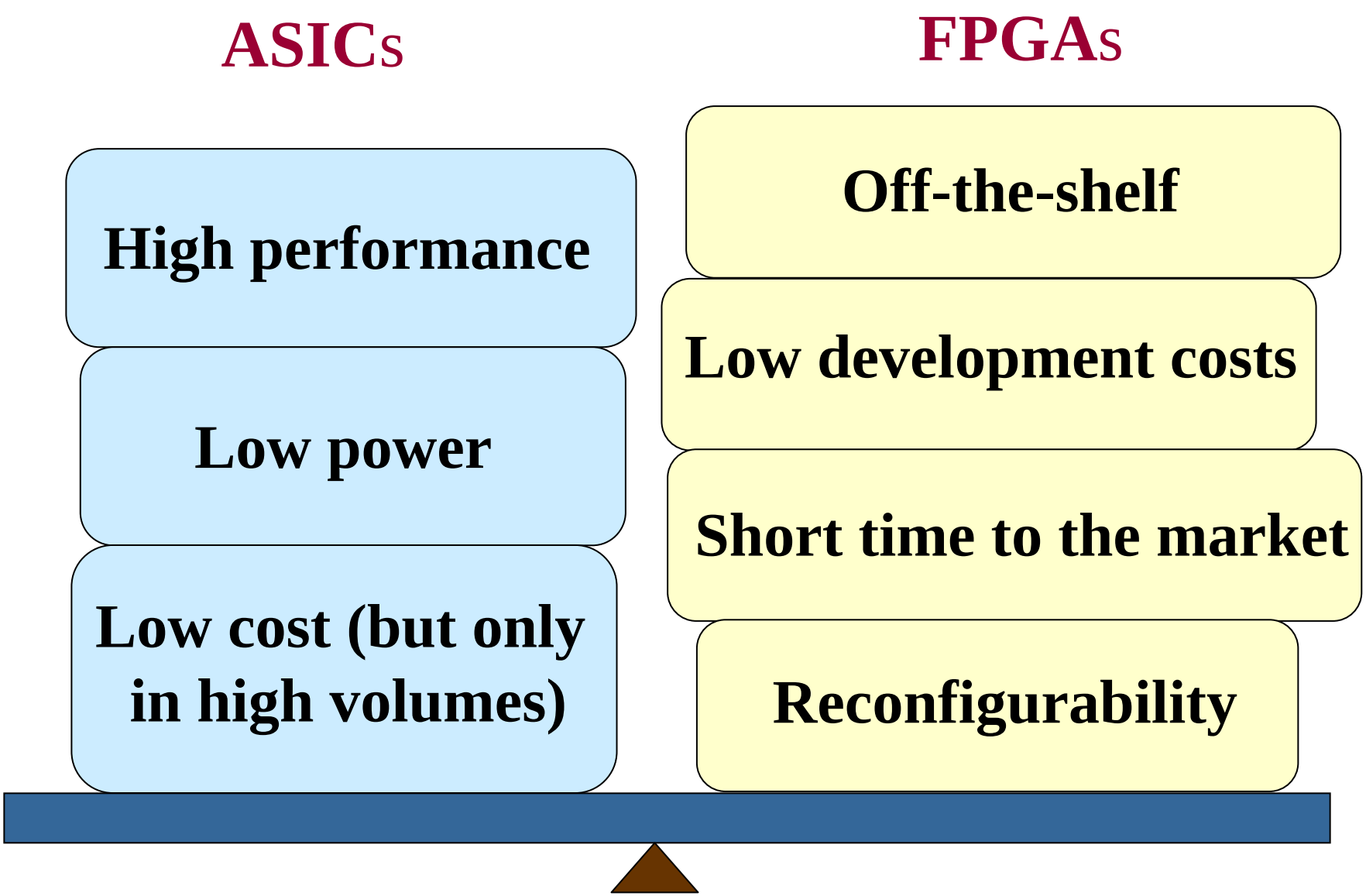
ASIC
Application **S**pecific
Integrated **C**ircuit

- designs must be sent for expensive and time consuming fabrication in semiconductor foundry
- designed all the way from behavioral description to physical layout

FPGA
Field **P**rogrammable
Gate **A**rray

- bought off the shelf and reconfigured by designers themselves
- no physical layout design; design ends with a bitstream used to configure a device

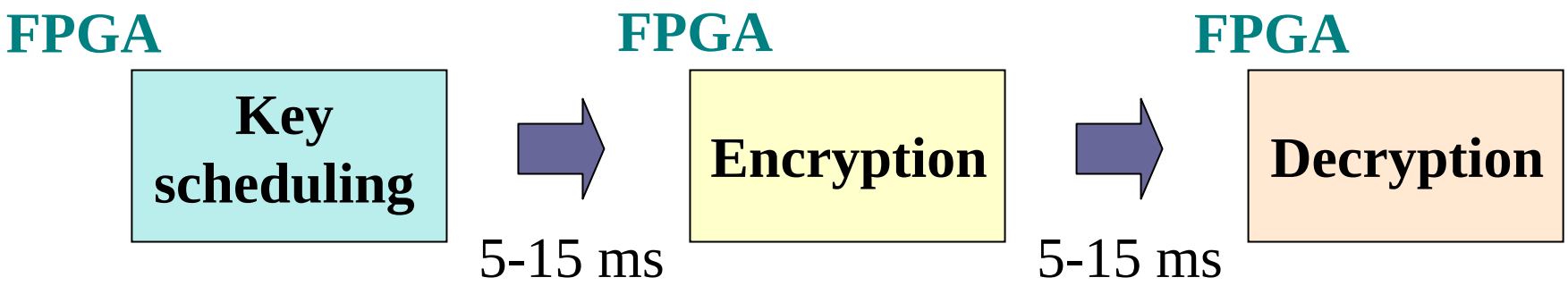
Which way to go?



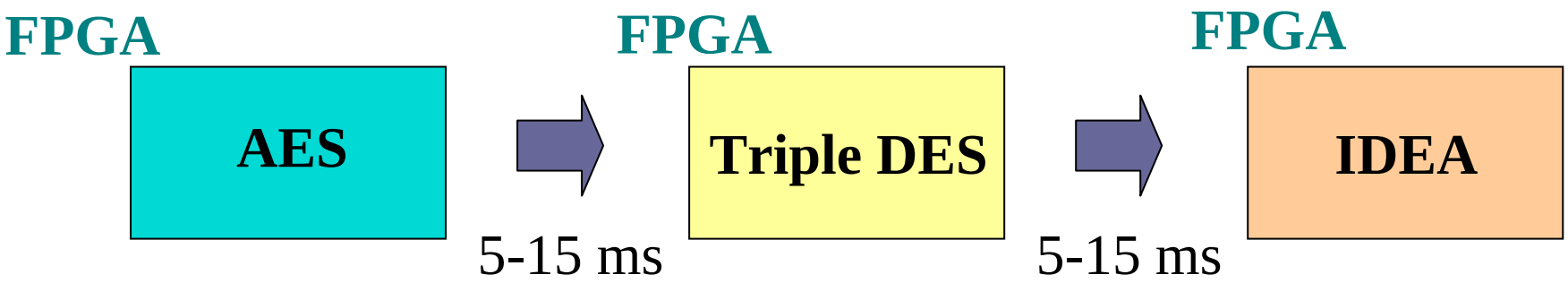
Reconfigurability

External ROM and microprocessor enables changing an FPGA function in several milliseconds

Encryption vs. decryption vs. key scheduling

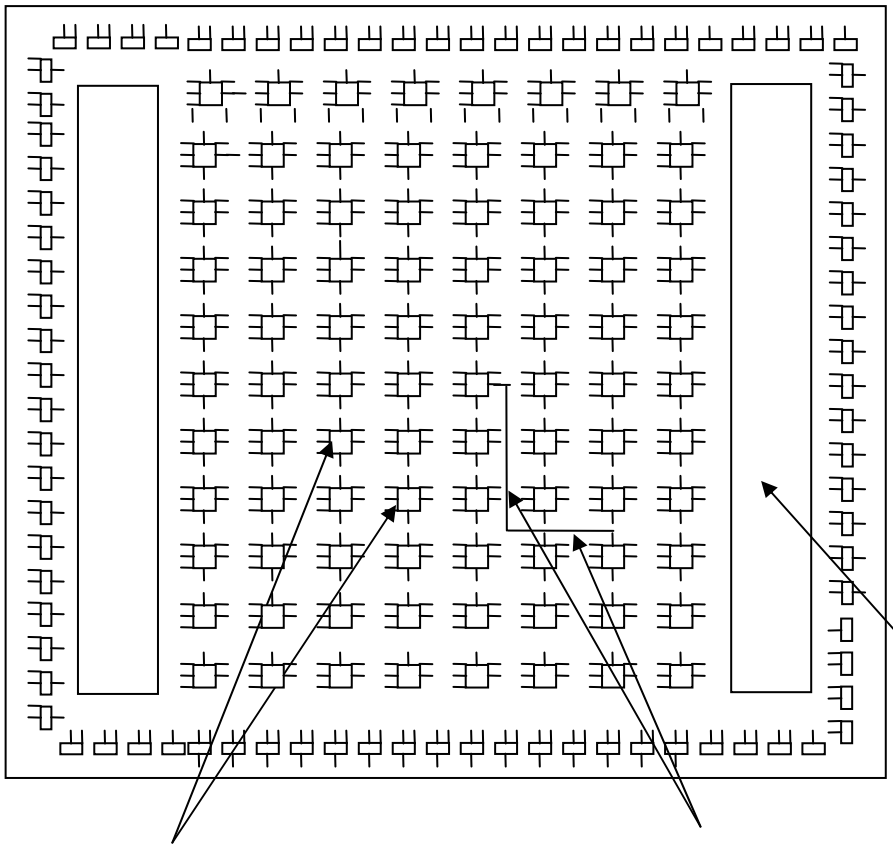


Various algorithms



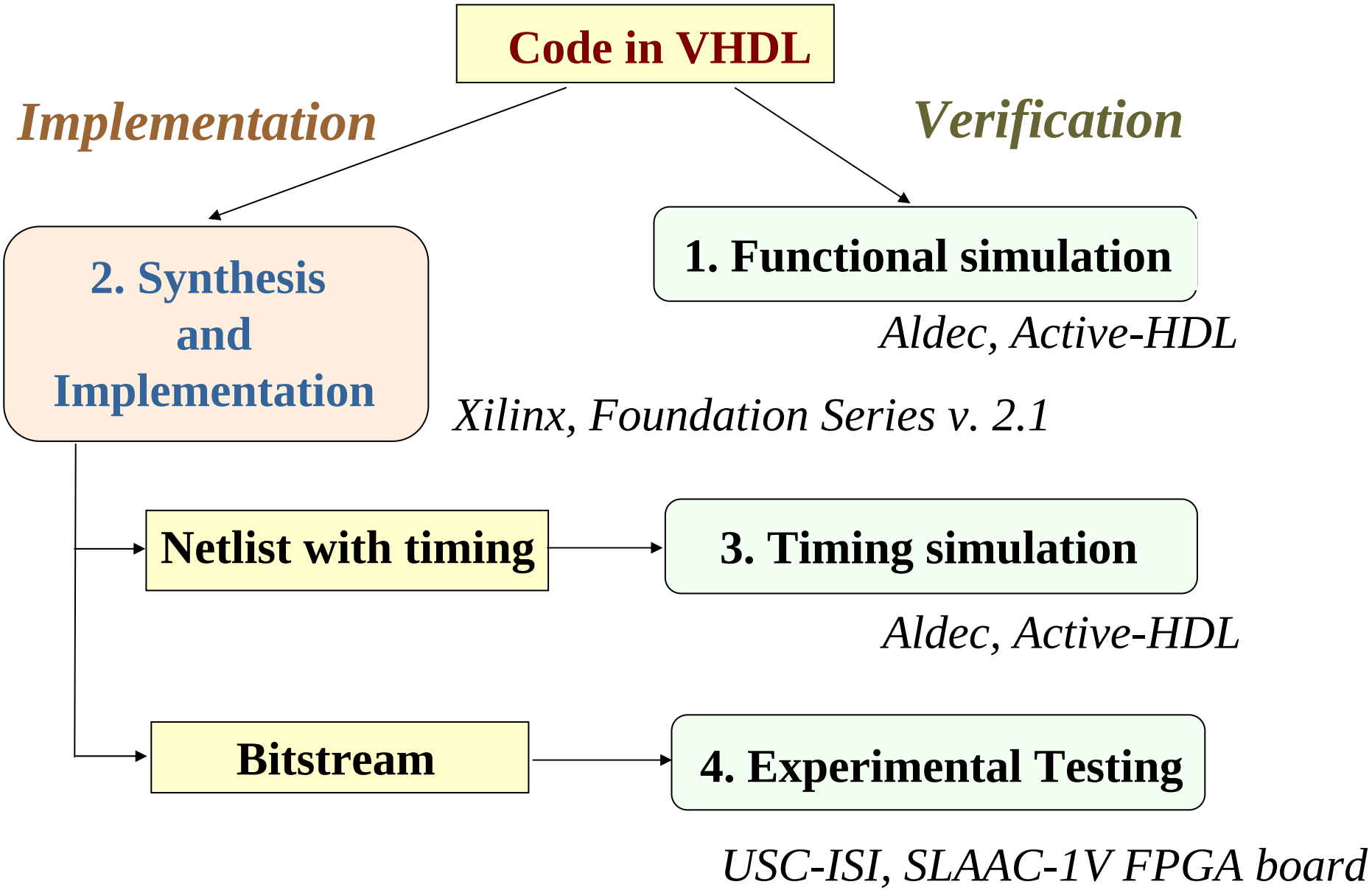
Target FPGA devices

Xilinx Virtex - XCV 1000



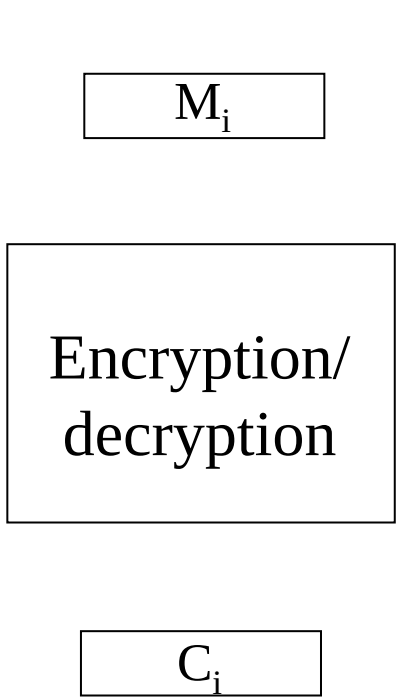
- 0.22 μm CMOS process
- 12 288 CLB slices
- 10 4-kbit block RAMs
- 1 mln equivalent logic gates
- Up to 200 MHz clock

Methodology and Tools



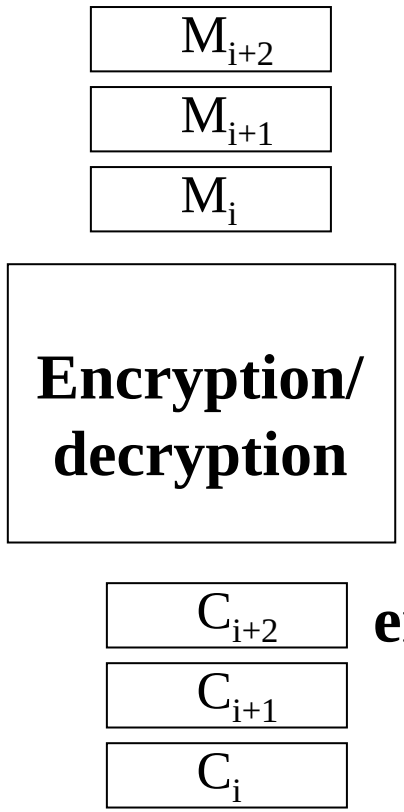
Primary parameters of hardware implementations for secret-key block ciphers

Latency



Time to encrypt/decrypt a single block of data

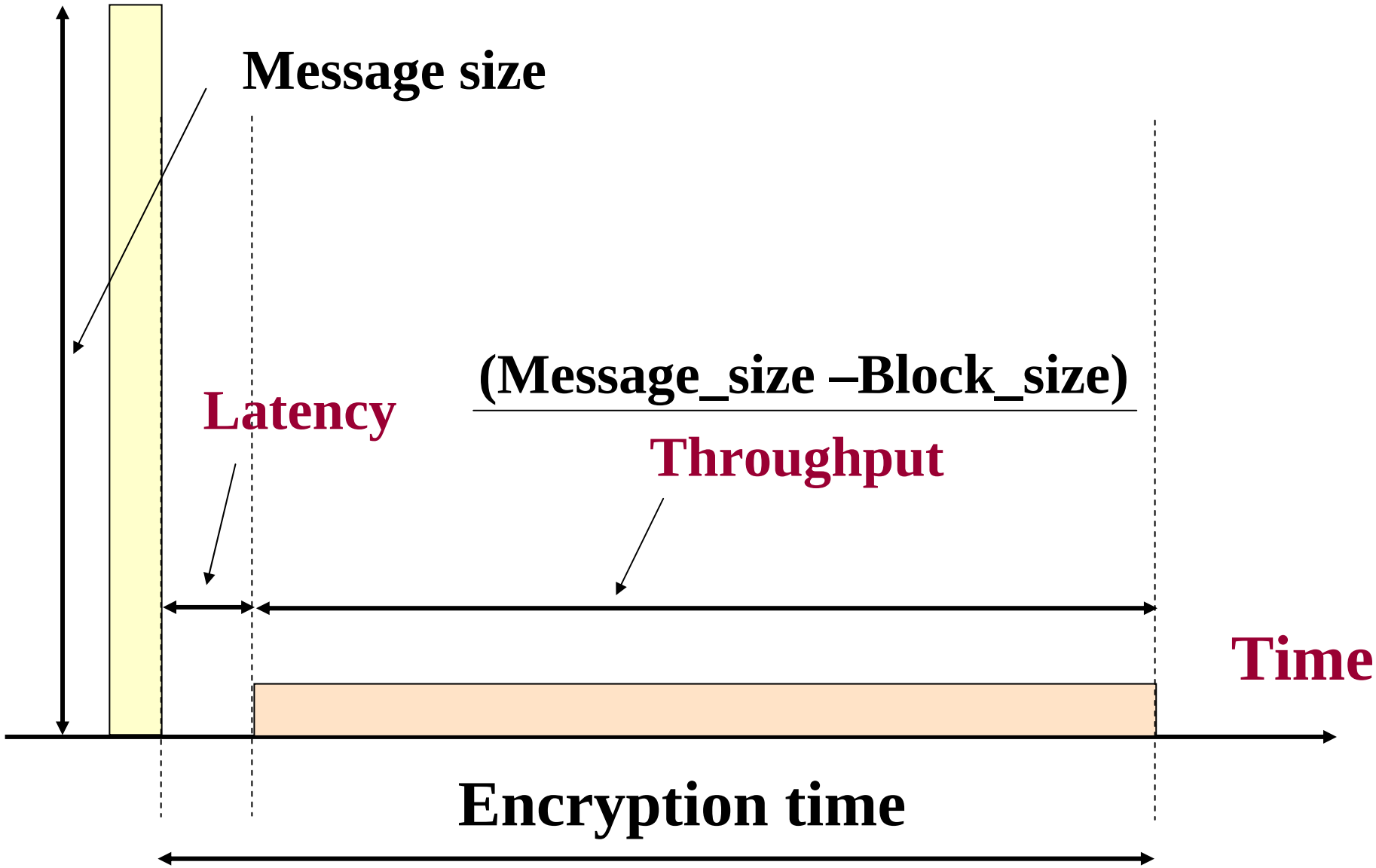
Throughput



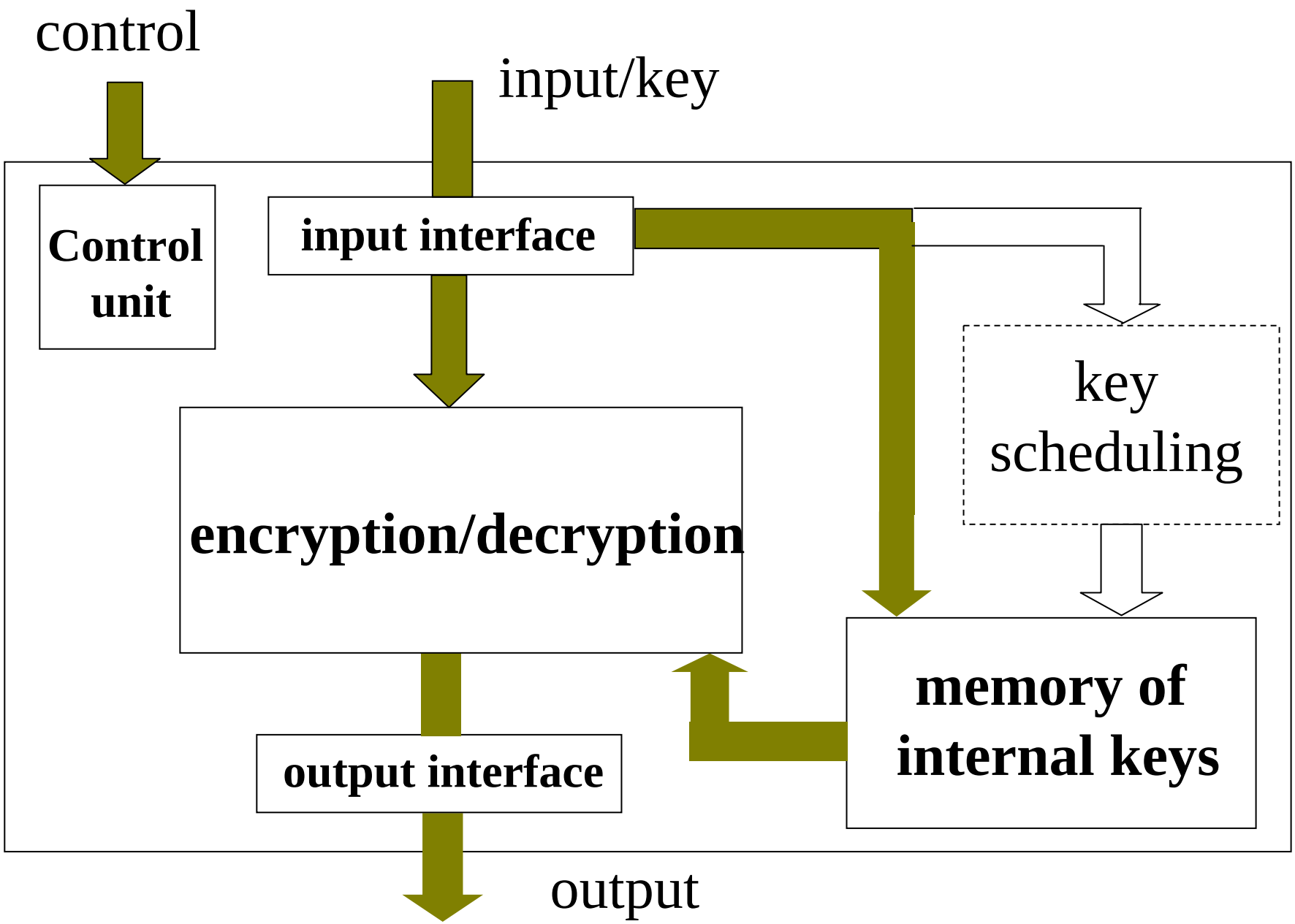
Number of bits encrypted/decrypted in a unit of time

$$\text{Throughput} = \frac{\text{Block\_size} \cdot \text{Number\_of\_blocks\_processed\_simultaneously}}{\text{Latency}}$$

Dependence of the encryption time on latency and throughput



Top level block diagram



Primary factor in choosing the encryption/decryption unit architecture

Symmetric-key cipher mode of operation:

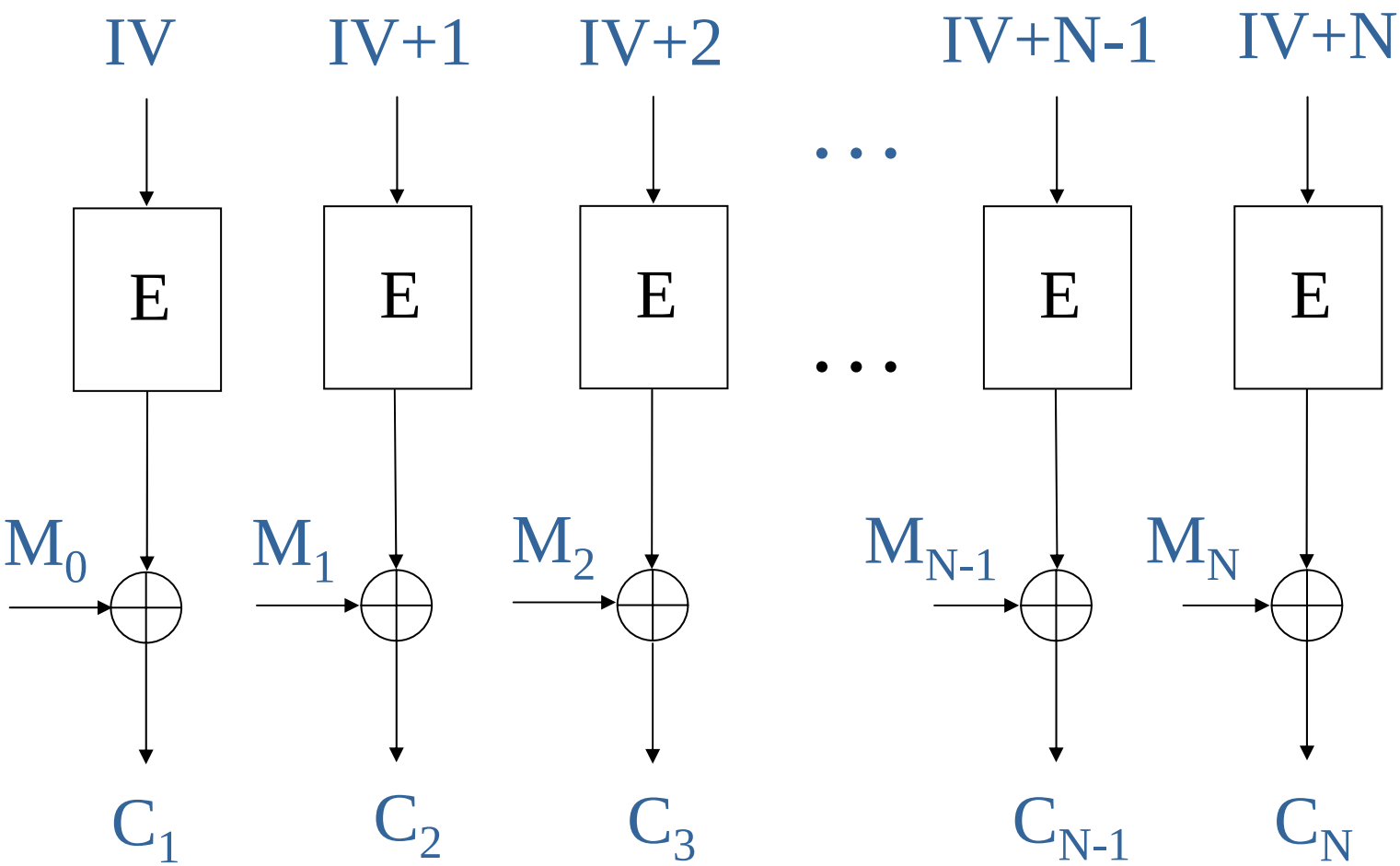
1. Non-feedback cipher modes

ECB, counter mode

2. Feedback cipher modes

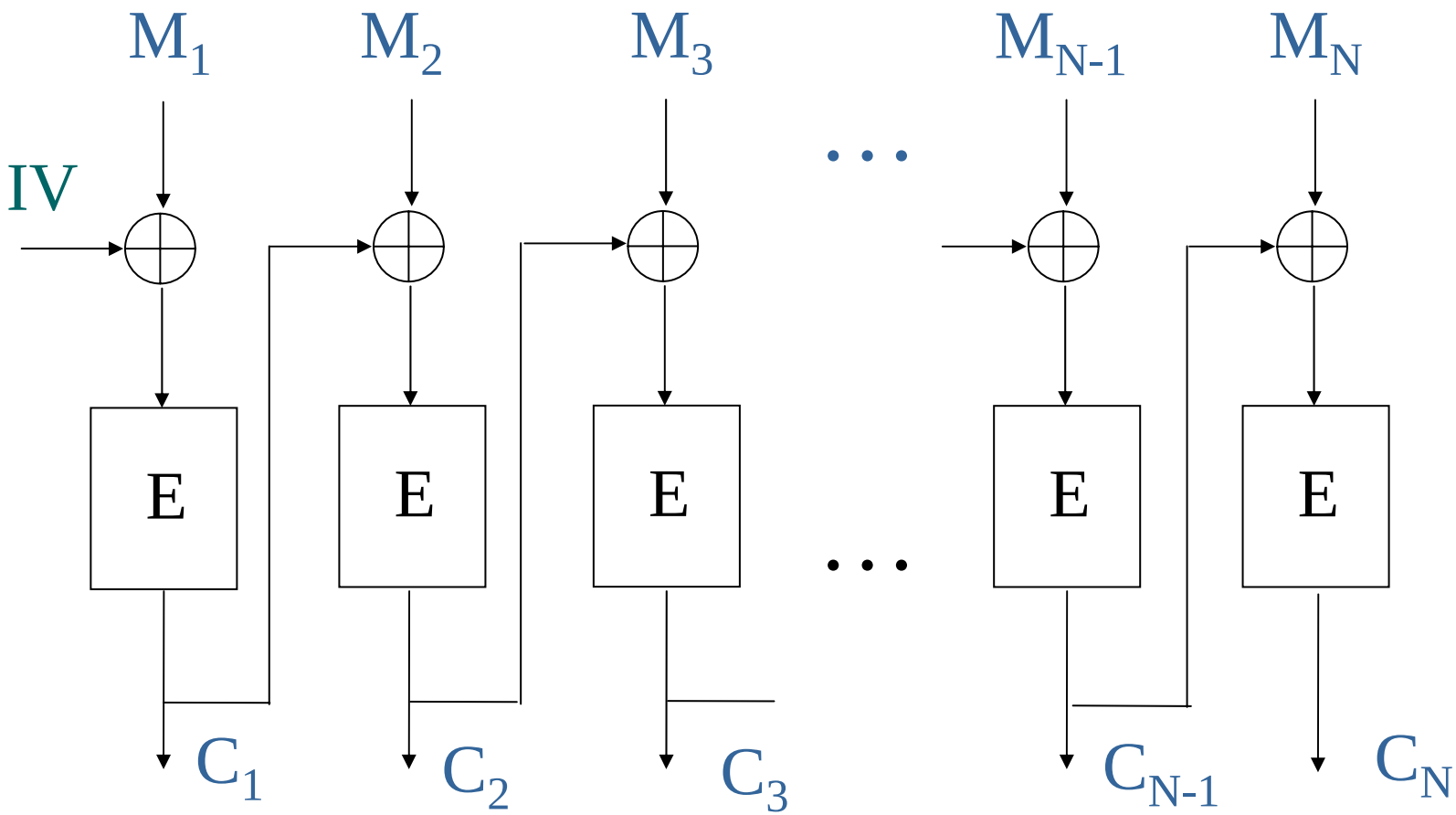
CBC, CFB, OFB

Non-feedback Counter Mode - CTR



$C_i = M_i \oplus AES(IV+i)$ for i=0..N

Feedback cipher modes - CBC

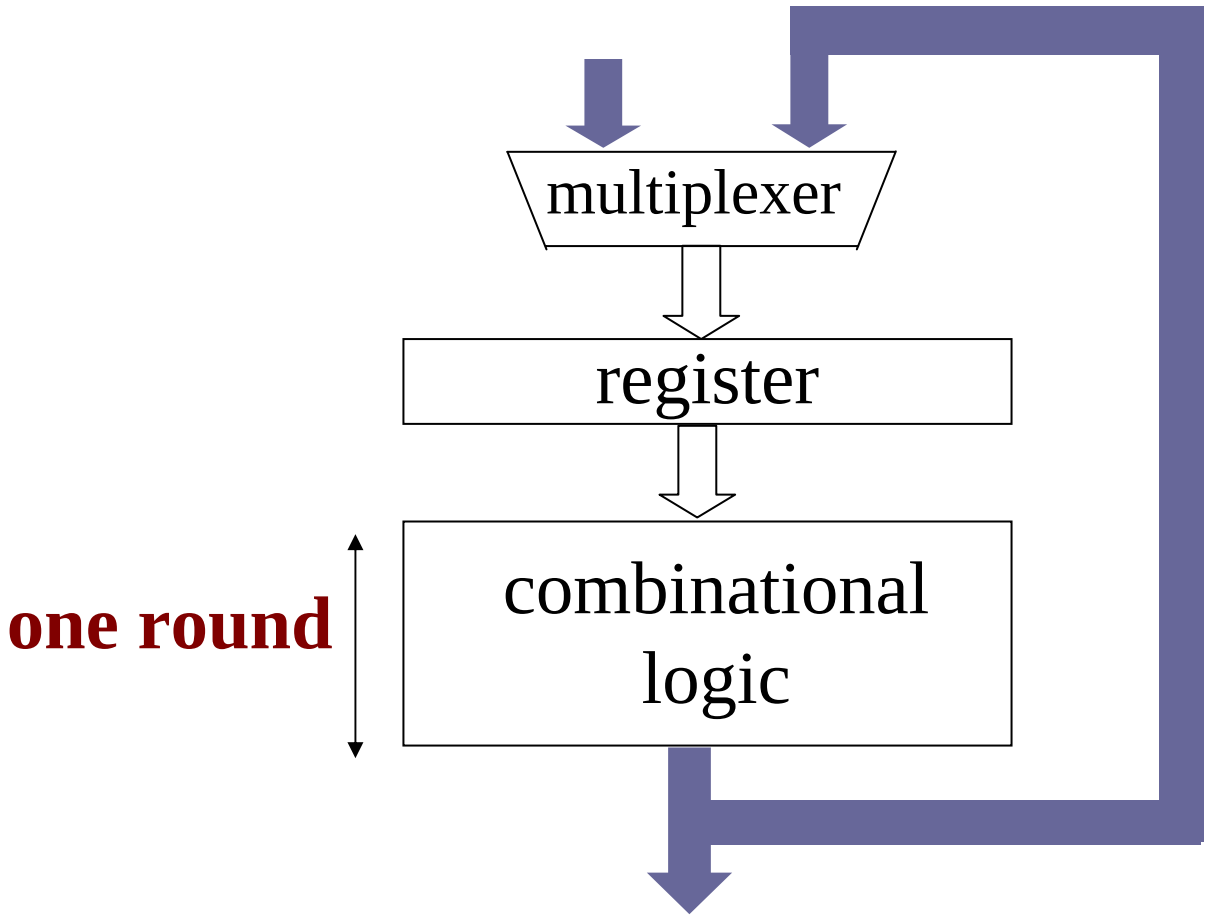


$C_1 = \text{AES}(M_i \oplus IV)$

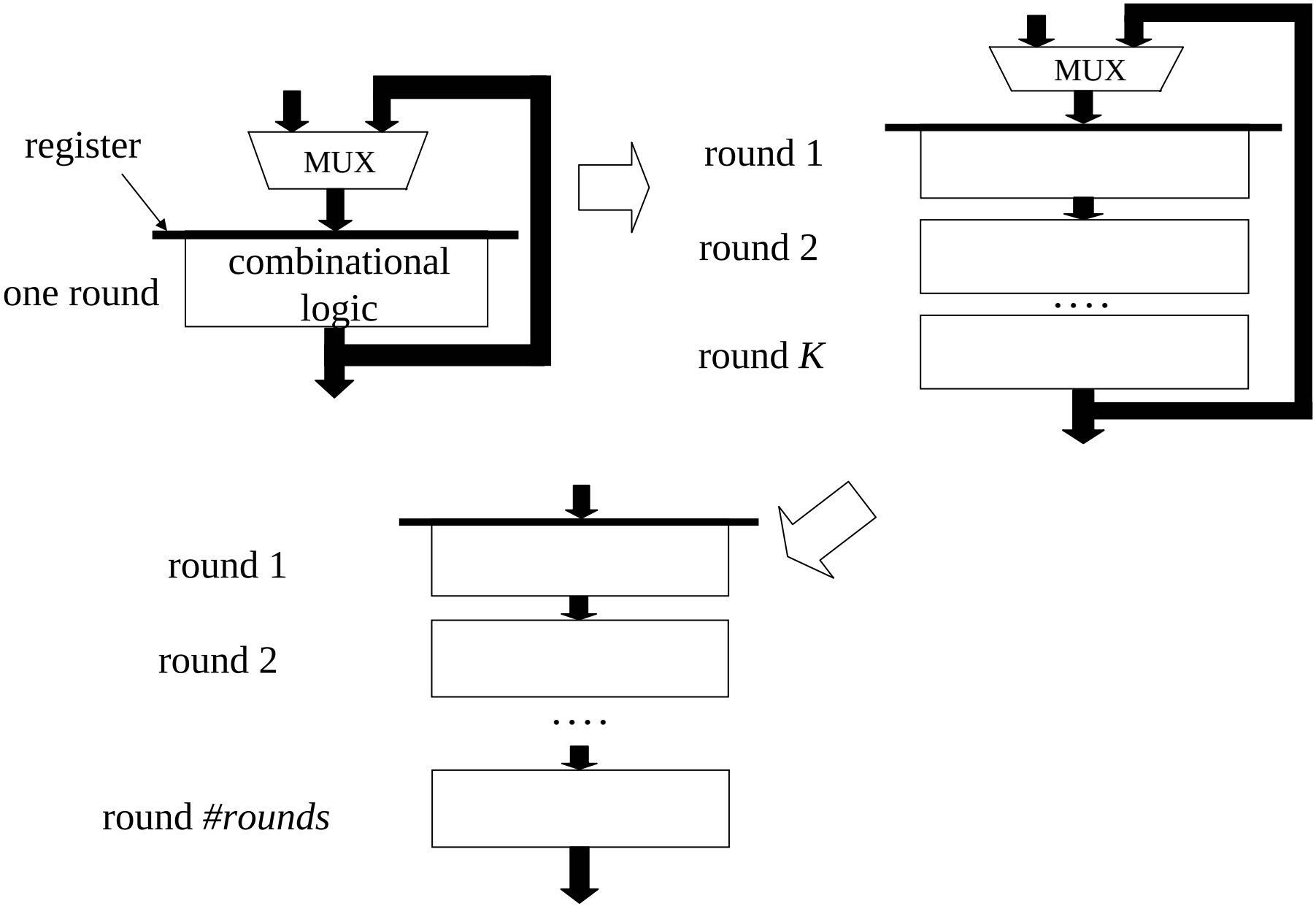
$C_i = \text{AES}(M_i \oplus C_{i-1})$ for i=2..N

Feedback cipher modes
CBC, CFB, OFB

Basic iterative architecture



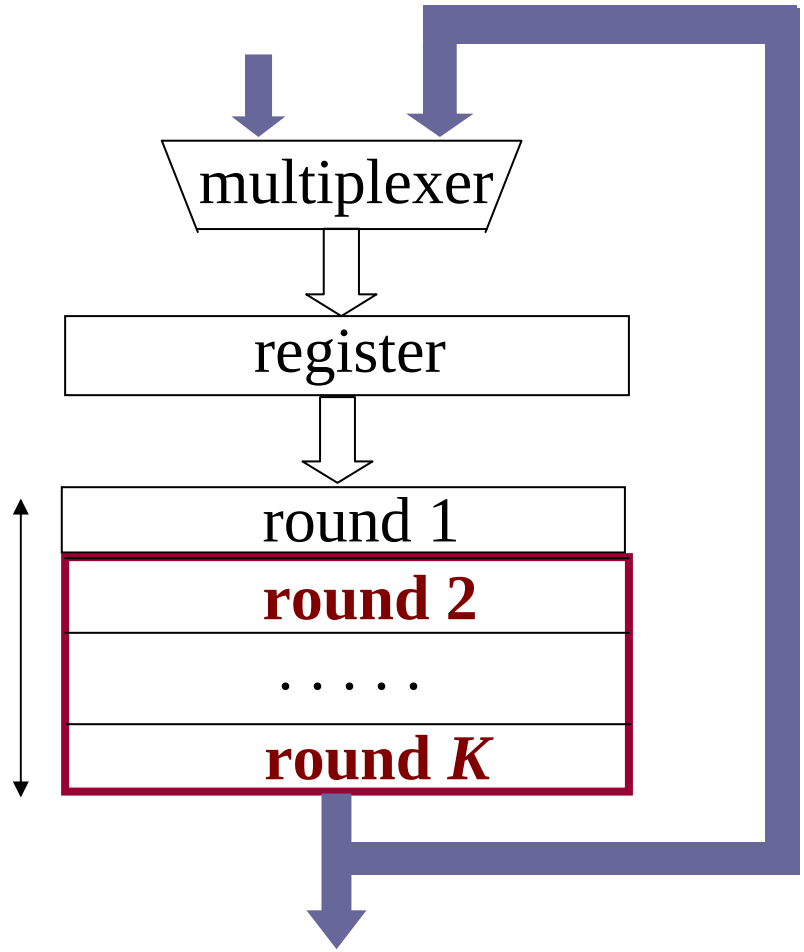
Architectures suitable for feedback modes



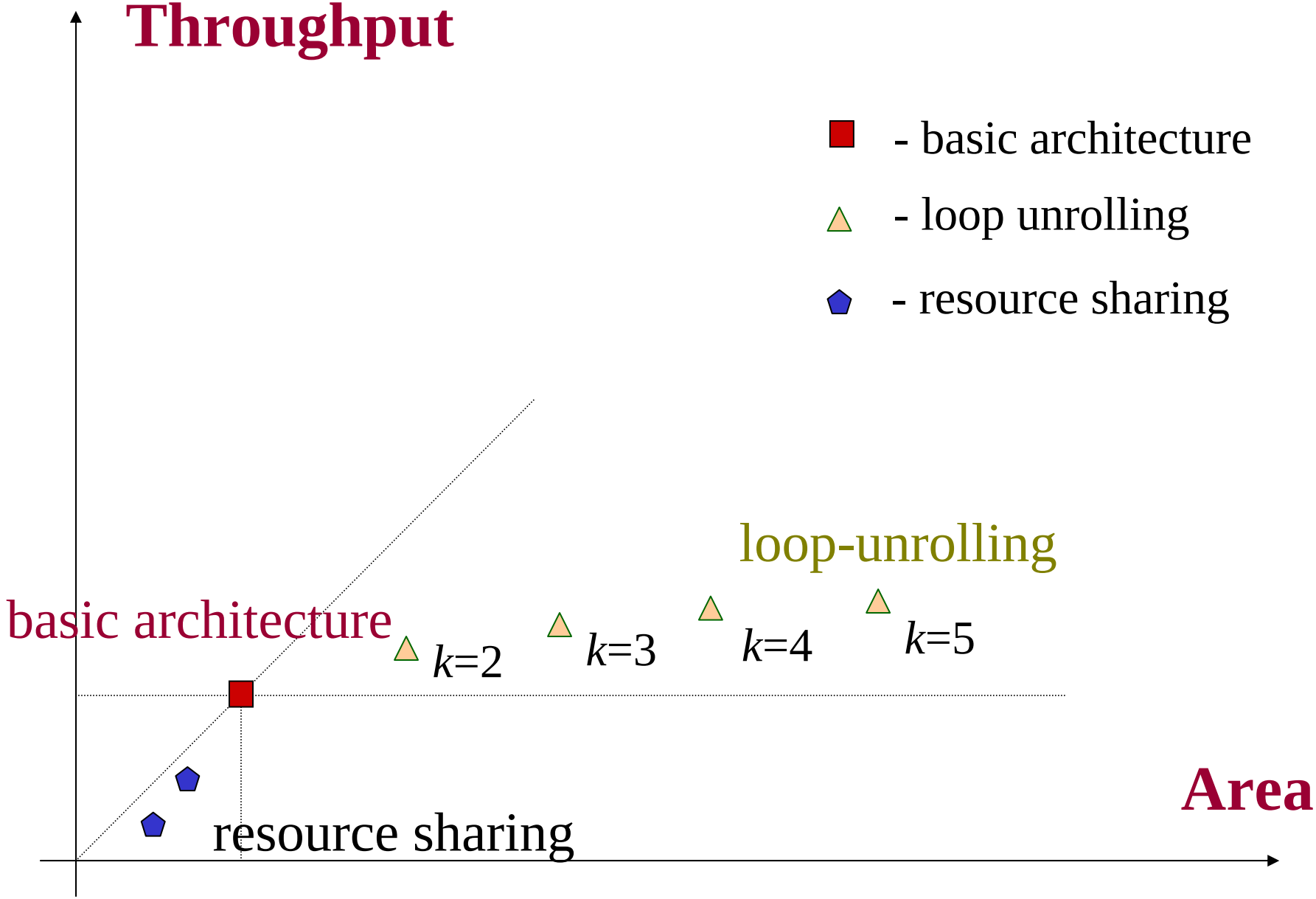
Partial Loop Unrolling

***K* rounds**

combinational logic

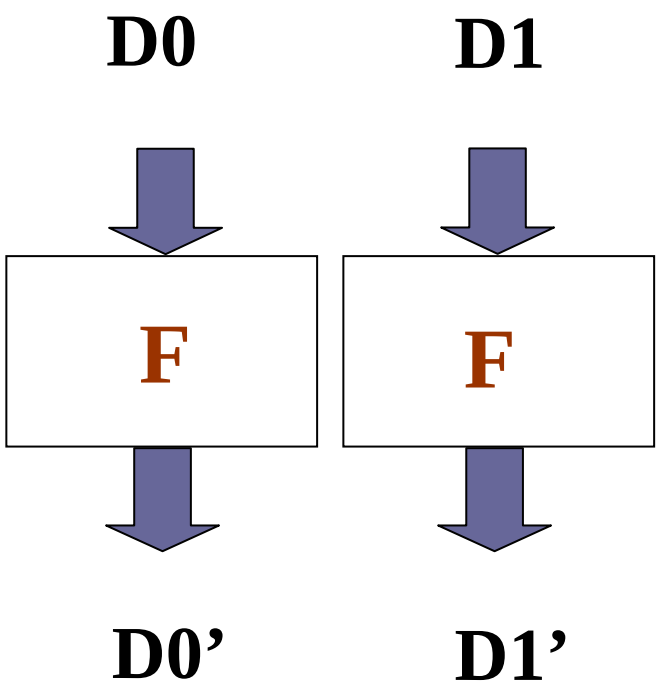


Loop Unrolling: Speed vs. Area

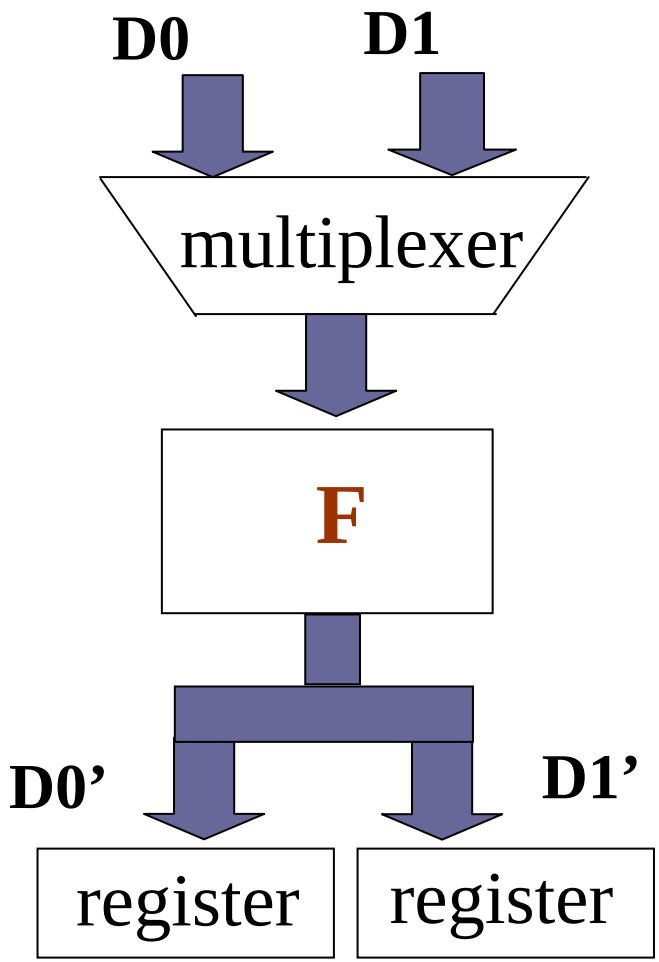


Decreasing area by resource sharing

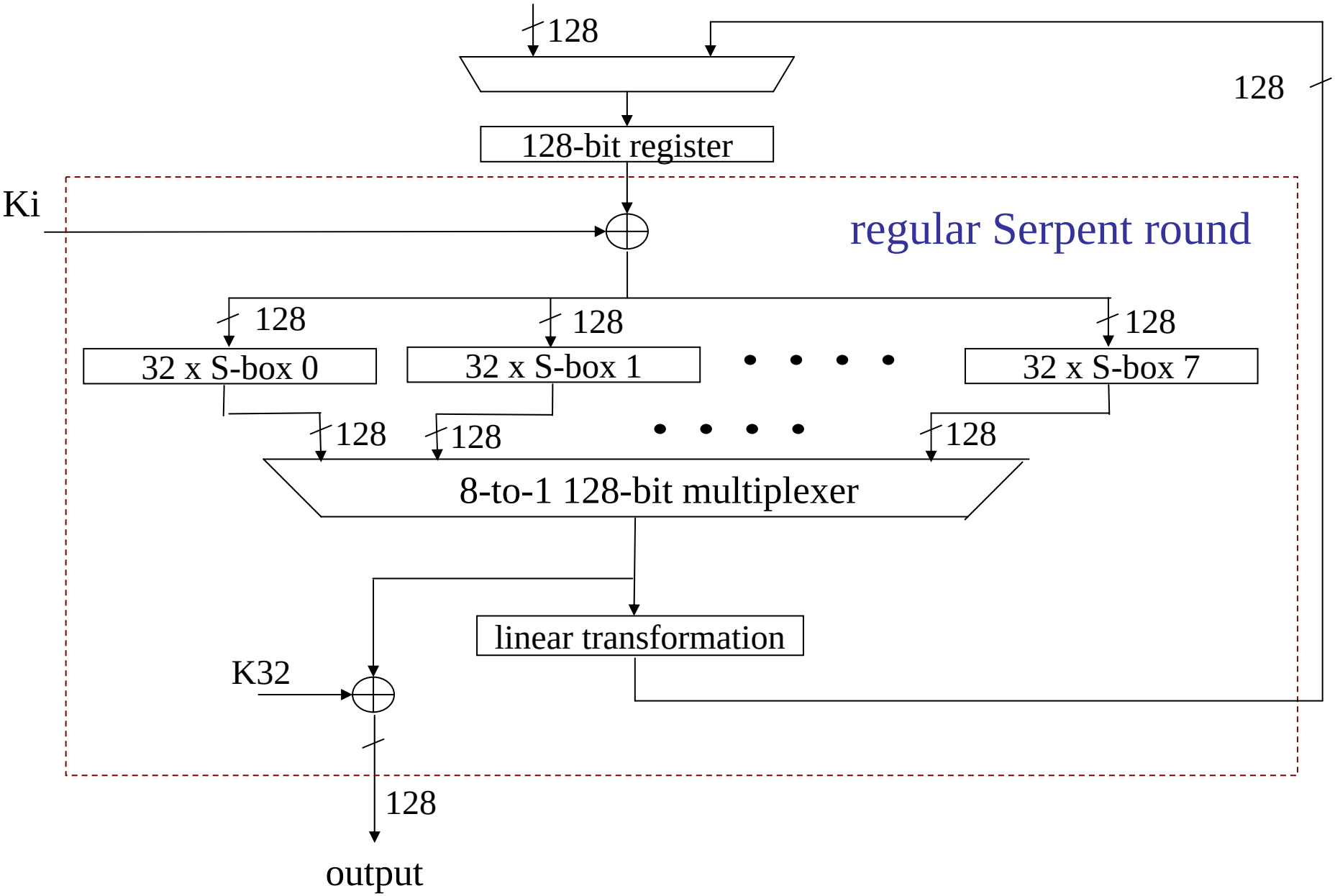
Before



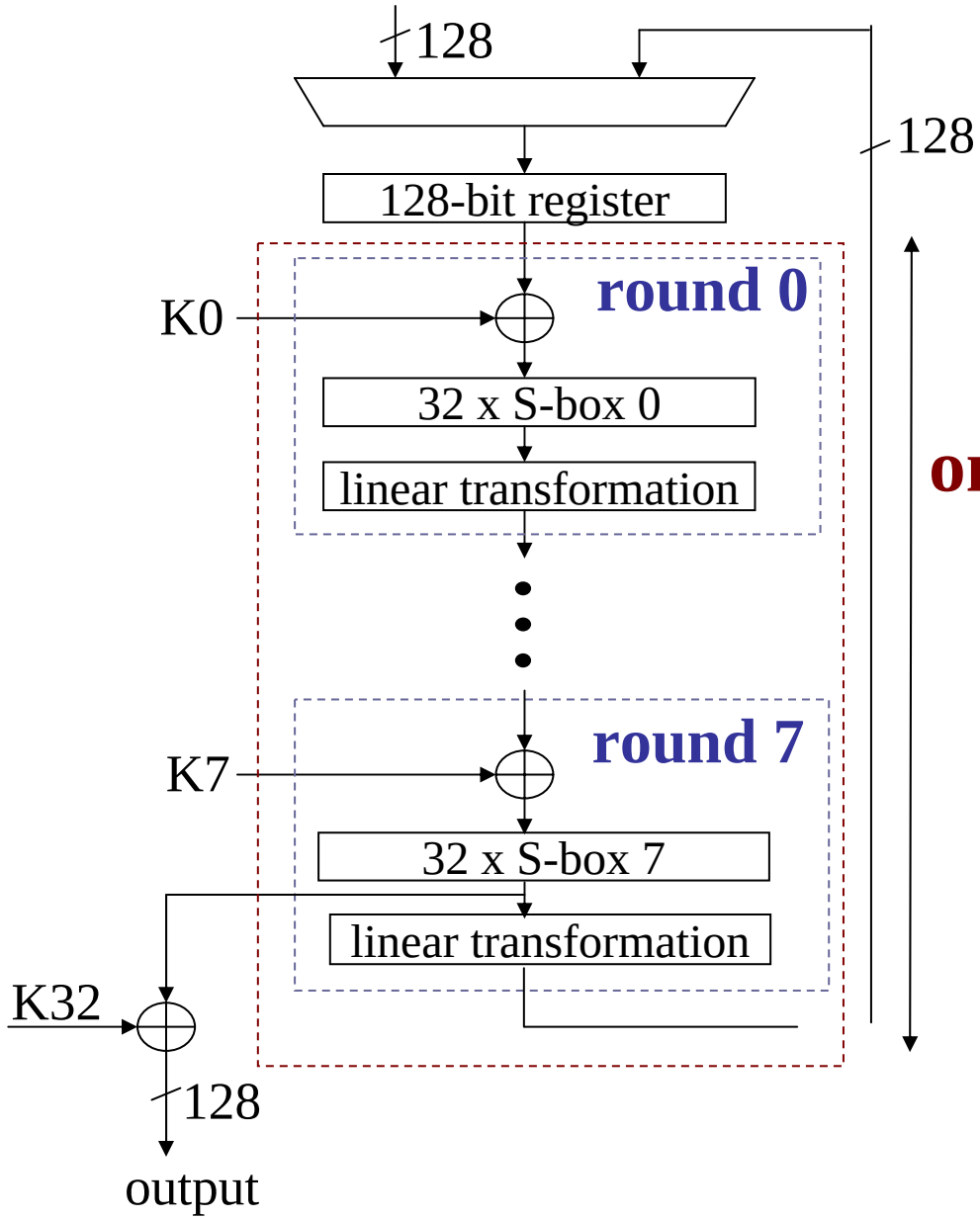
After



First basic architecture of Serpent - Serpent I1



Alternative basic architecture of Serpent: Serpent I8



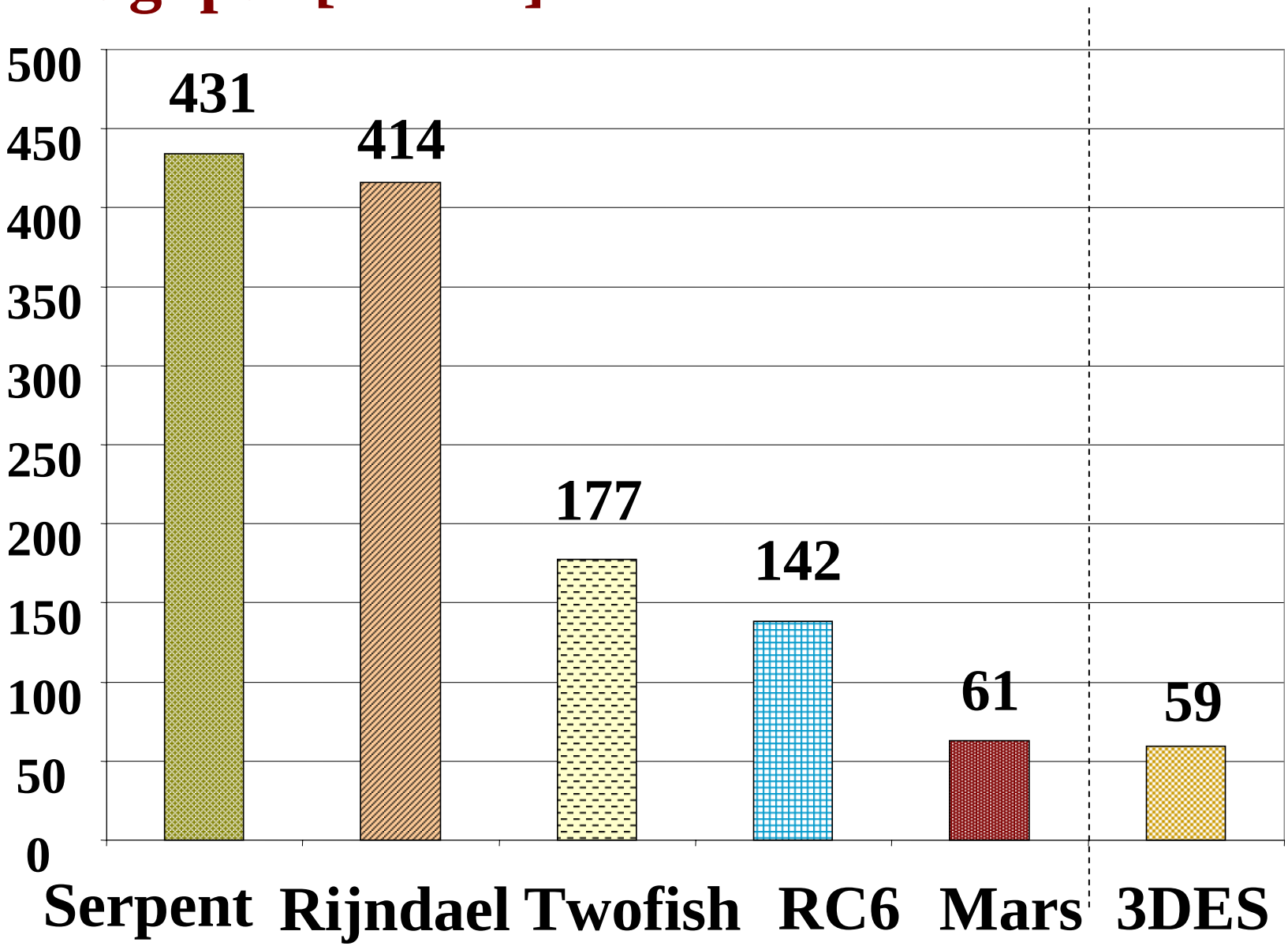
one implementation round of Serpent

=

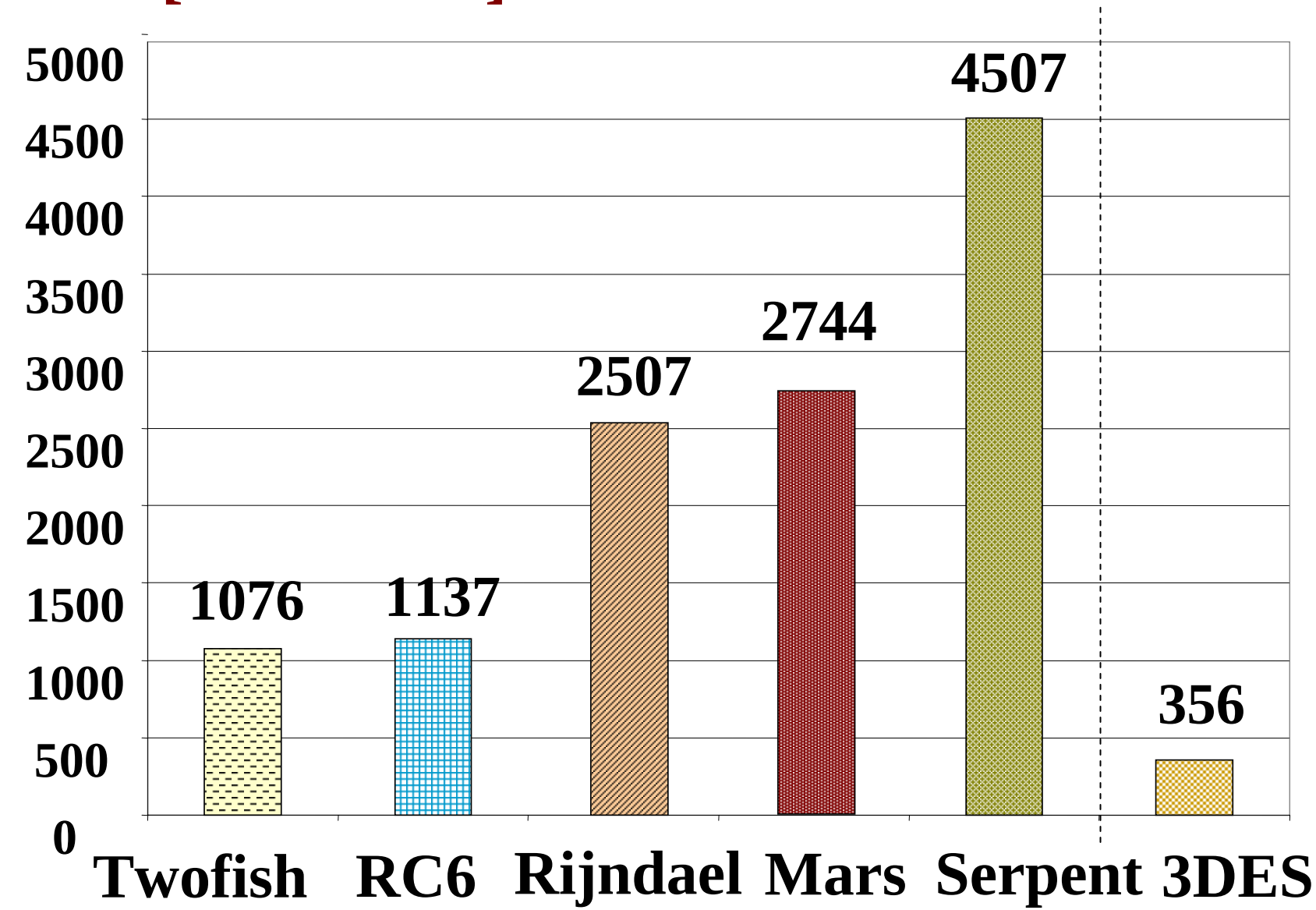
8 regular cipher rounds

Our Results: Basic architecture - Speed

Throughput [Mbit/s]

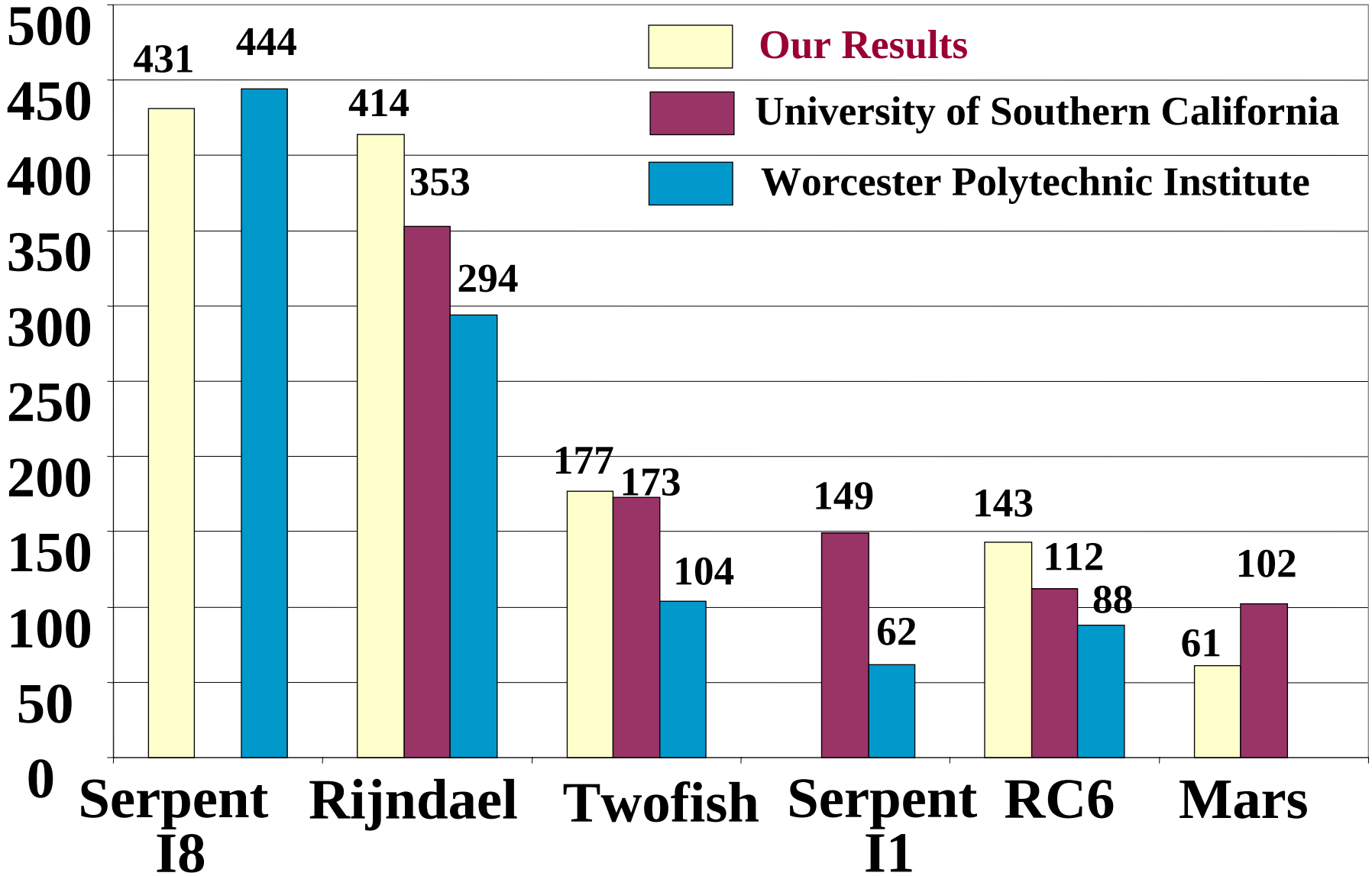


Our Results: Basic architecture - Area



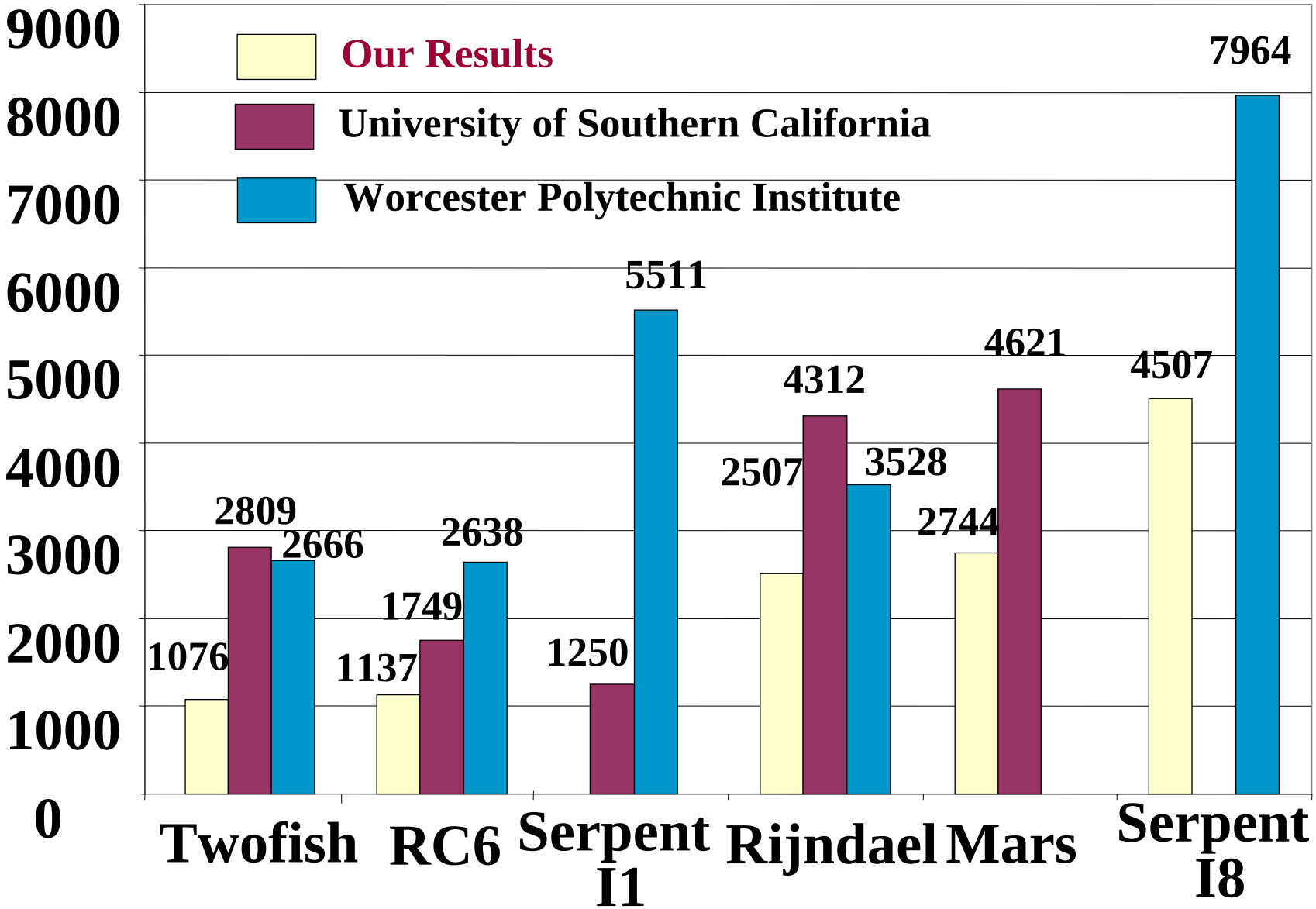
Comparison with results of other groups: Speed

Throughput [Mbit/s]

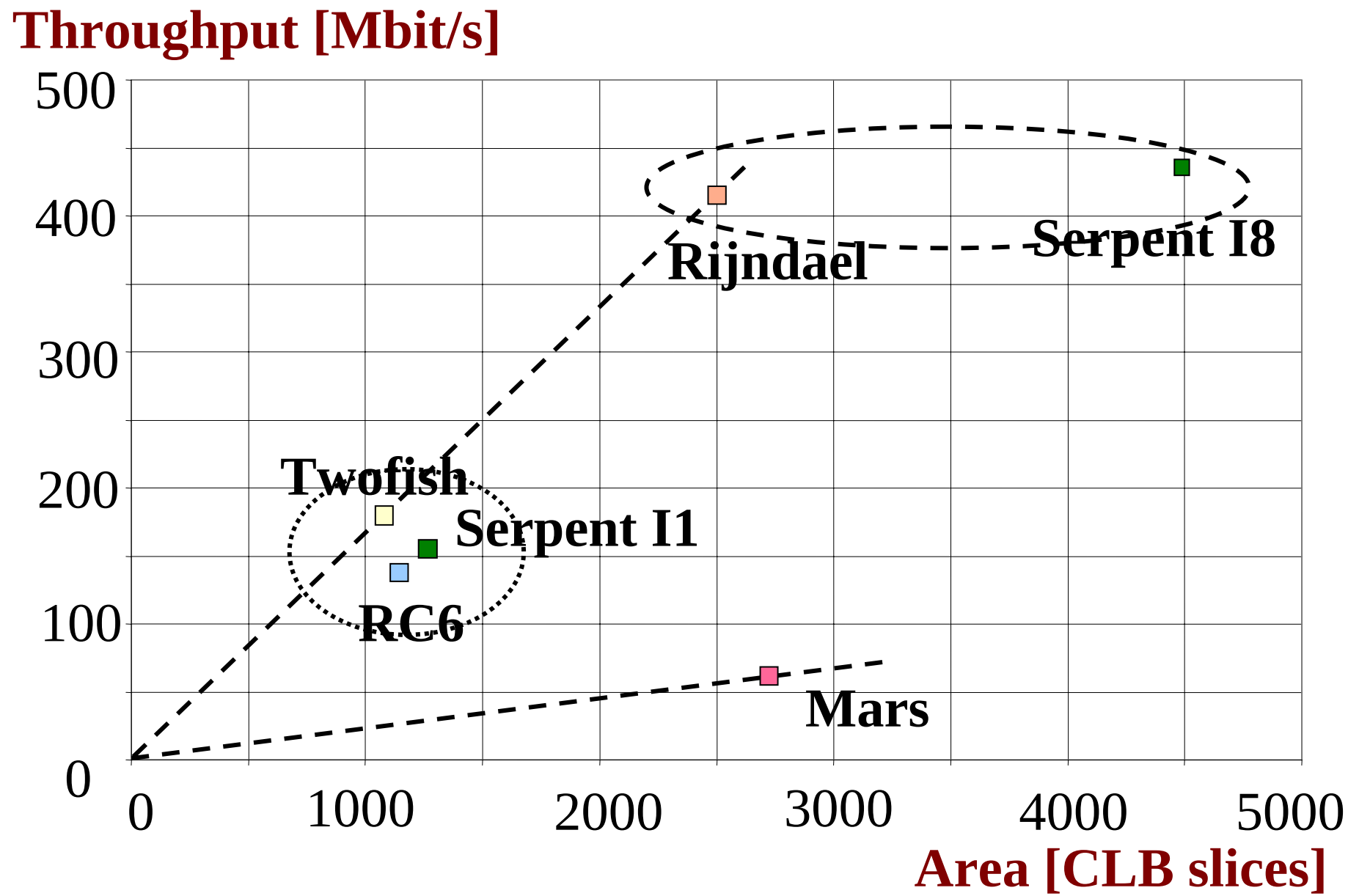


Comparison with results of other groups: Area

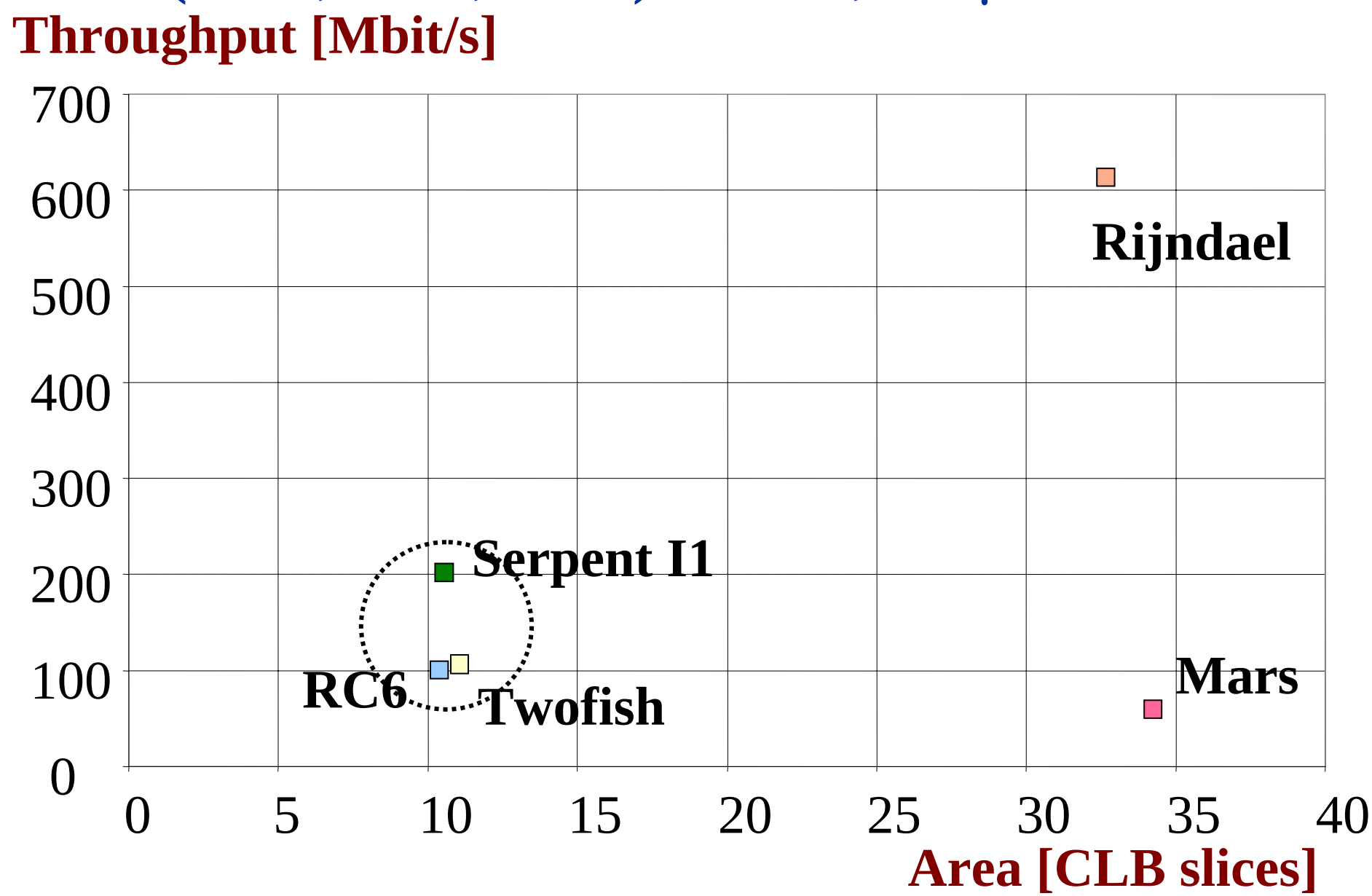
Area [CLB slices]



Our Results: Encryption in cipher feedback modes (CBC, CFB, OFB) - Virtex FPGA



NSA Results: Encryption in cipher feedback modes (CBC, CFB, OFB) - ASIC, 0.5 μm CMOS



Conclusions for feedback cipher modes (1) (CBC, CFB, OFB)

- **Speed** (throughput) should be the primary criteria of comparison

- **Basic iterative architecture** is the most appropriate for comparison and future implementations

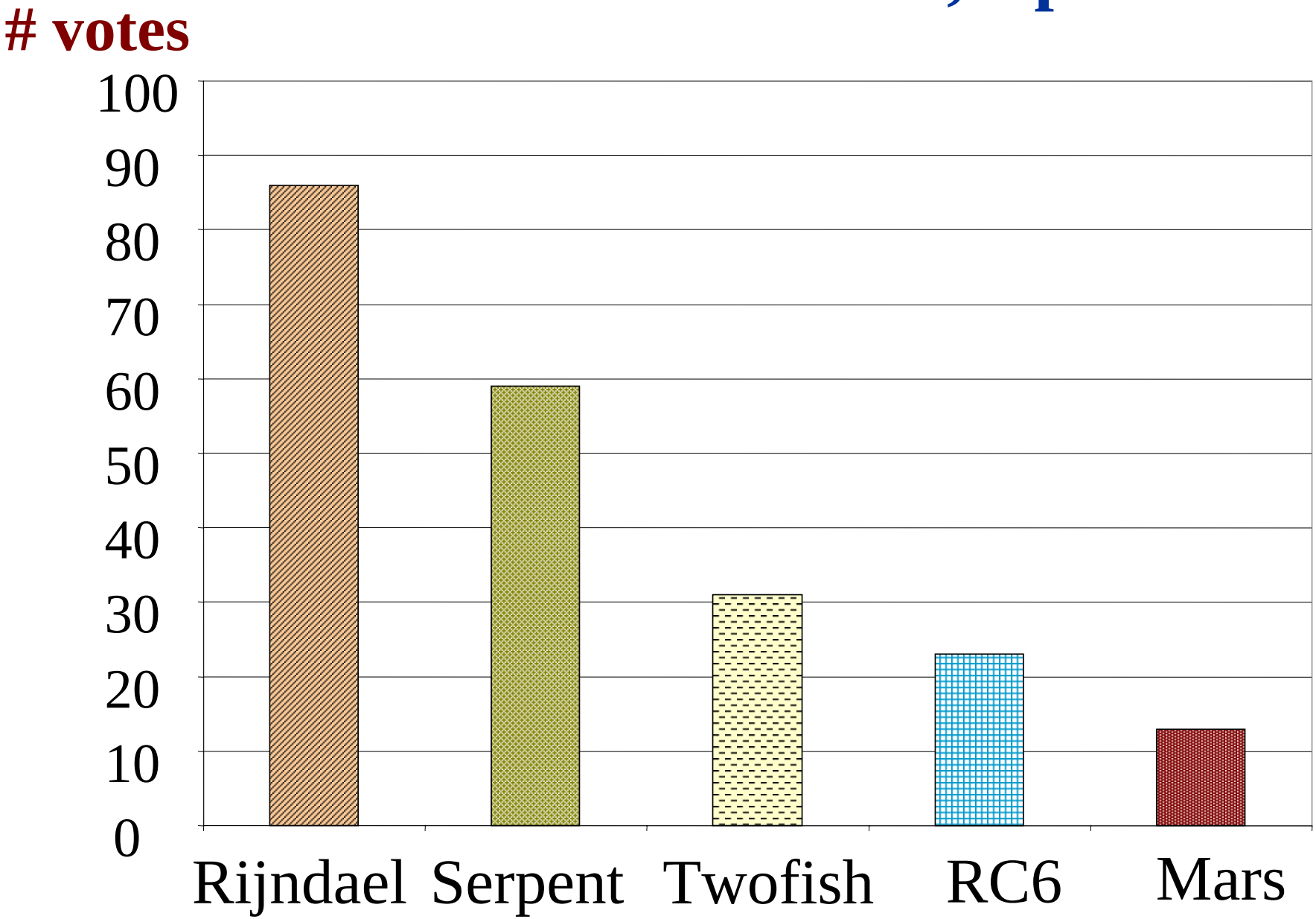
- **Serpent** and **Rijndael** are over twice as fast as the next best candidate for all implementations

Conclusions for feedback cipher modes (2) (CBC, CFB, OFB)

- **Results confirmed by**
  - **three independent university groups for FPGAs, and**
  - **NSA group for ASICs**

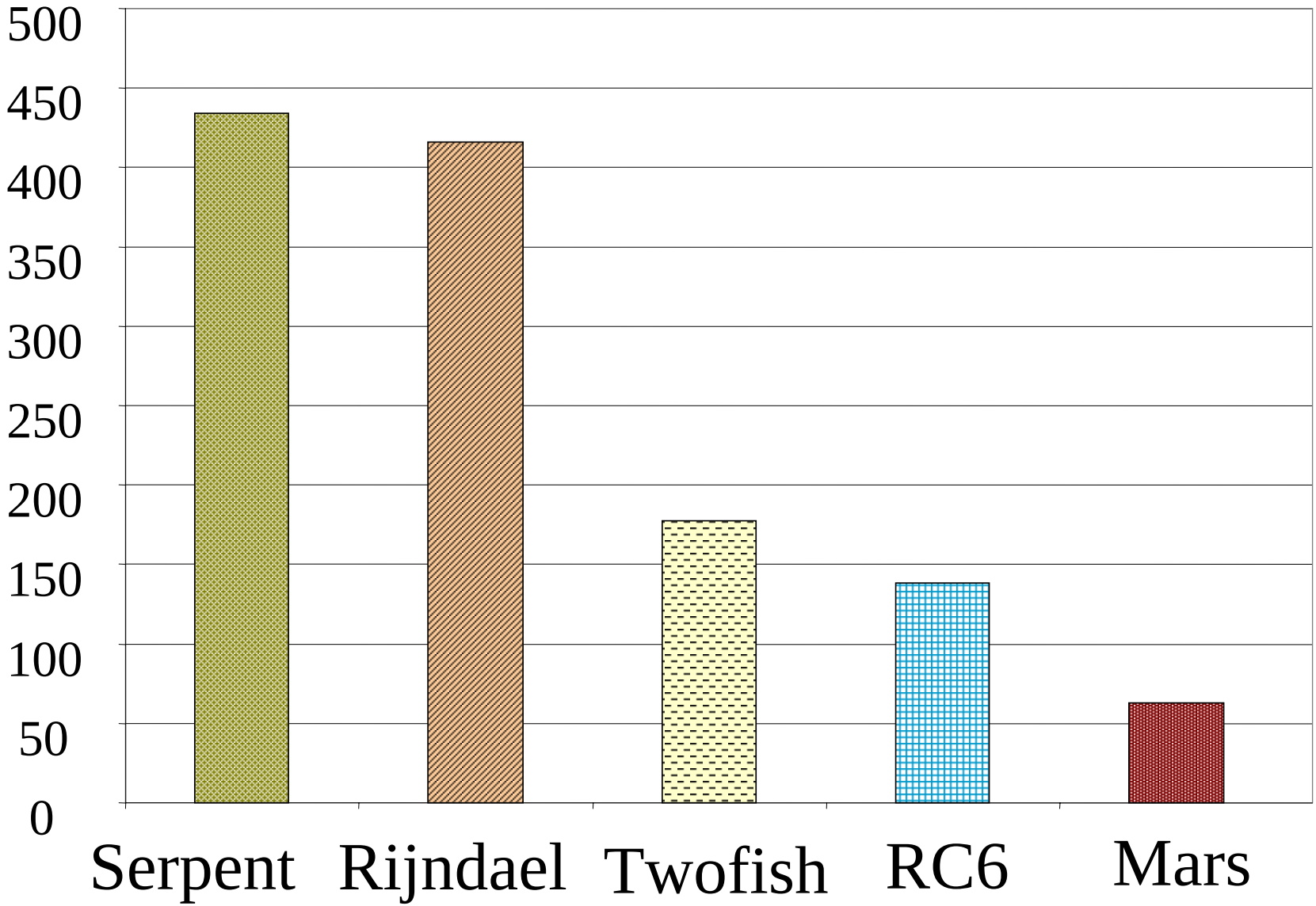
- **Results of comparison independent of implementation technology (FPGAs vs. ASICs)**

Survey filled by 167 participants of the Third AES Conference, April 2000



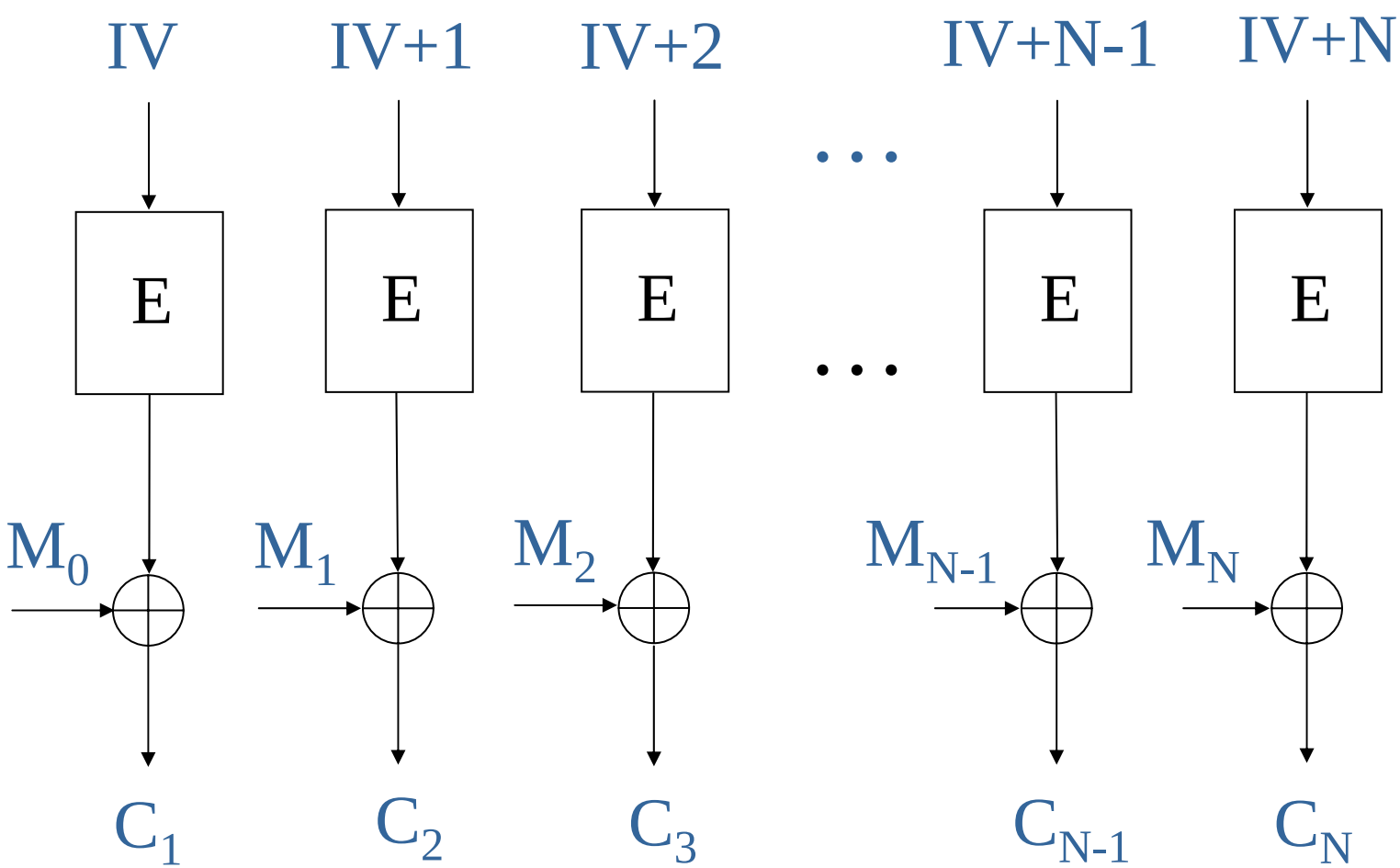
Our Results: Basic architecture - Speed

Throughput [Mbit/s]



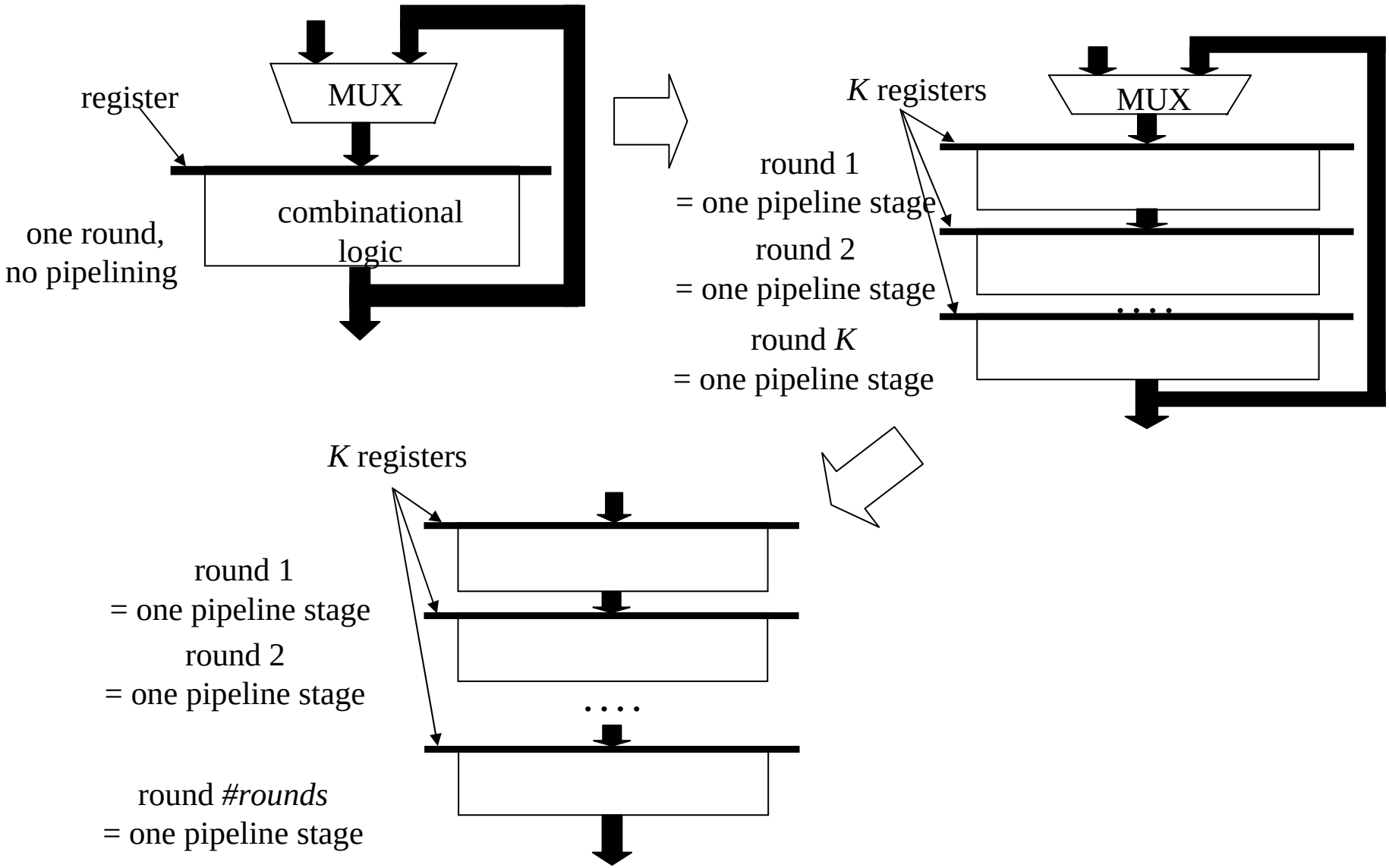
Non-Feedback Cipher Modes
ECB, counter

Comparison for non-feedback cipher modes, e.g. Counter Mode - CTR

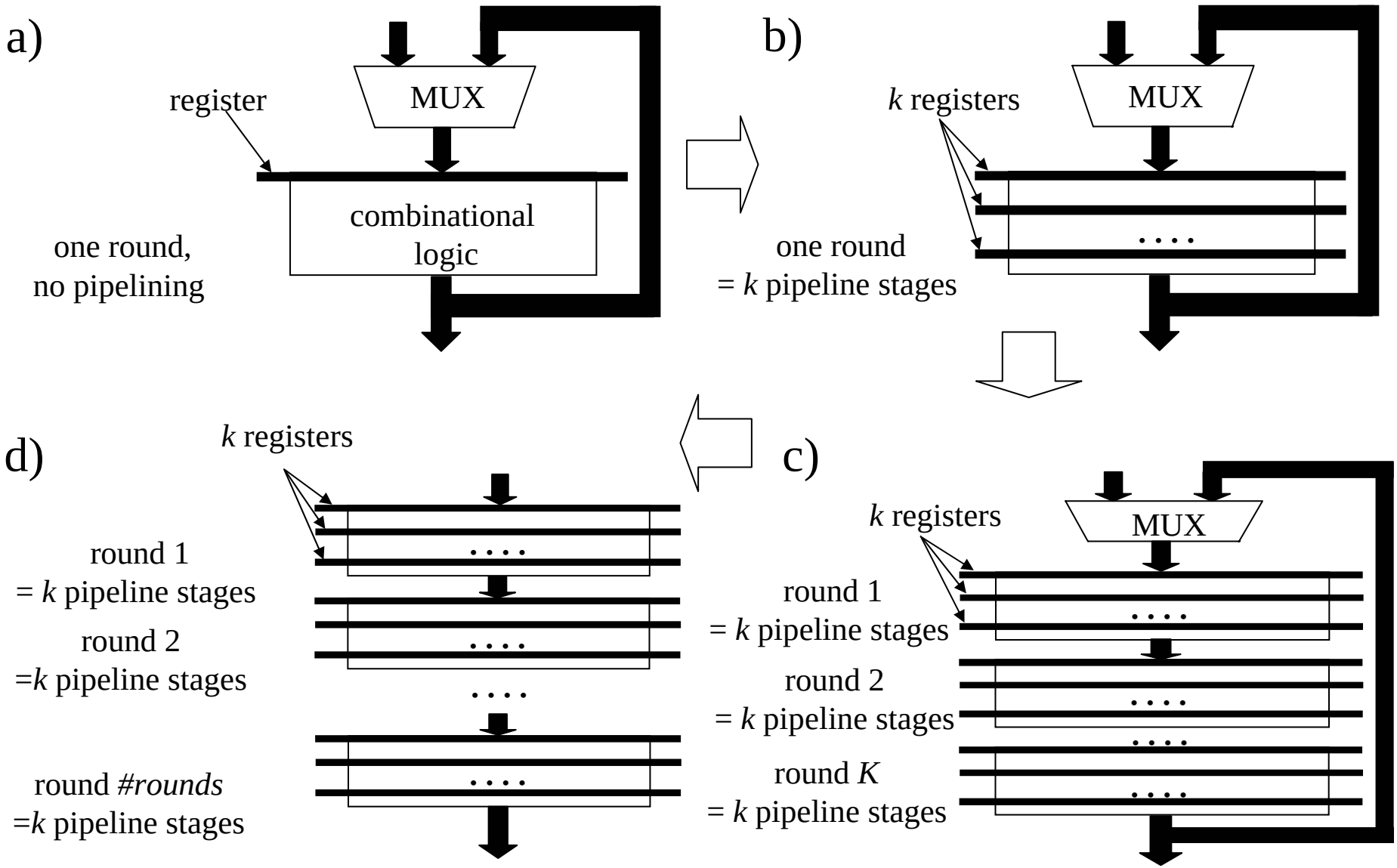


$C_i = M_i \oplus AES(IV+i)$ for i=0..N

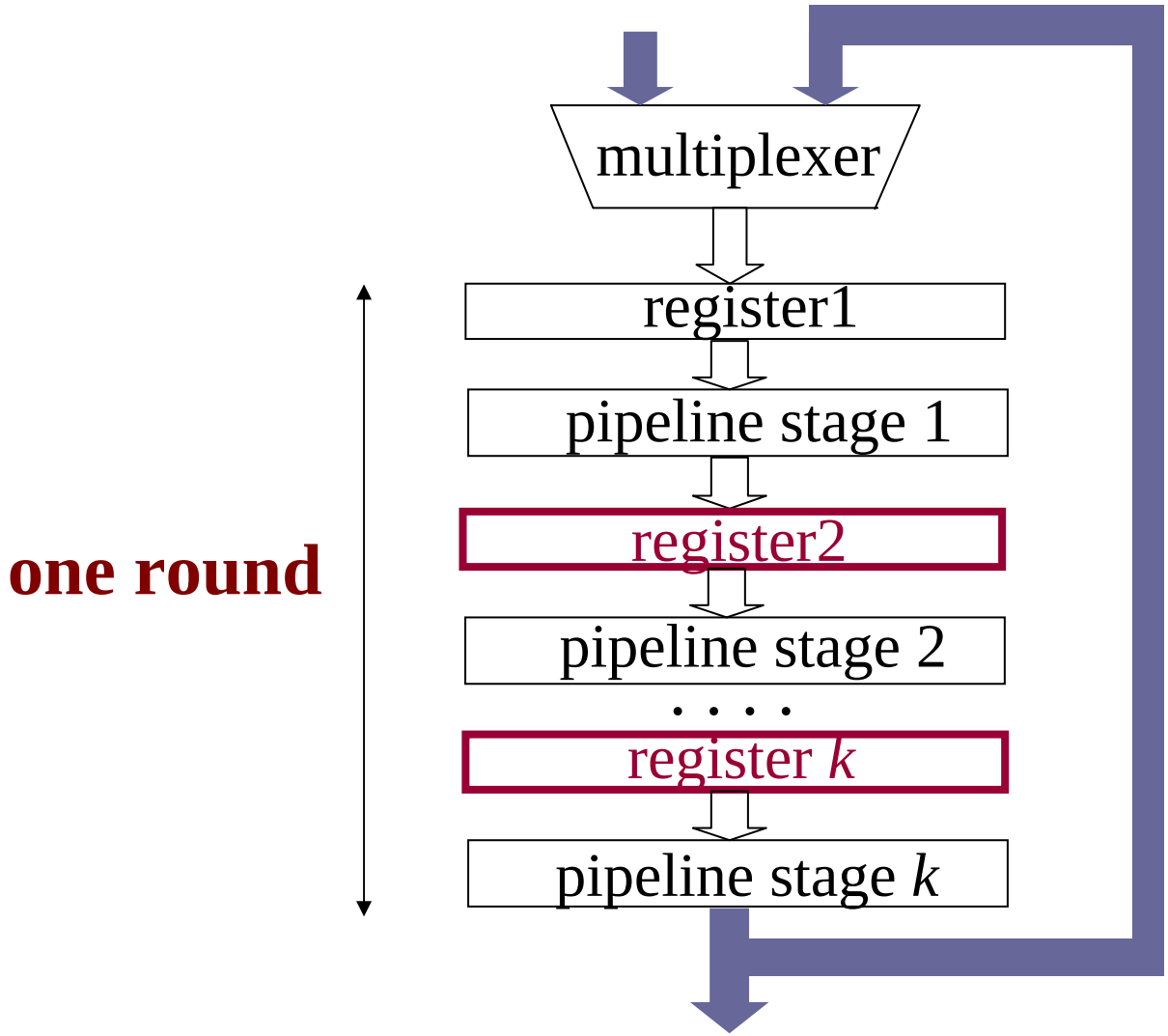
NSA approach: Traditional methodology



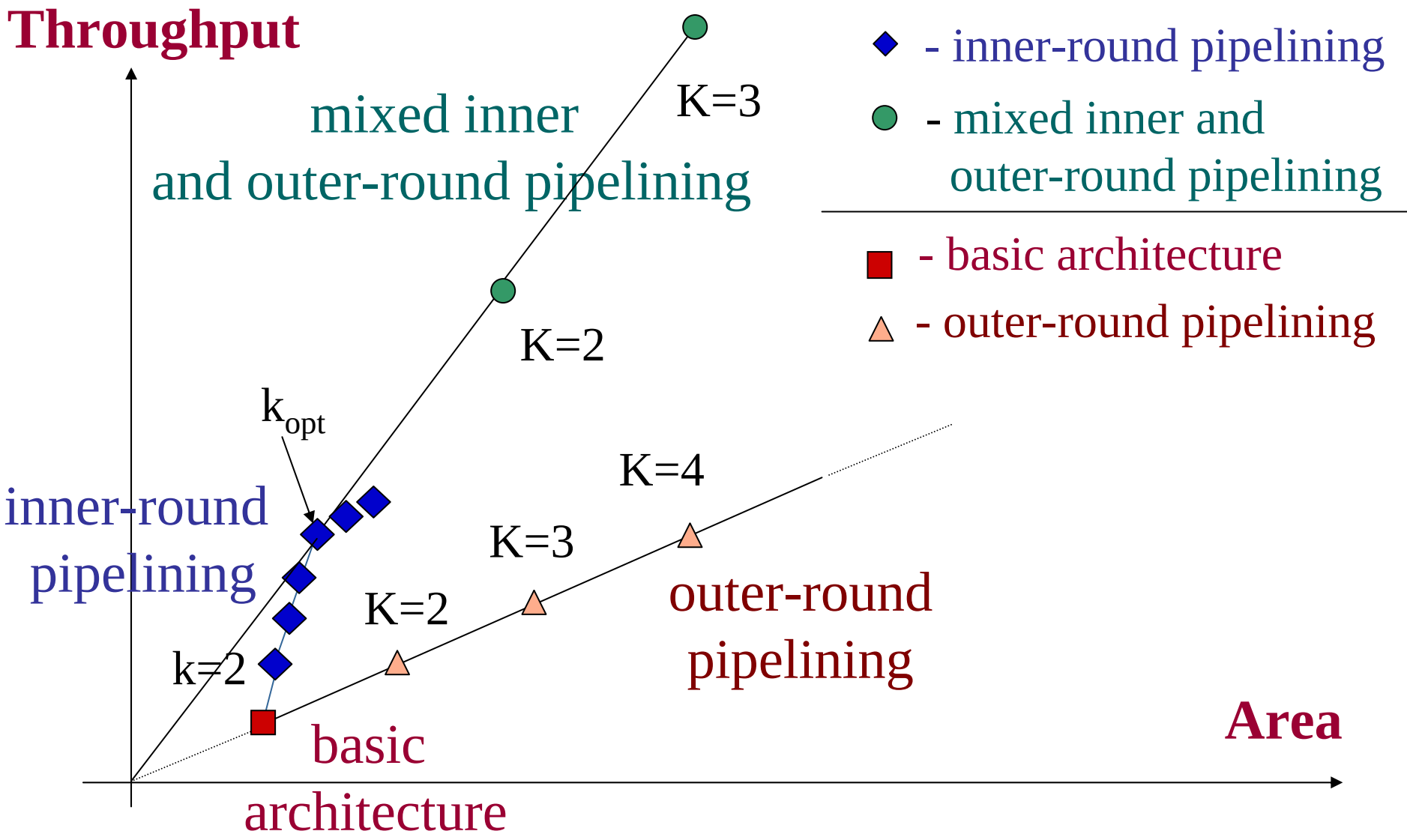
Our approach: New methodology



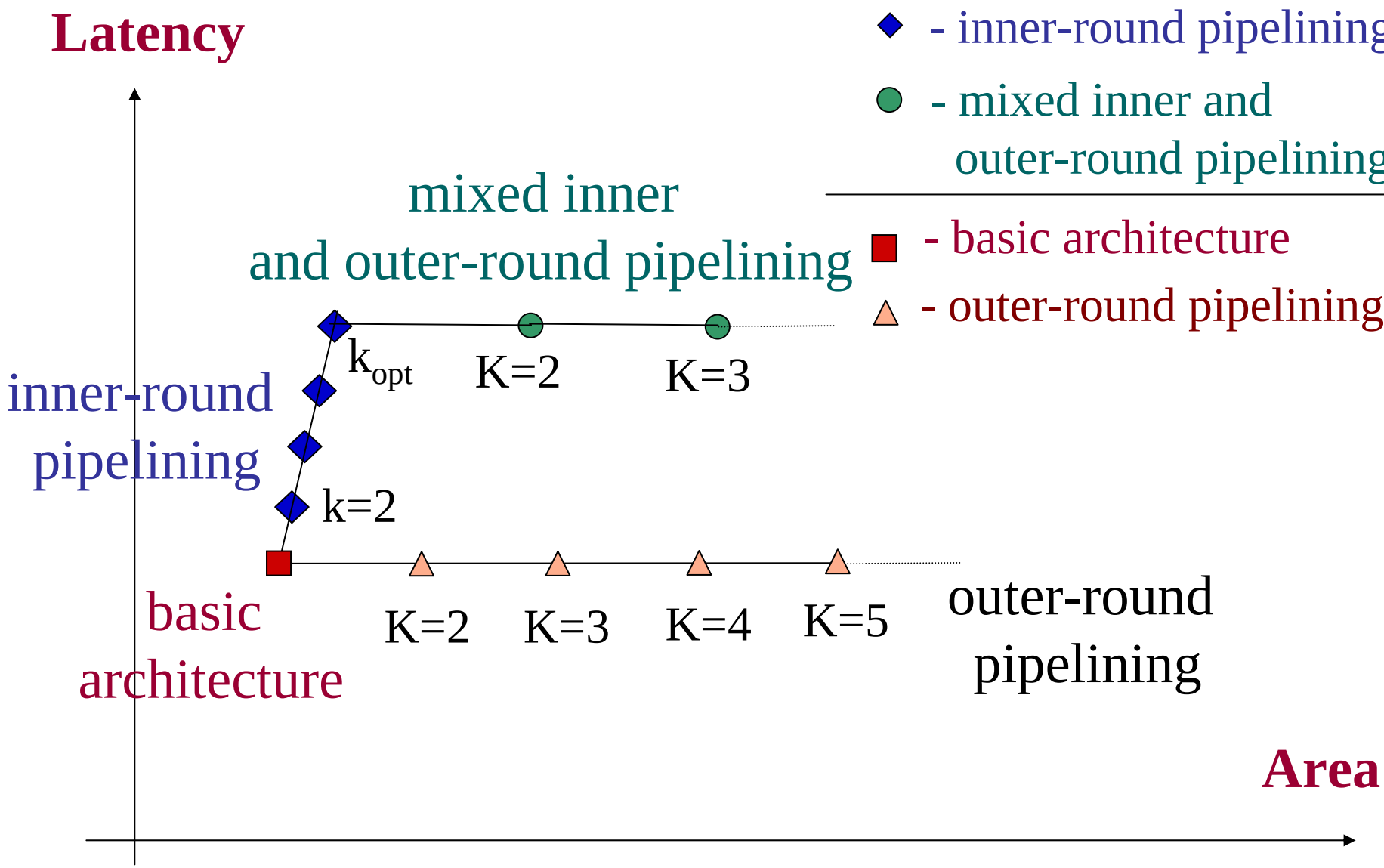
Our approach: Inner-Round Pipelining



Comparison of the traditional and new design methodologies



Latency vs. area dependence for the new design methodology



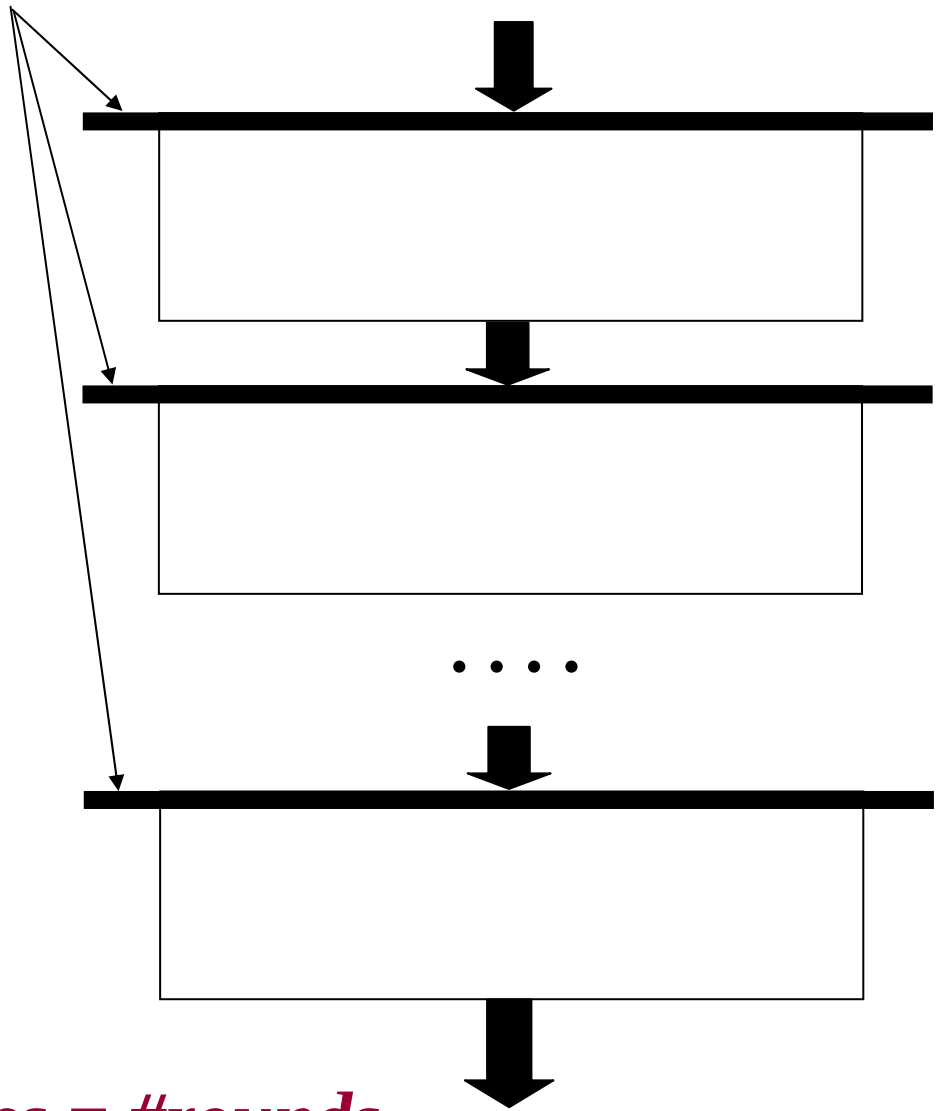
NSA architecture:
Full outer-round pipelining

***#rounds* registers**

round 1
= one pipeline stage

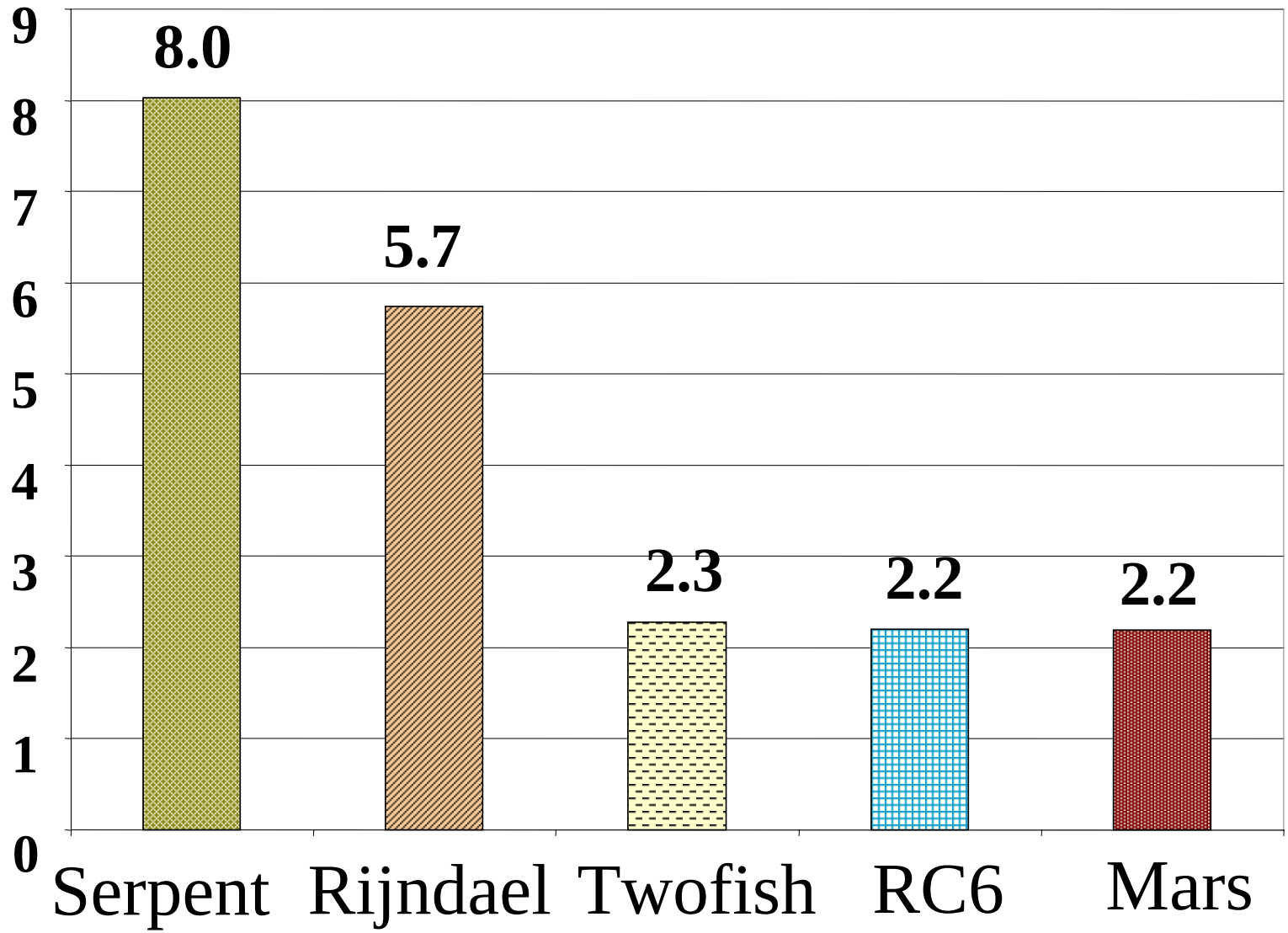
round 2
= one pipeline stage

round *#rounds*
= one pipeline stage



Total # of pipeline stages = #rounds

NSA Results: Full outer-round pipelining CMOS ASIC 0.5 μm



Our approach:

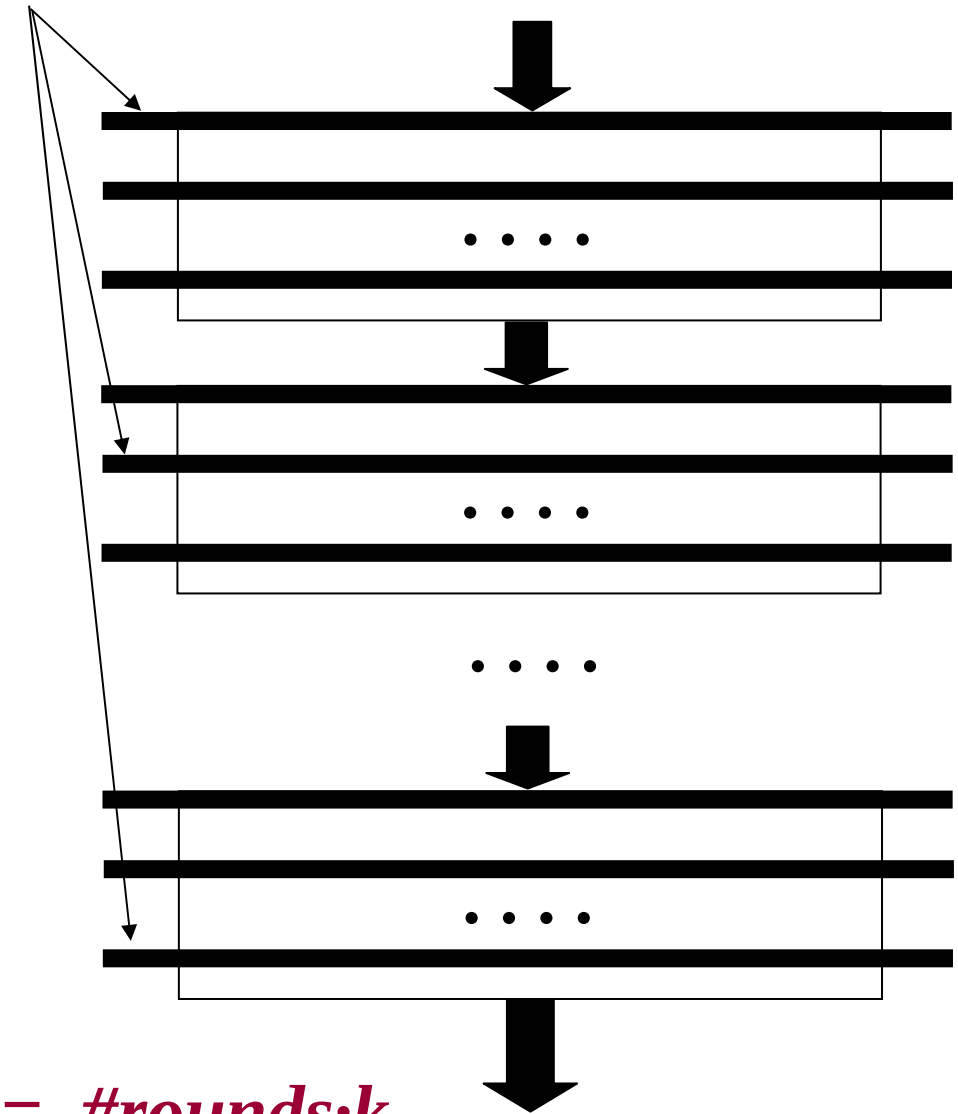
Full mixed inner- and outer-round pipelining

***k* registers**

round 1
= *k* pipeline stages

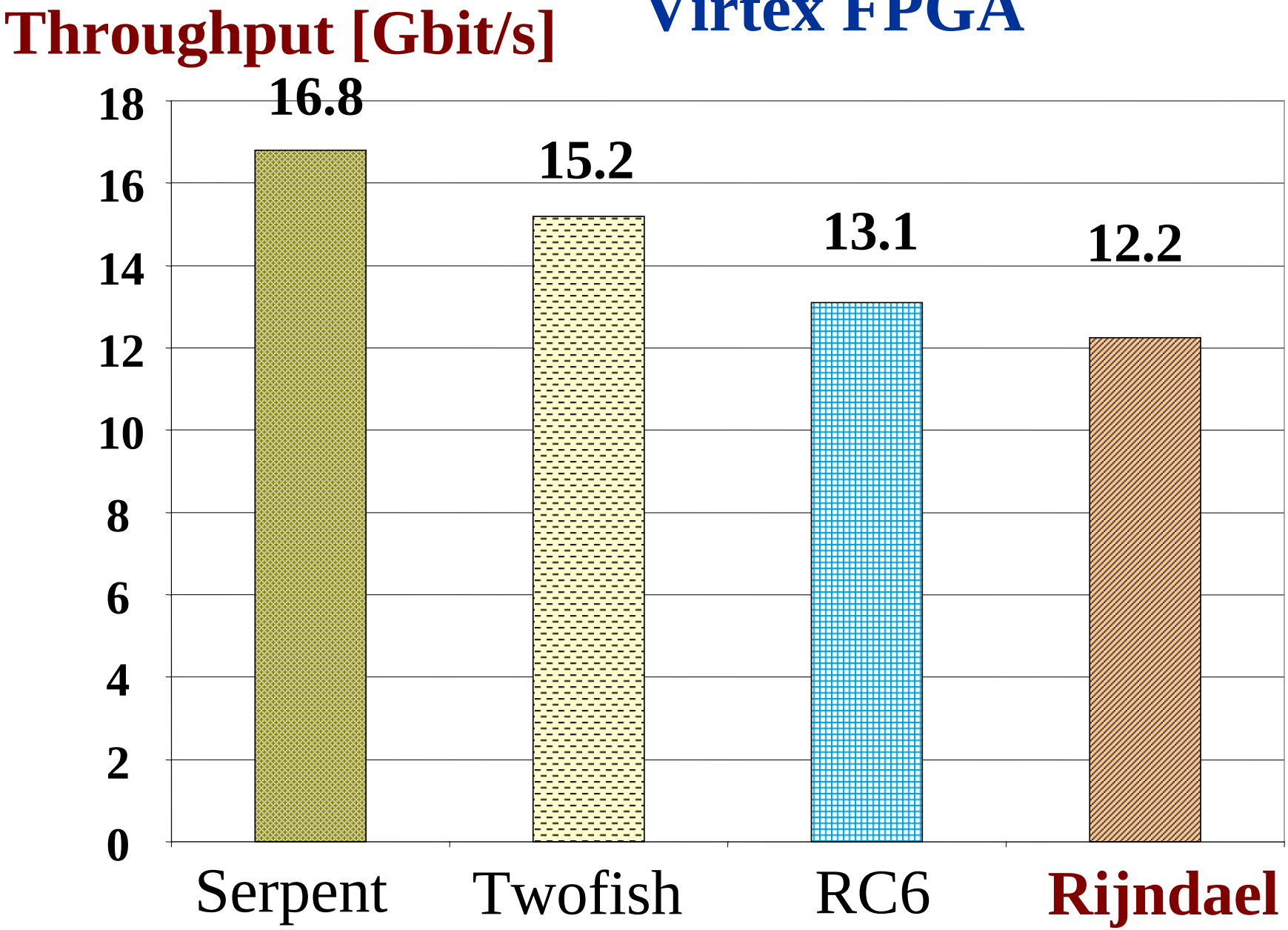
round 2
=*k* pipeline stages

round *#rounds*
=*k* pipeline stages

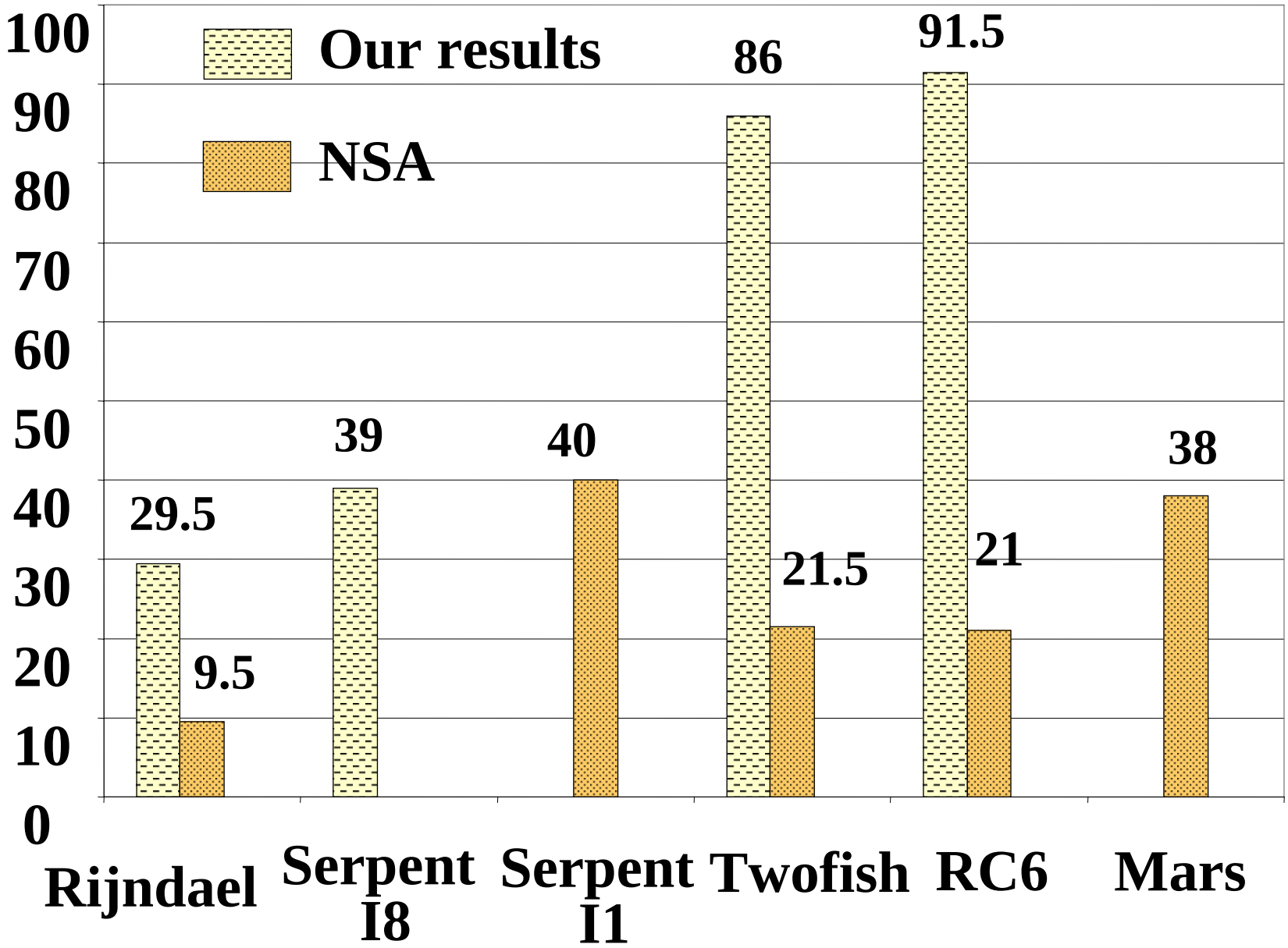


Total # of pipeline stages = #rounds·k

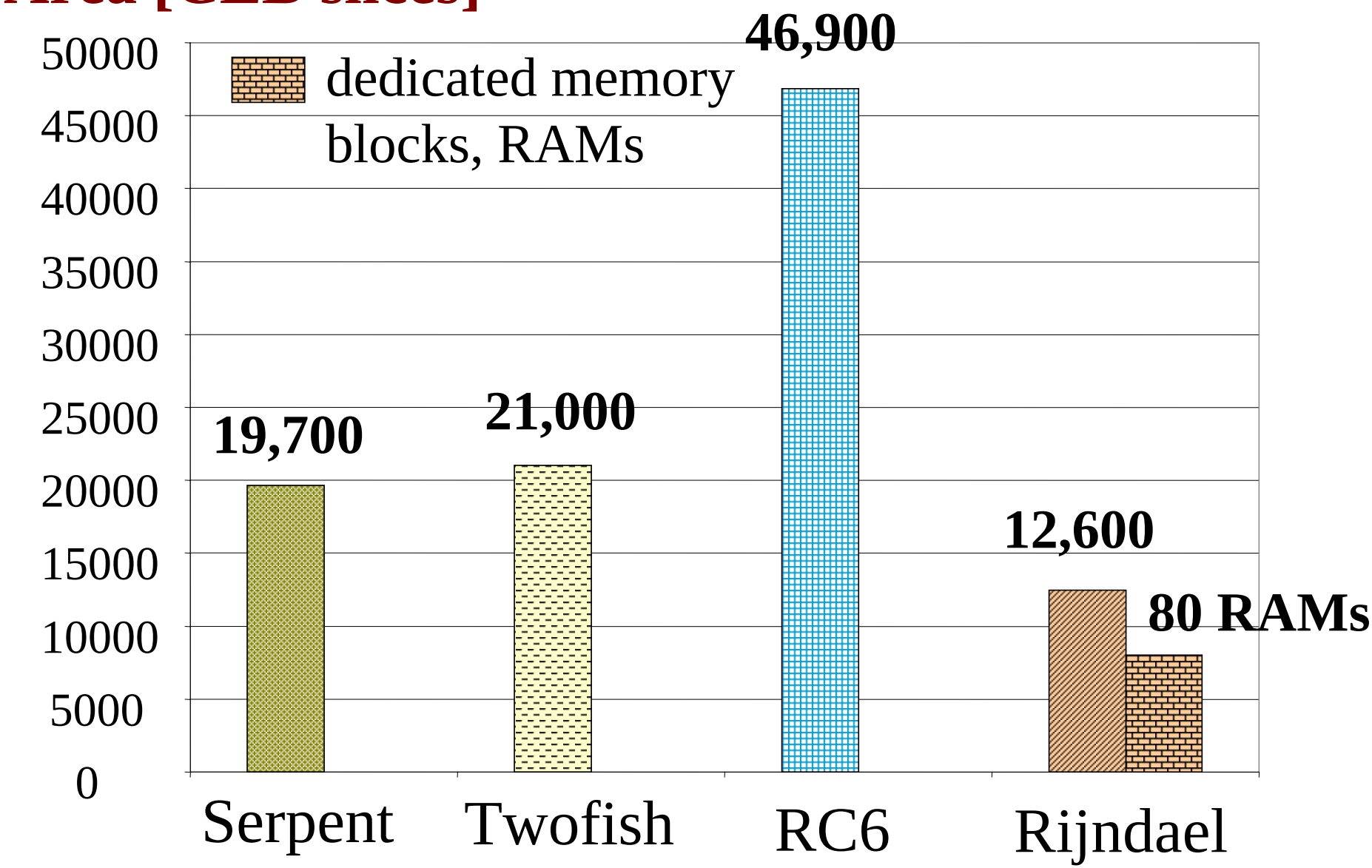
Our Results: Full mixed pipelining Virtex FPGA



Speed-up compared to the basic architecture

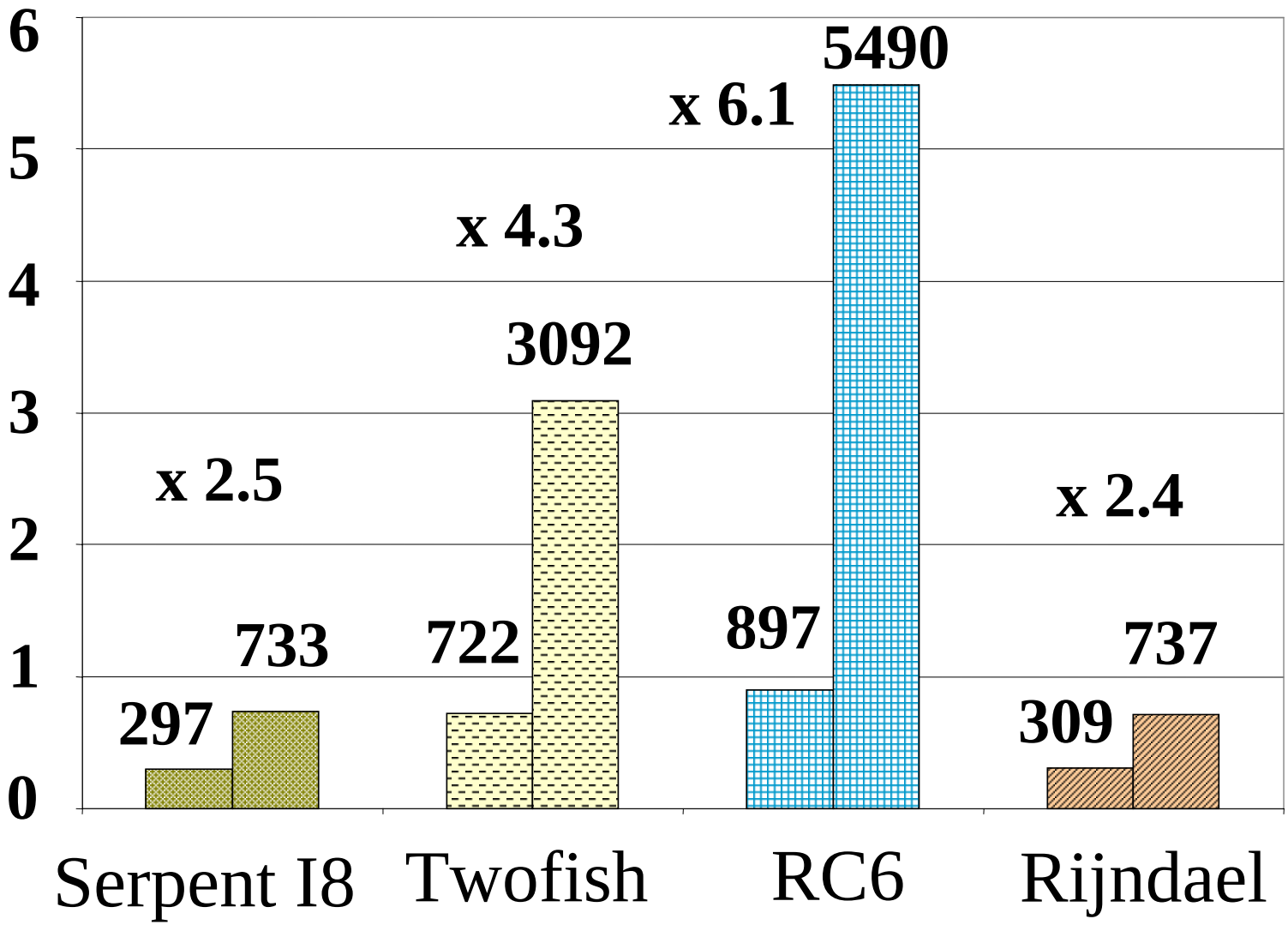


Our Results: Full mixed pipelining



Our Results: Increase in the circuit latency

Latency without and with pipelining [μs]



Conclusions for non-feedback cipher modes (1) ECB, counter

- **All ciphers can achieve approximately 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**

Conclusions for non-feedback cipher modes (2)
ECB, counter

No agreement regarding the methodology and architecture used for comparison

NSA methodology favored ciphers with

- **short cipher round**
- **large number of rounds**

Our methodology

- **fair**
- **practical (superior throughput/area ratio)**

Importance of the AES candidate hardware efficiency comparison

- **Important factor used to differentiate among final candidates**

  - objective and commonly accepted measures
  - good agreement among results from various groups
  - large differences among final candidates

- **Efficient architectures and methodologies developed for all algorithms**

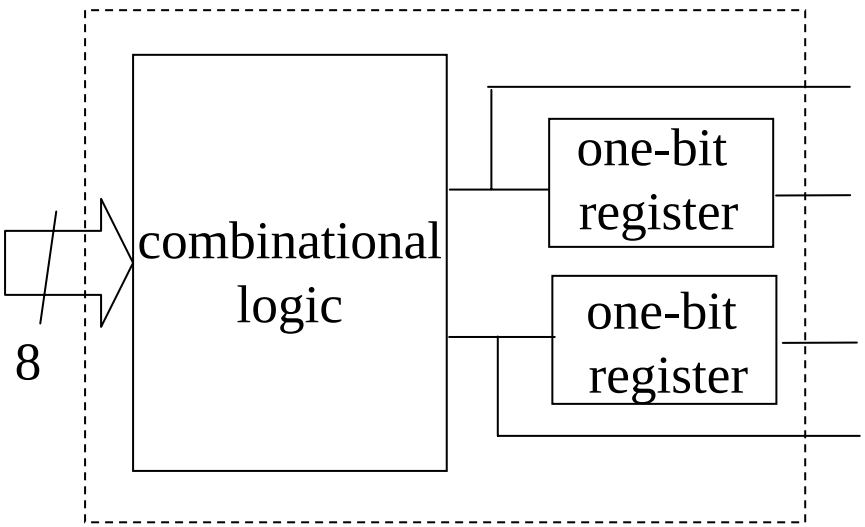
Basic building blocks of FPGA devices

Virtex

CLB slice = 1/2 of a CLB

CLB - Configurable Logic Block

Logic mode



Memory mode