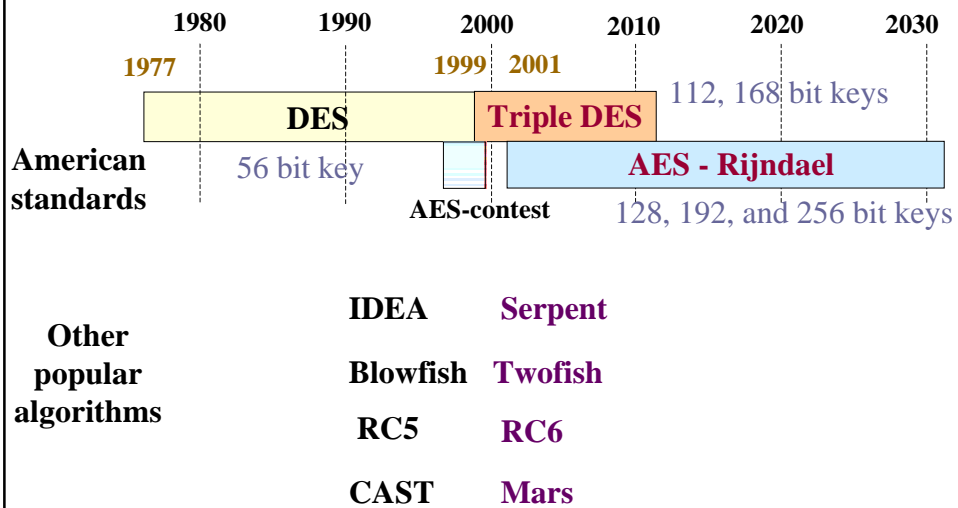


Pawel Chodowiec, Po Khuon, Kris Gaj
Electrical and Computer Engineering
George Mason University

**Fast implementations of
secret-key block ciphers using
mixed inner- and outer-round
pipelining**

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

Most popular secret-key ciphers



AES Contest

June 1998

15 Candidates

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

Round 1

Security
Software implementations

August 1999

5 final candidates

Mars, RC6, Rijndael, Serpent, Twofish

Round 2

Security
Hardware implementations

October 2000

1 winner: Rijndael
Belgium

Selected applications of secret-key ciphers

E-banking

ATM machines
Home-banking
Inter-bank transfers

Internet

Server-browser - SSL
Virtual Private Networks - IPsec
Electronic Payment Cards - SET

Wireless communication

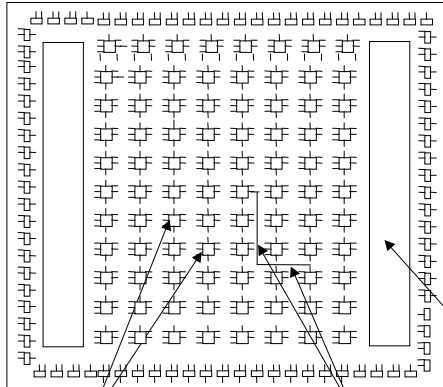
Mobile phones
Satellite communication

High-speed networks

ATM, B-ISDN, HDTV

Target FPGA devices

Xilinx Virtex - XCV 1000

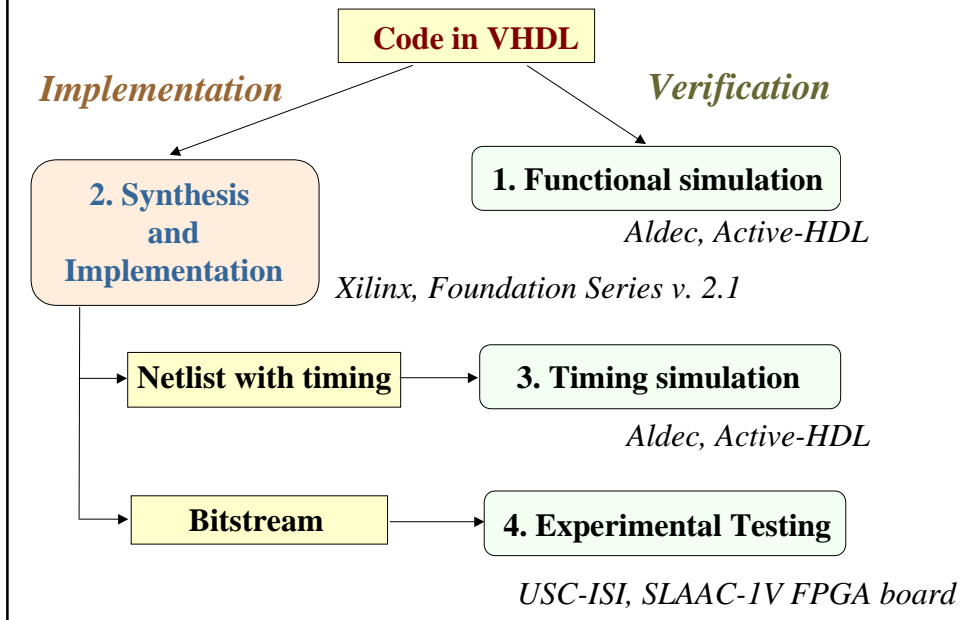


- 0.22 μm CMOS process
- 12 288 CLB slices
- 10 4-kbit block RAMs
- 1 mln equivalent logic gates
- Up to 200 MHz clock

Block RAMs

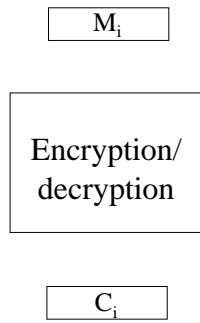
Configurable Logic Block slices (CLB slices) Programmable Interconnects

Methodology and Tools

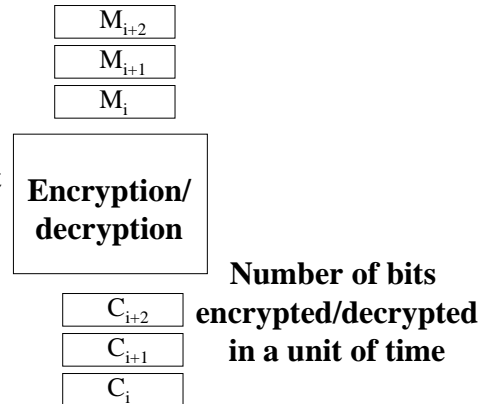


Primary parameters of hardware implementations of secret-key block ciphers

Latency



Throughput

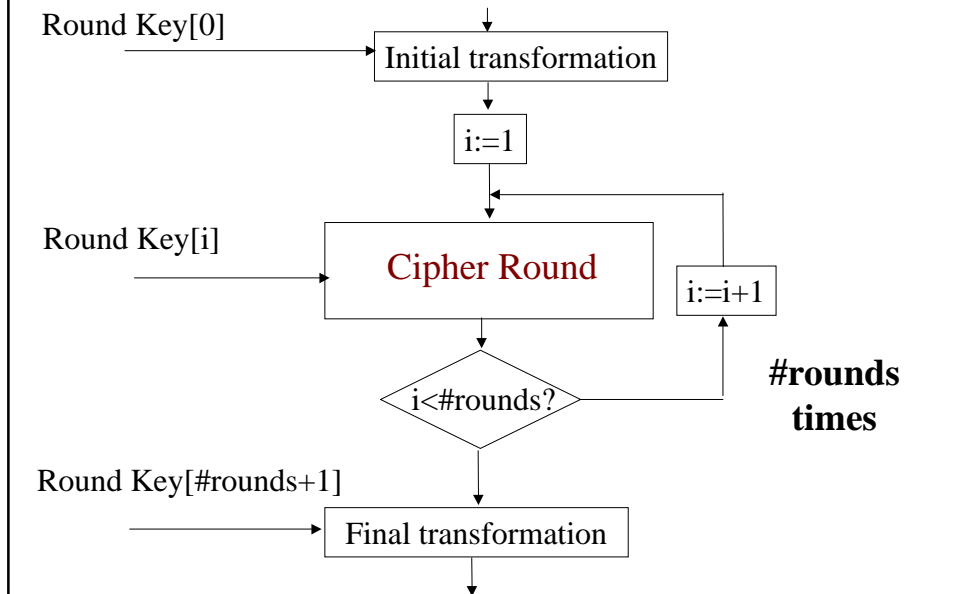


Time to
encrypt/decrypt
a single block
of data

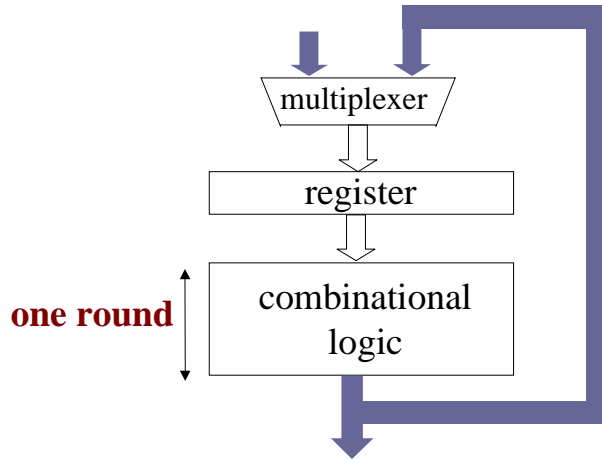
Number of bits
encrypted/decrypted
in a unit of time

$$\text{Throughput} = \frac{\text{Block_size} \cdot \text{Number_of_blocks_processed_simultaneously}}{\text{Latency}}$$

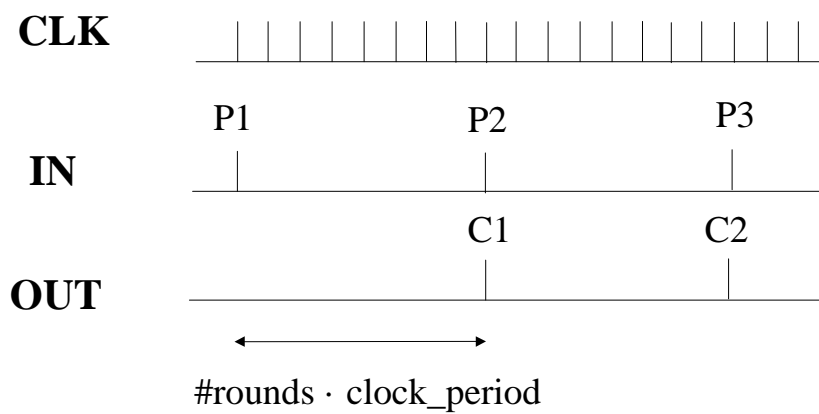
Typical Internal Structure of a Secret-Key Block Cipher

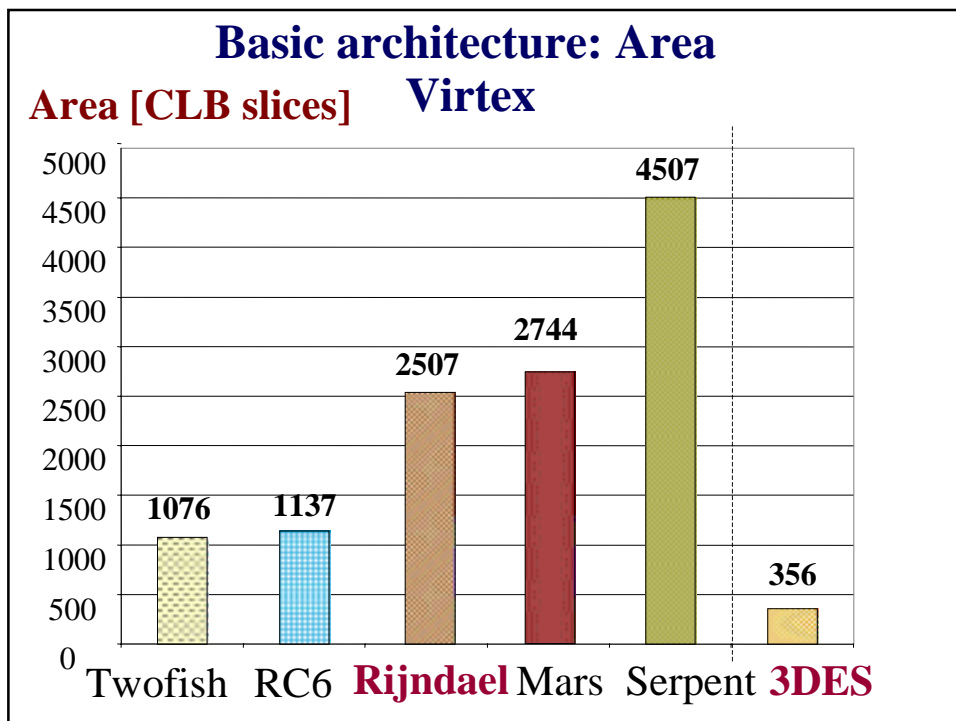
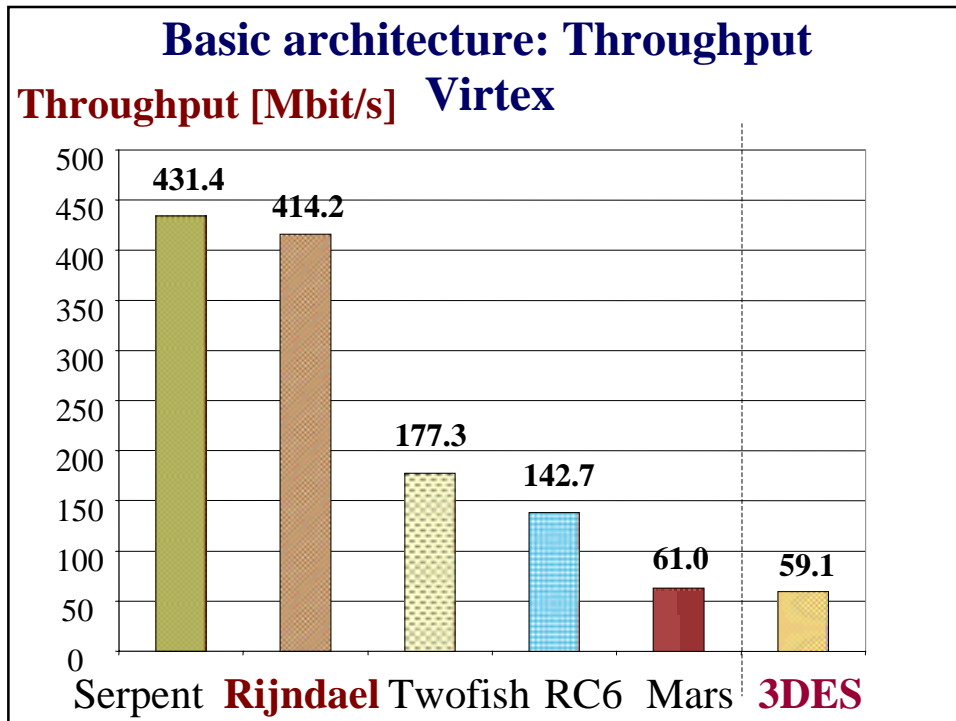


Basic iterative architecture

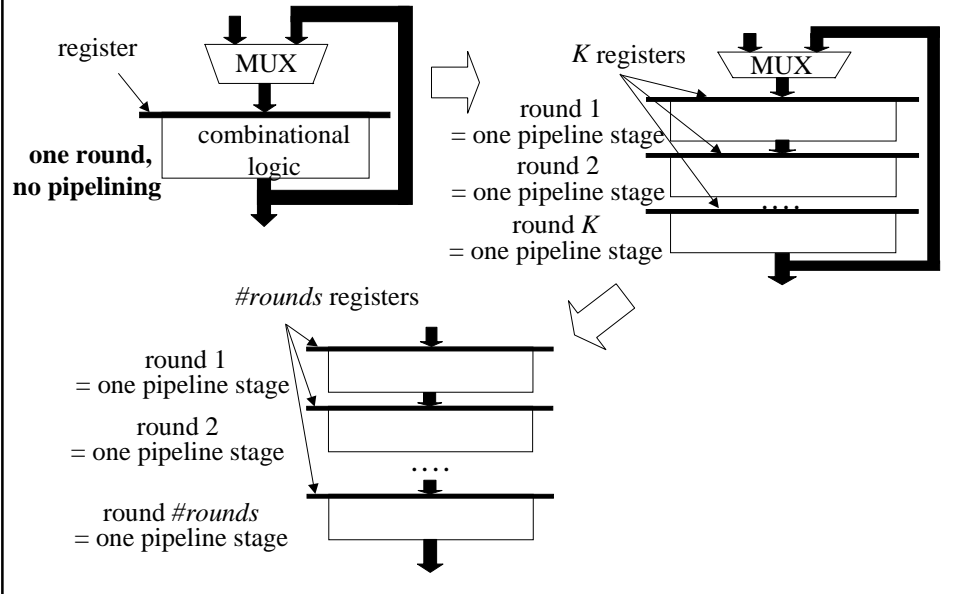


Basic architecture: Timing

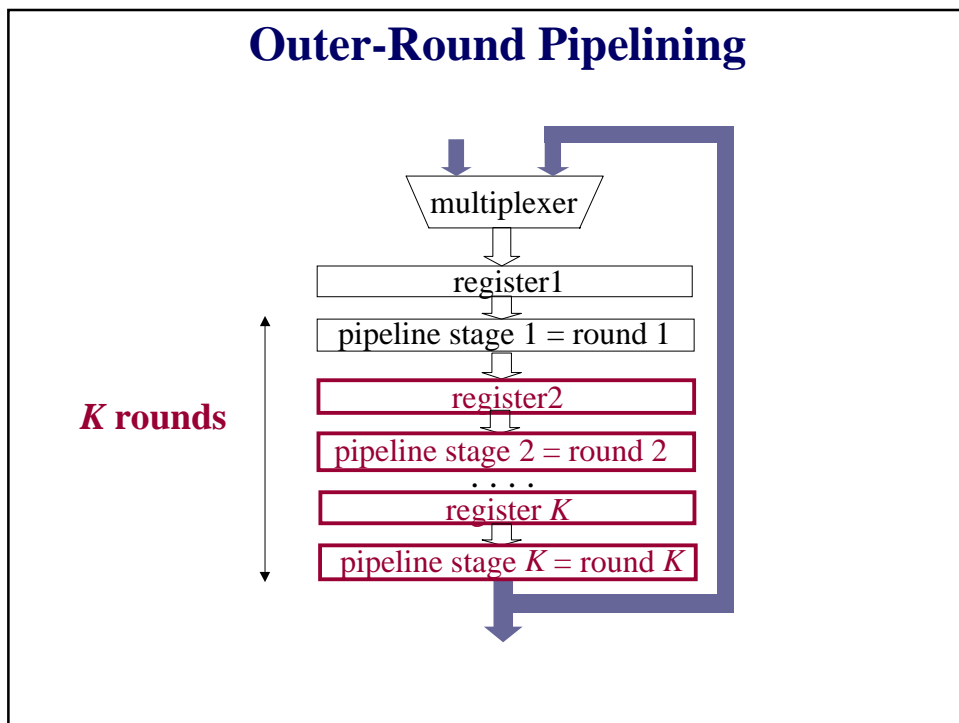




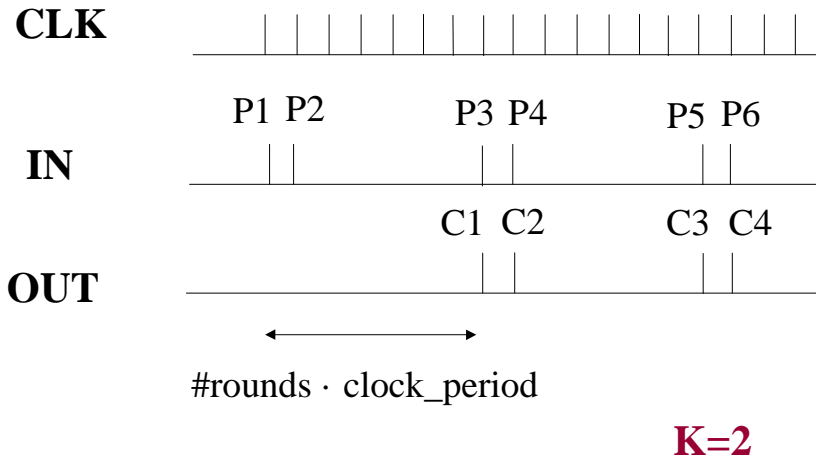
Traditional methodology



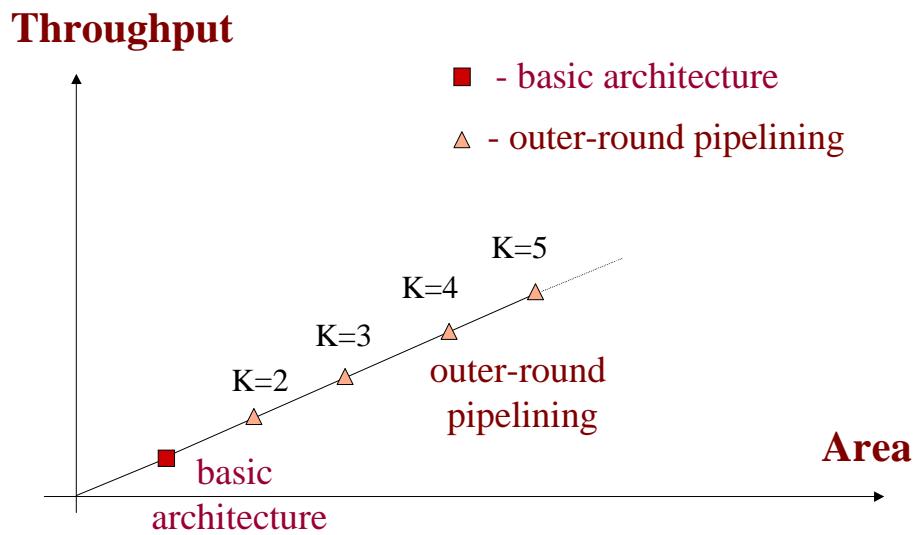
Outer-Round Pipelining



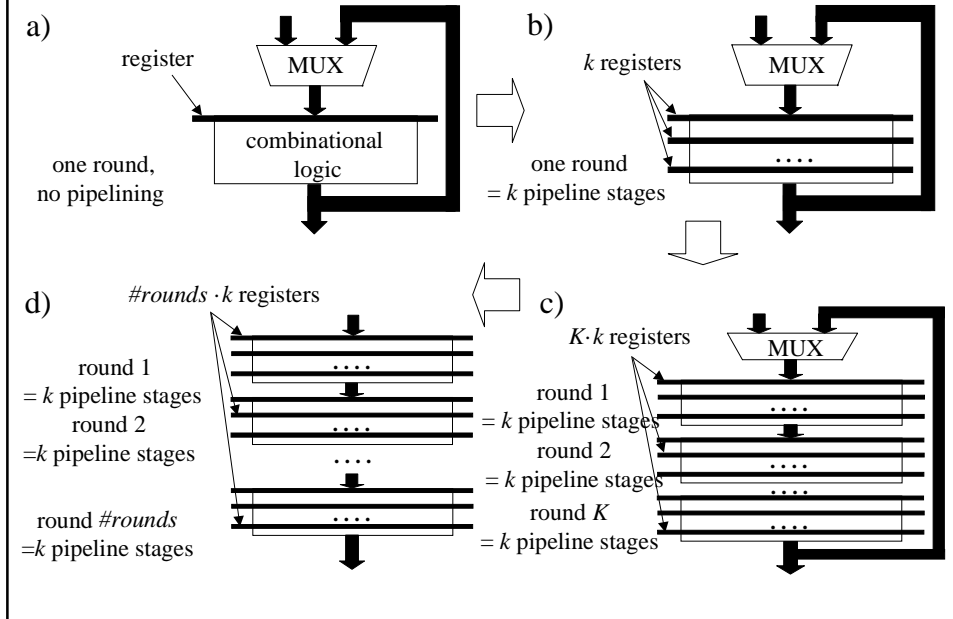
Outer-Round Pipelining: Timing



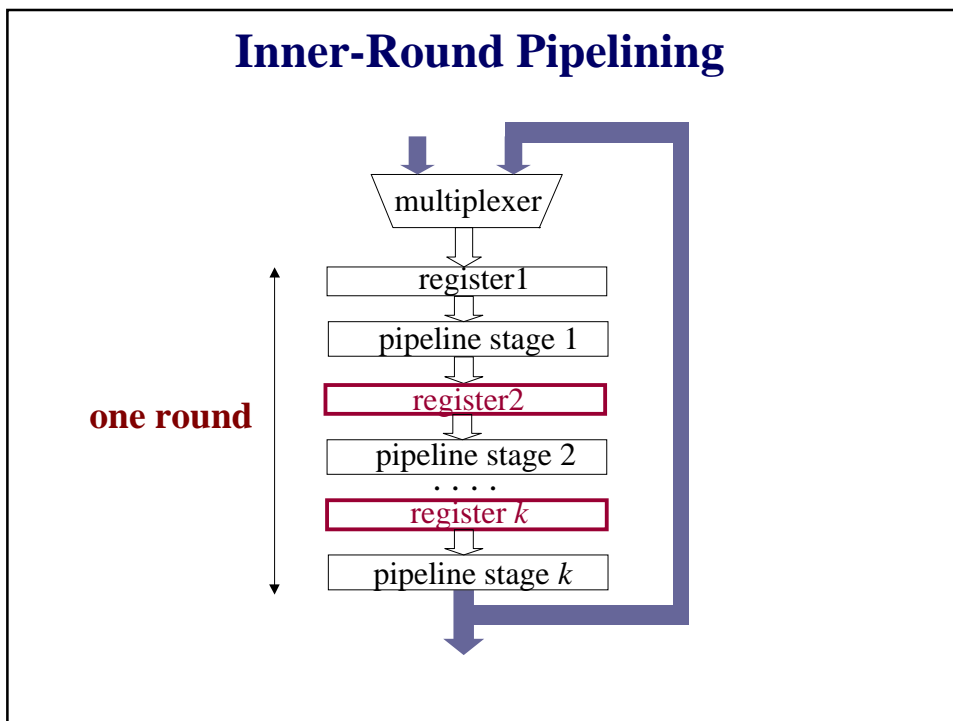
Throughput vs. area dependence for traditional design methodology



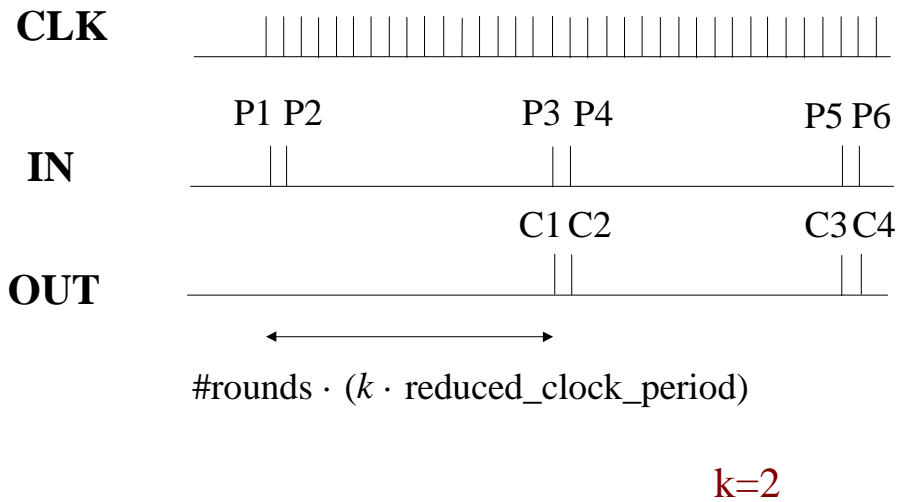
Our methodology



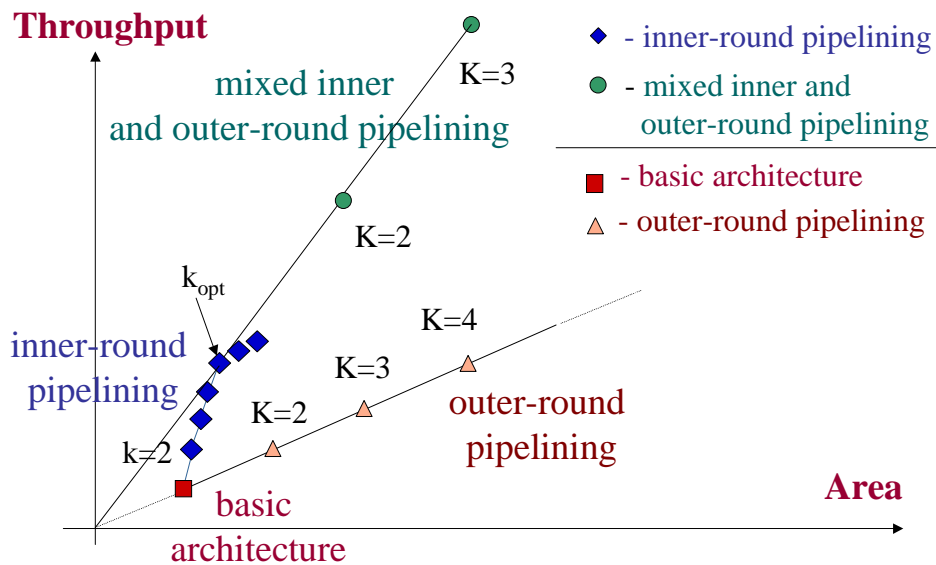
Inner-Round Pipelining



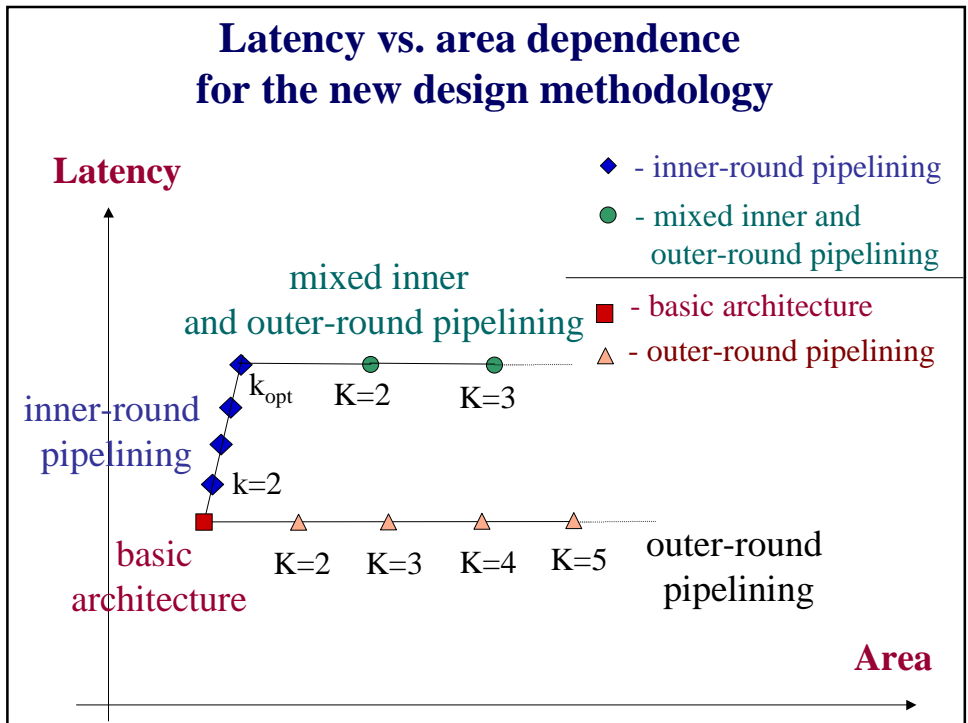
Inner-Round Pipelining: Timing



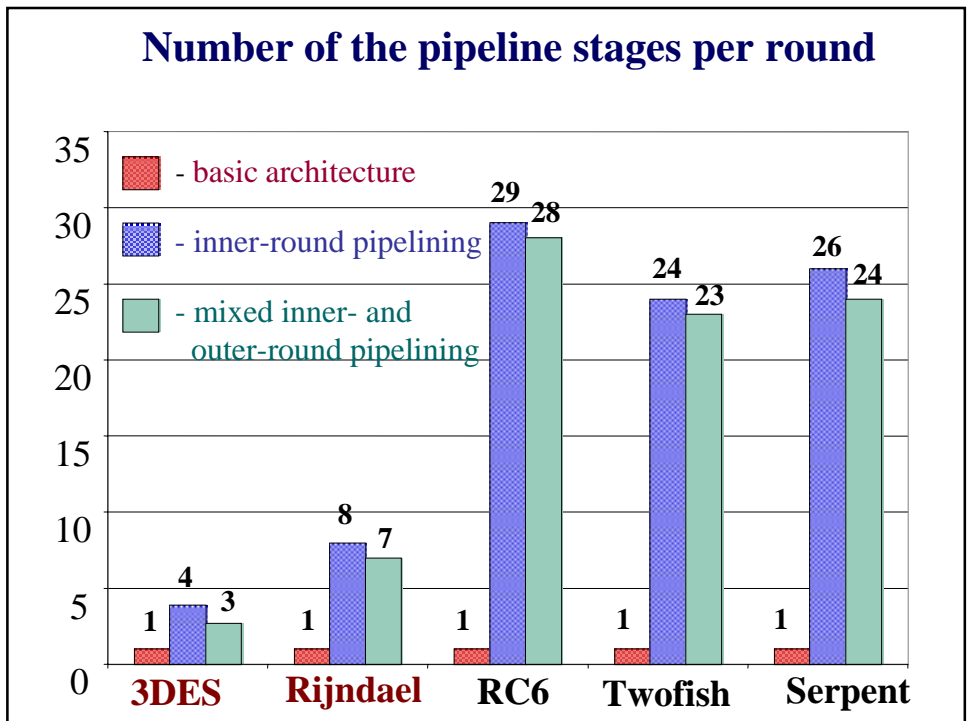
Throughput vs. area dependence for the new design methodology

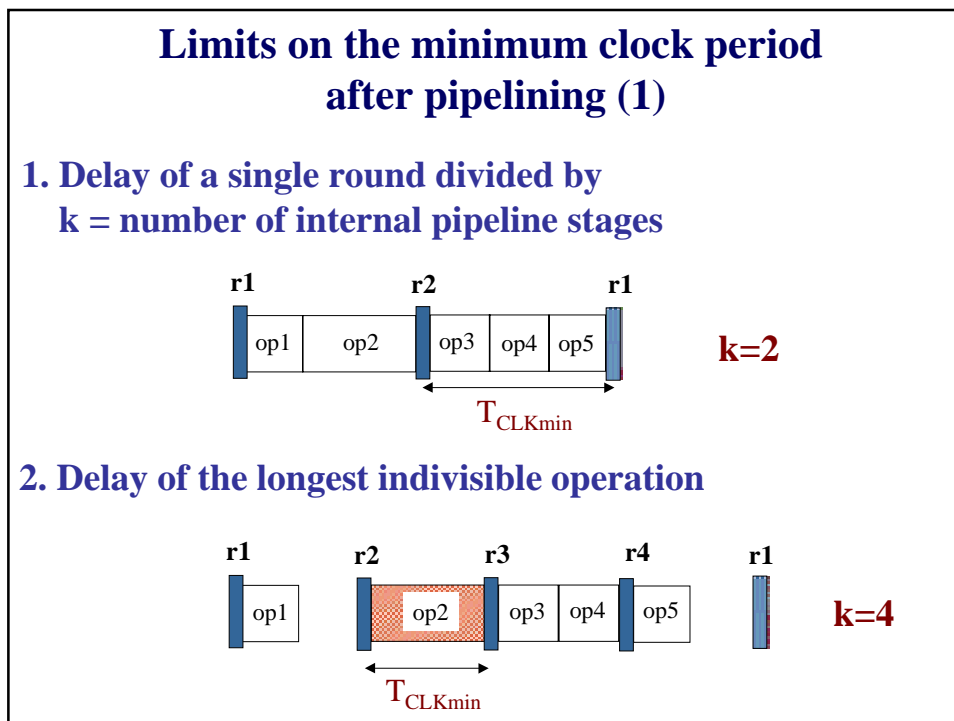
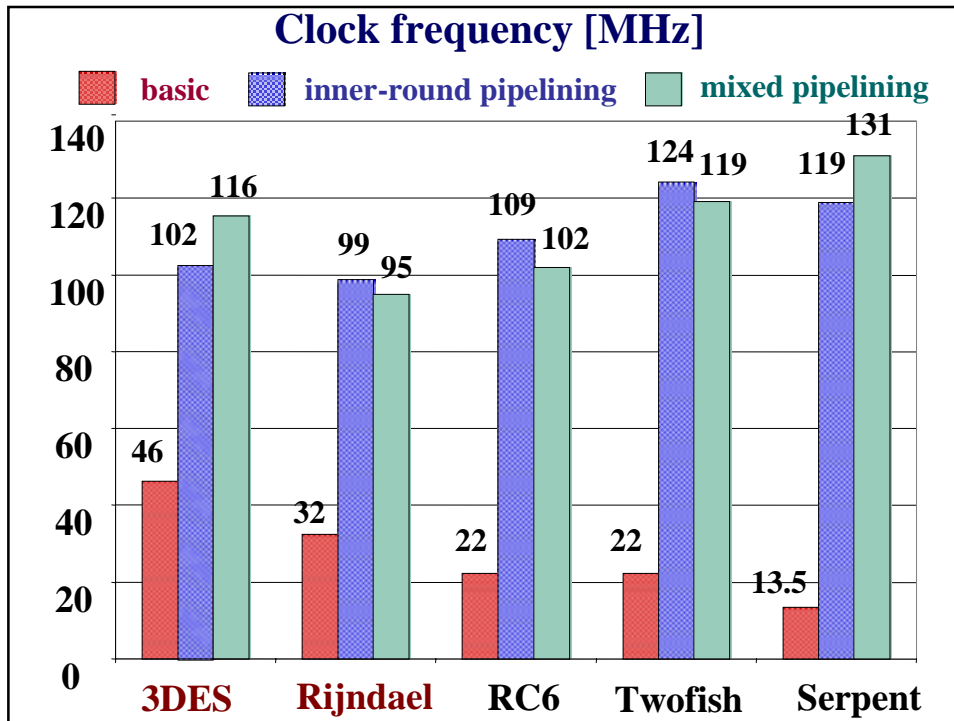


Latency vs. area dependence for the new design methodology



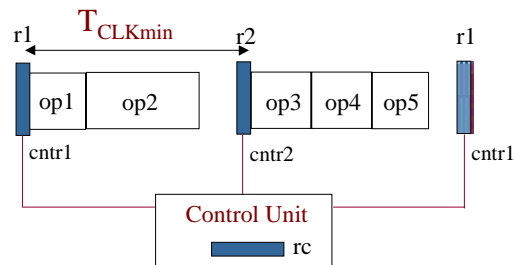
Number of the pipeline stages per round





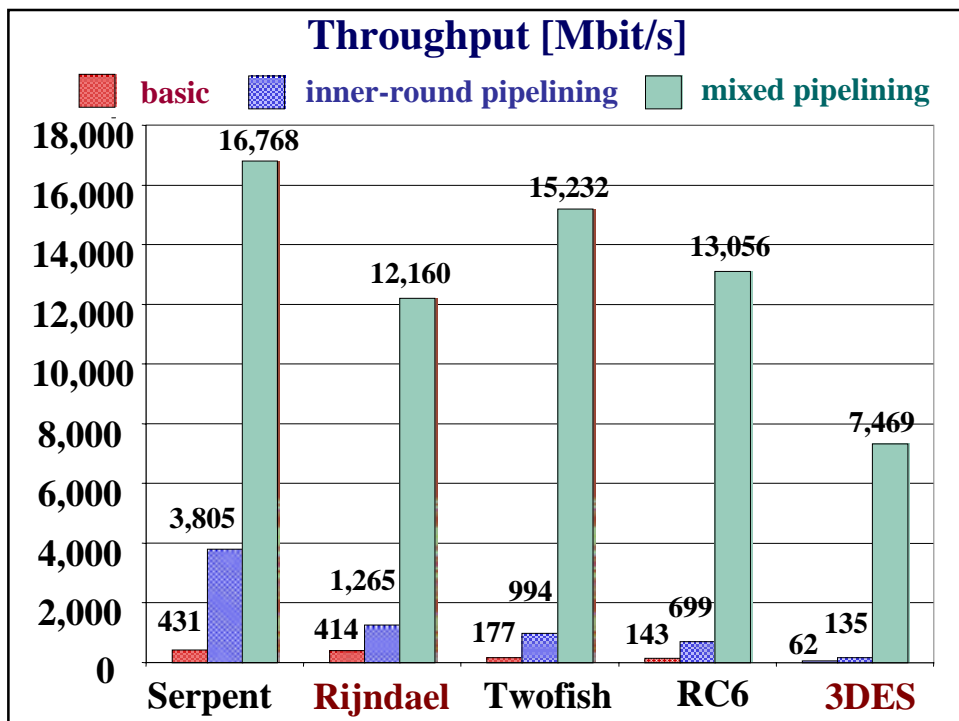
Limits on the minimum clock period after pipelining (2)

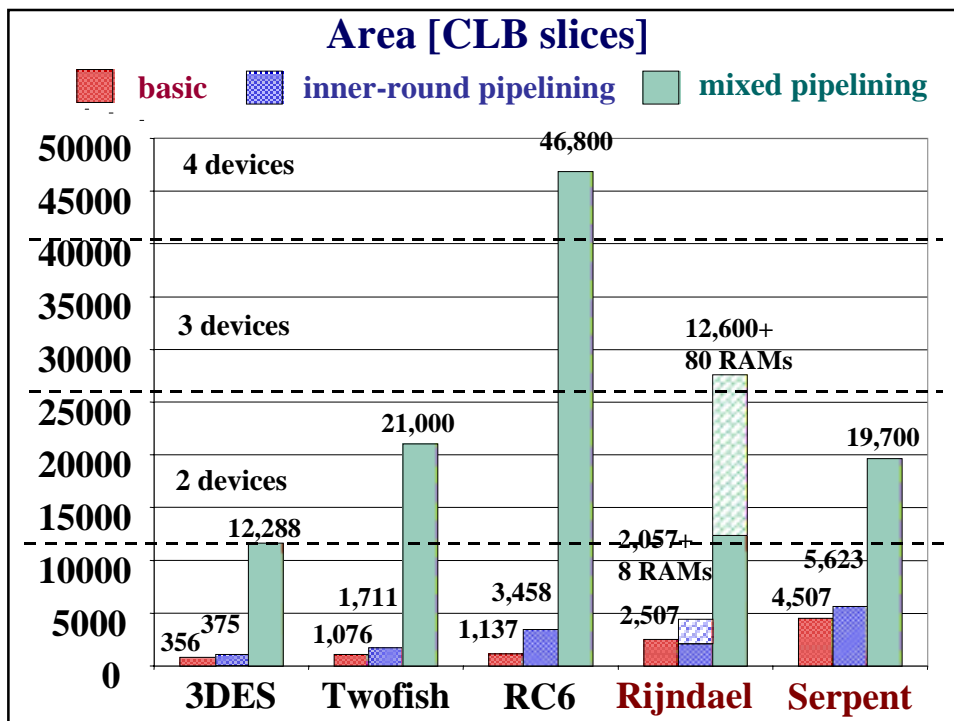
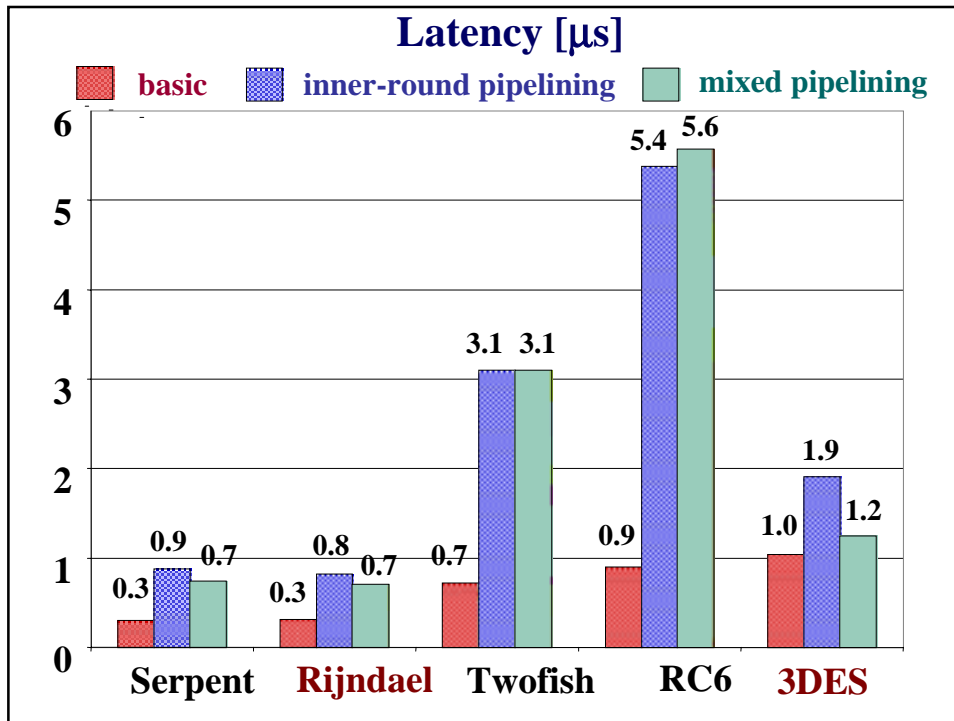
3. Delays within the control unit

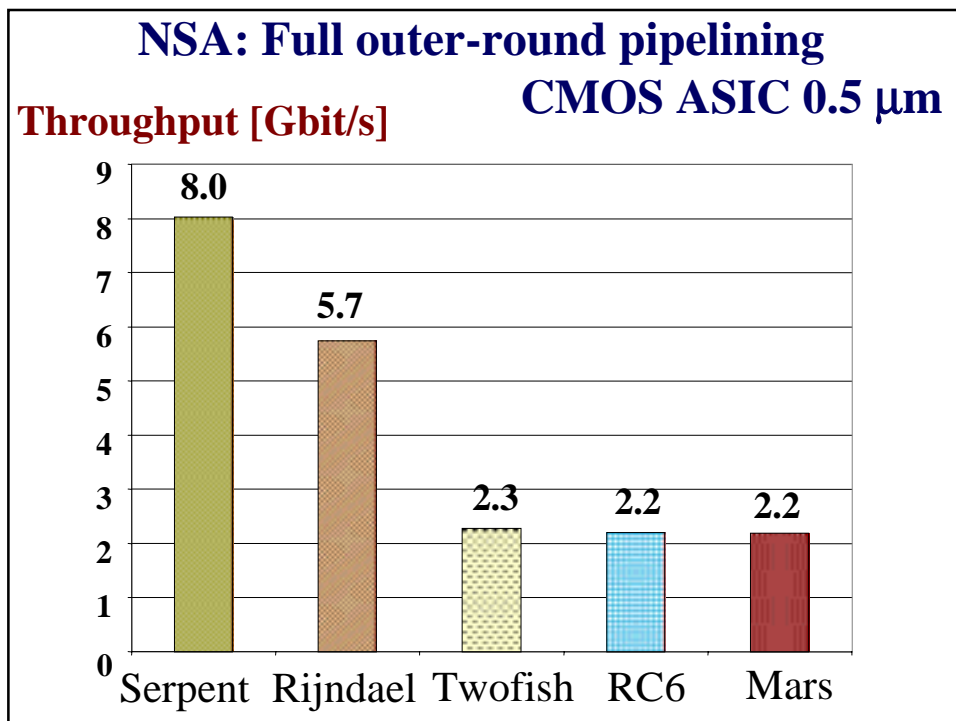
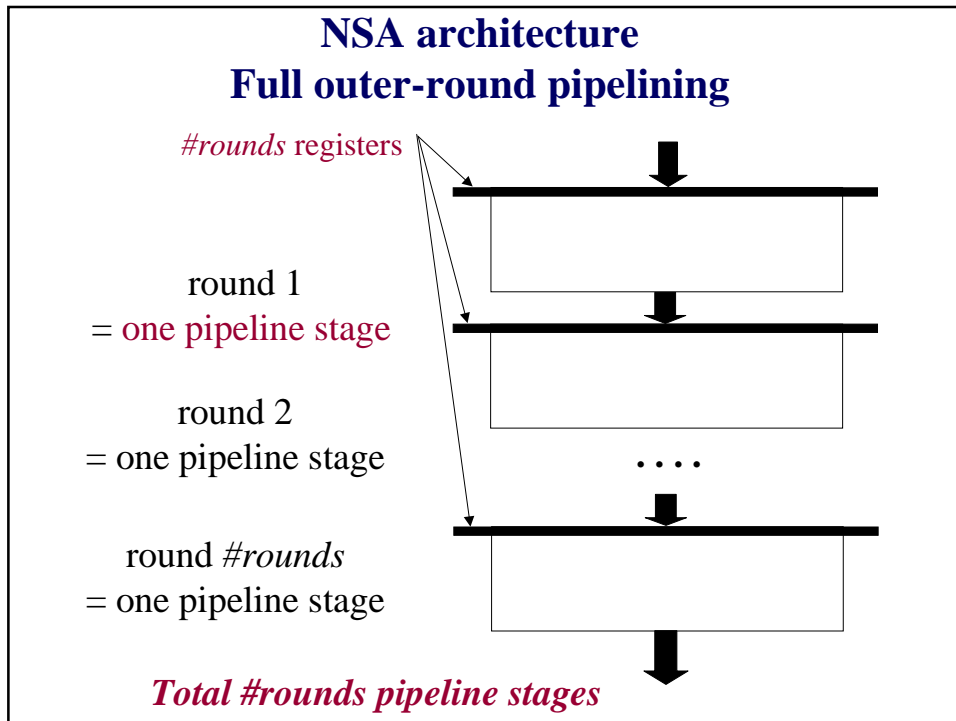


4. Maximum latency

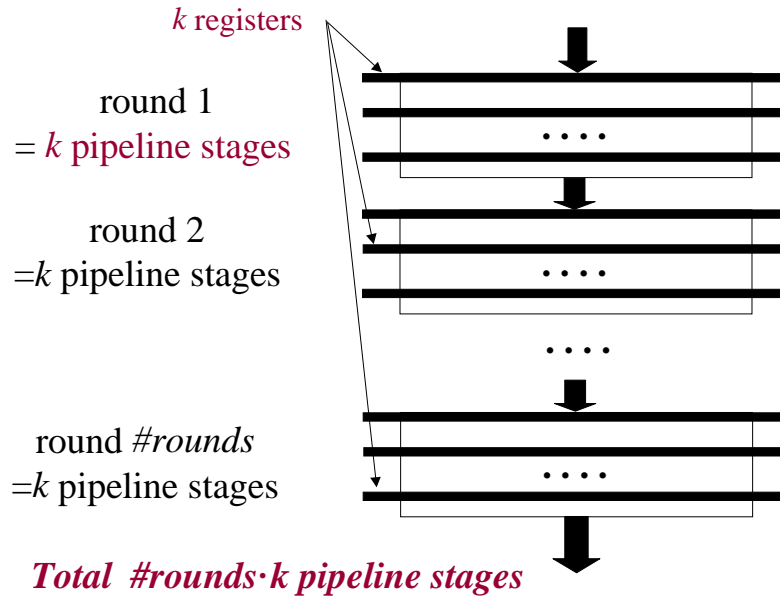
5. Maximum input/output bandwidth





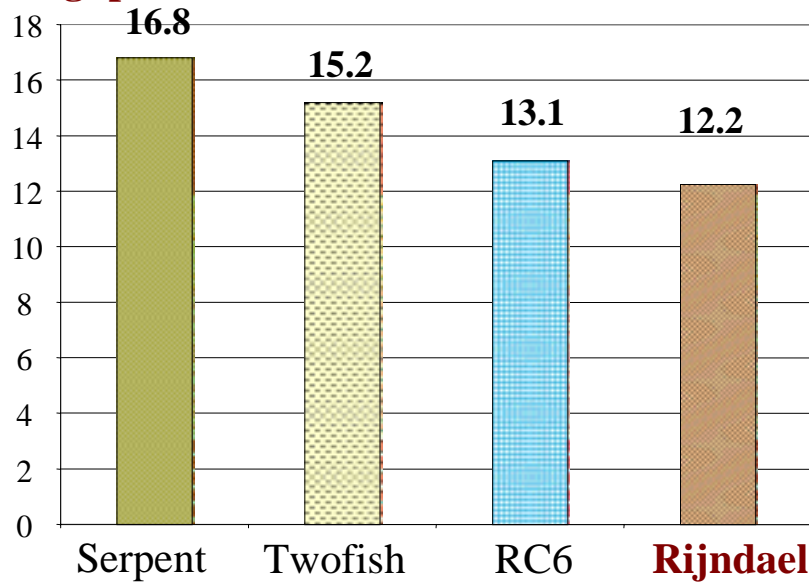


Full mixed inner- and outer-round pipelining

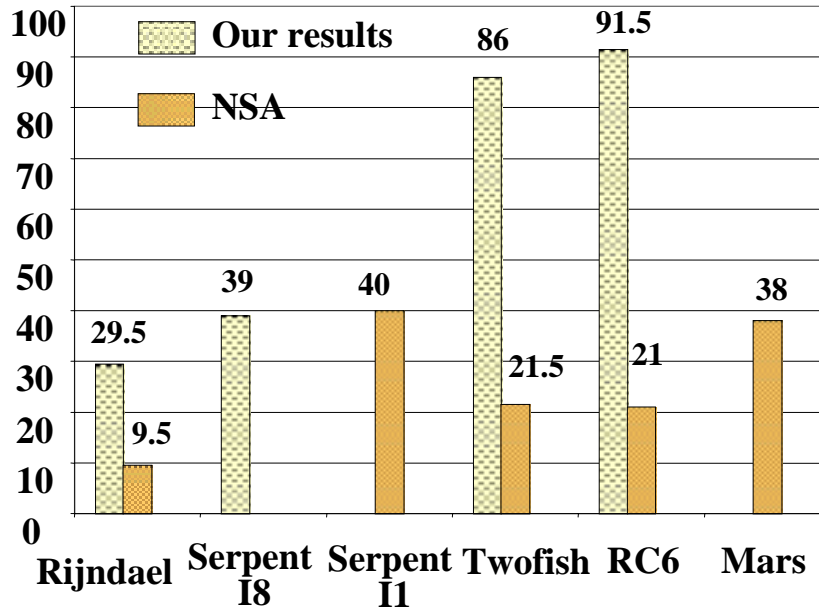


Our results: Full mixed pipelining

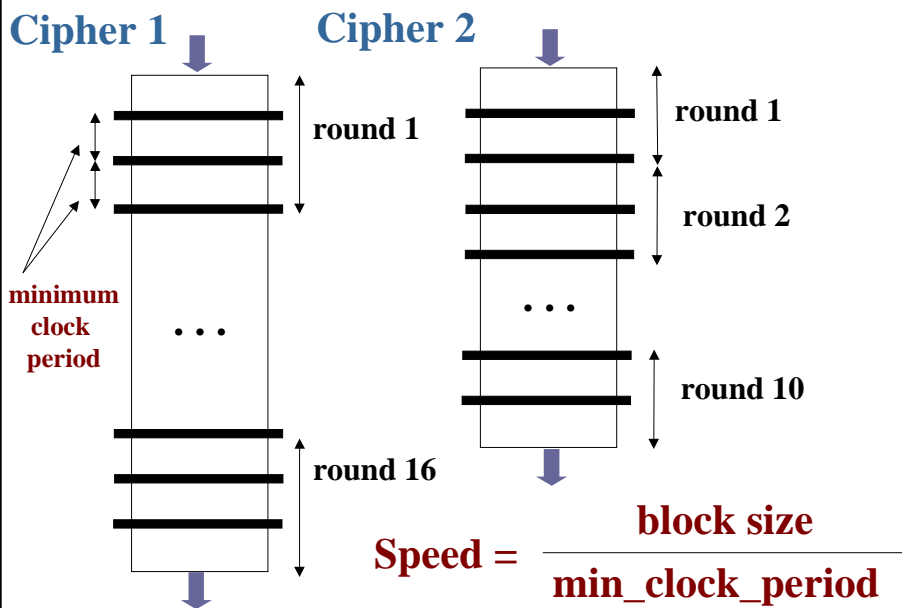
Throughput [Gbit/s] Virtex FPGA, 0.22 μm



Speed-up compared to the basic architecture



Full Mixed Inner and Outer-Round Pipelining



Application of the inner-round pipelining in the secret-key cipher design

April 2000, AES 3, Advanced Encryption Standard Conference

K. Gaj, P. Chodowicz
George Mason University

A.J. Elbirt, W. Yip, B. Chetwynd, C. Paar
Worcester Polytechnic Institute
- small (2-3) and arbitrarily chosen number of pipeline stages

**August 2000, CHES, Cryptographic Hardware and
Embedded Systems Conference**

S. Trimberger, Xilinx, R. Pang, A. Singh, UCSB
12 Gbps DES implementation

Conclusions (1)

**New methodology for high-throughput implementation
of secret-key ciphers proposed and analyzed**

- **optimum number of pipeline stages inside
of a cipher round**
- **very high throughput**
- **ultimate throughput/area ratio**
- **throughput independent of the**
 - **number of cipher rounds**
 - **complexity of a cipher round**

Conclusions (2)

Five modern secret-key ciphers, including two new federal standards, AES and Triple DES implemented

Throughputs

**from 12.2 to 16.8 Gbit/s for AES candidates
(128-bit i/o block)**
**7.5 Gbit/s for Triple DES
(64-bit i/o block)**

**Fastest reported designs of the AES candidates
in any technology**