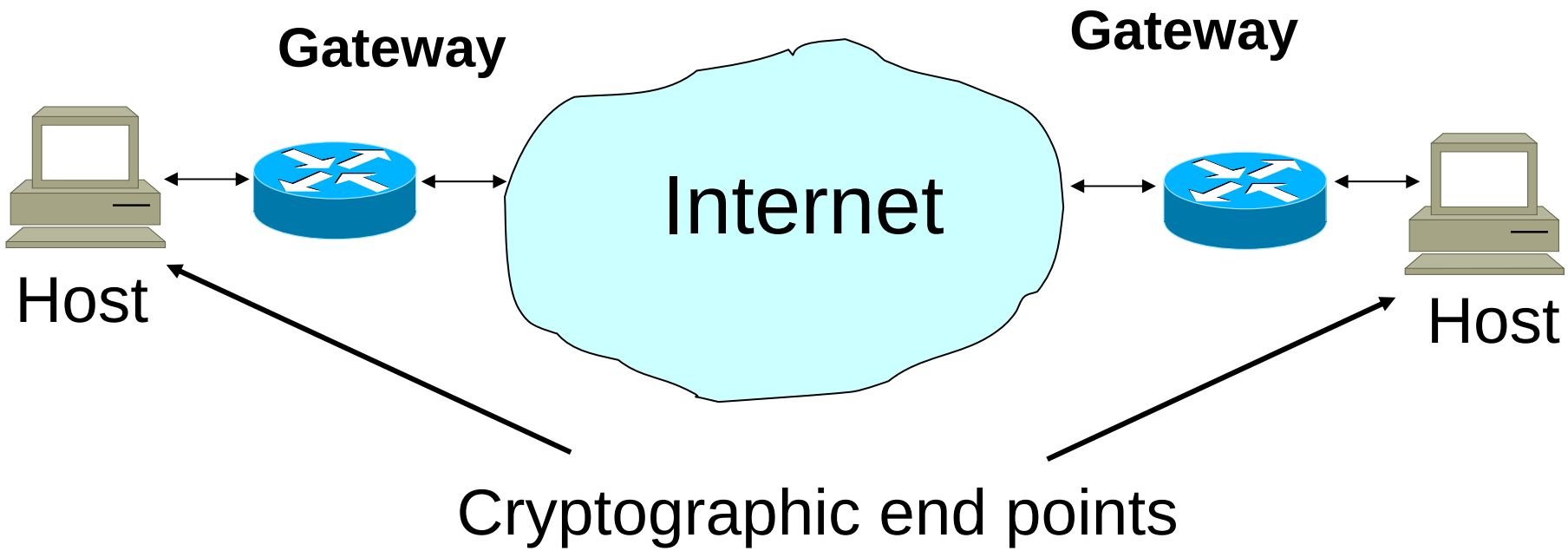
Paweł Chodowiec & Kris Gaj
George Mason University

Peter Bellows & Brian Schott
USC - Information Sciences Institute

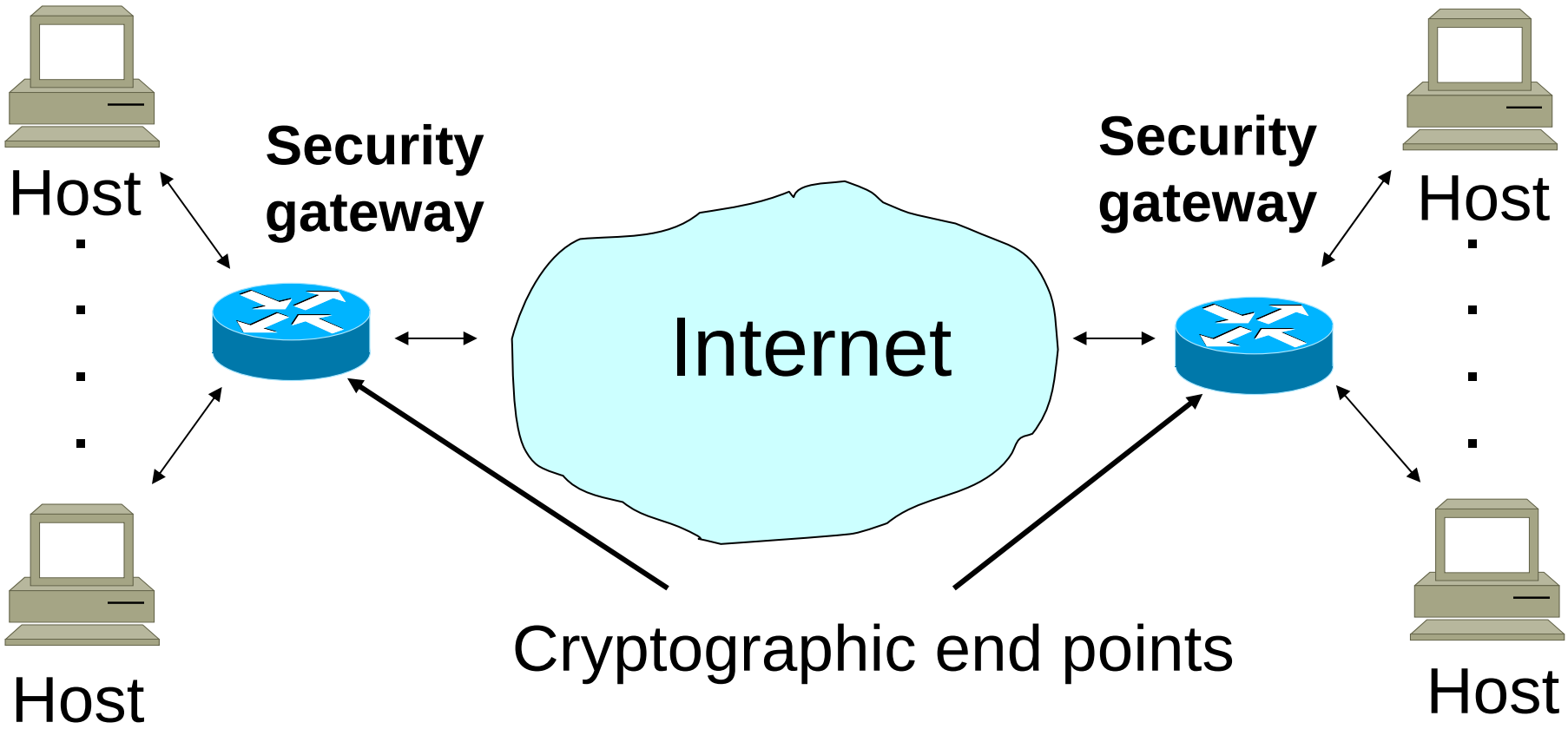
Experimental Testing of the Gigabit IPSec-Compliant Implementations of Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board

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

IPSec: Transport Mode



IPSec: Tunnel Mode

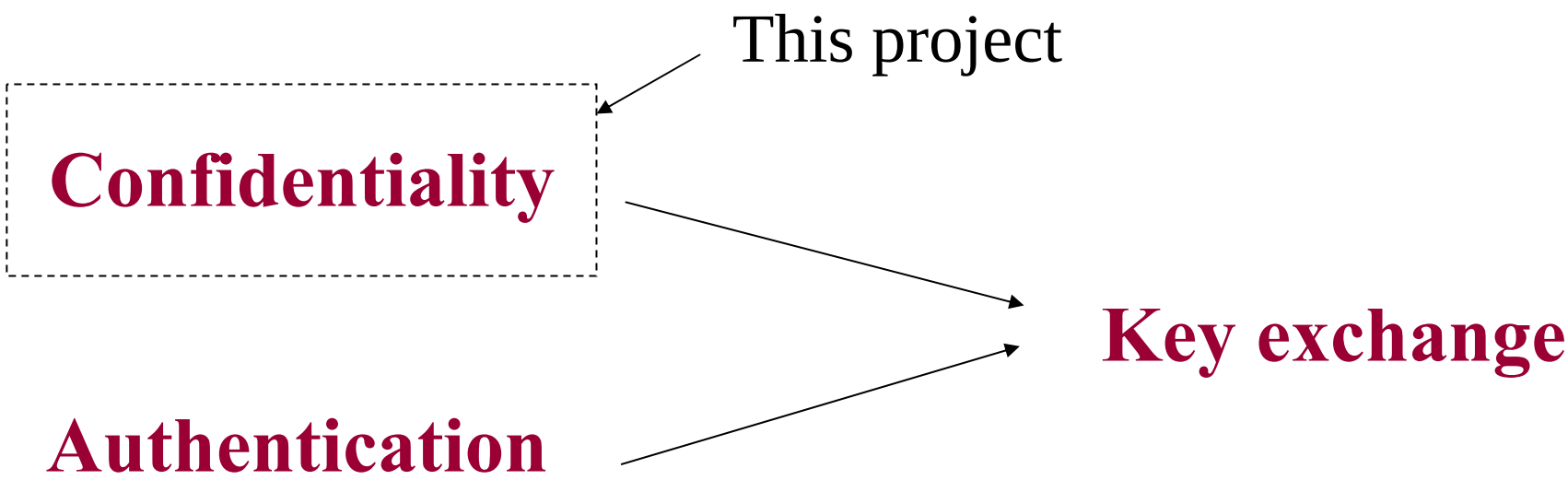


IPSec: Need for hardware accelerators

- large amount of secure associations processed by a single device
- cryptographic operations computationally expensive compared with regular IP operations

Cryptographic transformations in IPSec

Security Services



IPSec: Cryptographic algorithms Confidentiality (1)

Required:

Algorithm	Key length
DES	**56 bits**

Document: RFC 2405

Optional:

Document: RFC 2451

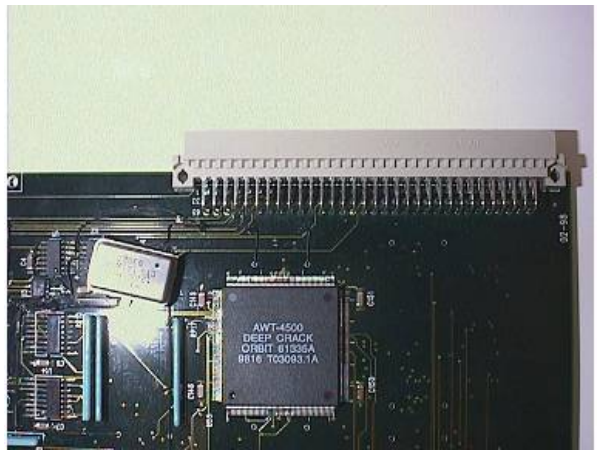
Algorithm	Key length [bits]	Popular sizes	Default size
Triple DES	168	168	168
Blowfish	40..448	128	128
CAST-128	40..128	40, 64, 80, 128	128
IDEA	128	128	128
RC5	40..2040	40, 64, 80, 128	128

Breaking DES: Deep Crack

Electronic Frontier Foundation, 1998

Total cost: $220,000

Average time of search:
4.5 days/key

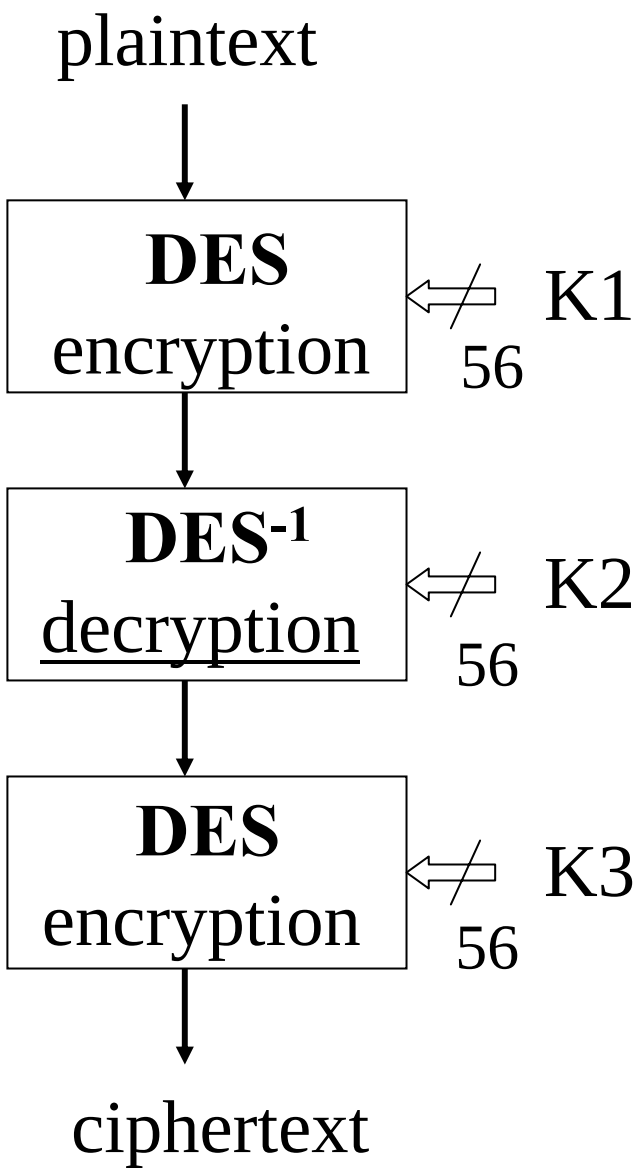


1800 ASIC chips, 40 MHz clock

Triple DES

Diffie, Hellman, 1977

EDE mode



K = (K1, K2, K3)

168 bits of the key

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

IPSec: Cryptographic algorithms Confidentiality (2)

Proposed:

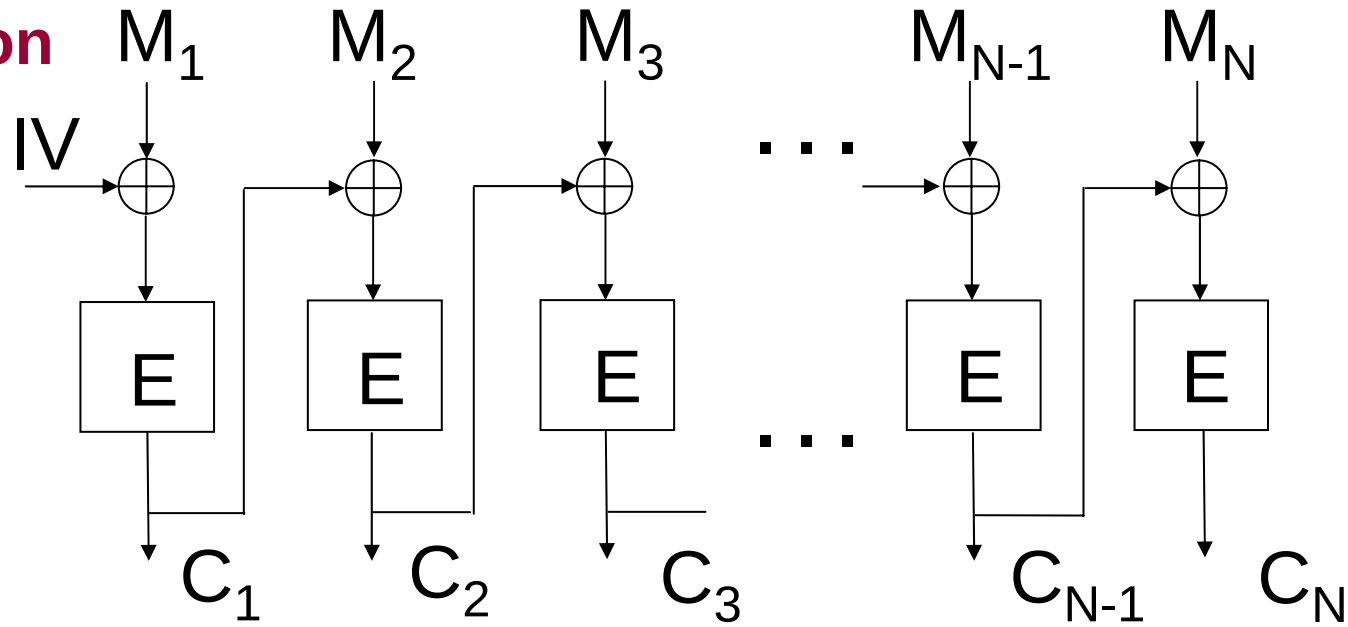
Document: Internet Draft, November 2000,

Algorithm	Key length [bits]	Popular sizes	Default size
AES (Rijndael)	128, 192, 256	128, 192, 256	128
MARS	128..448	128, 192, 256	128
RC6	≤ 2040	128, 192, 256	128
Serpent	≤ 256	128, 192, 256	128
Twofish	≤ 256	128, 192, 256	128

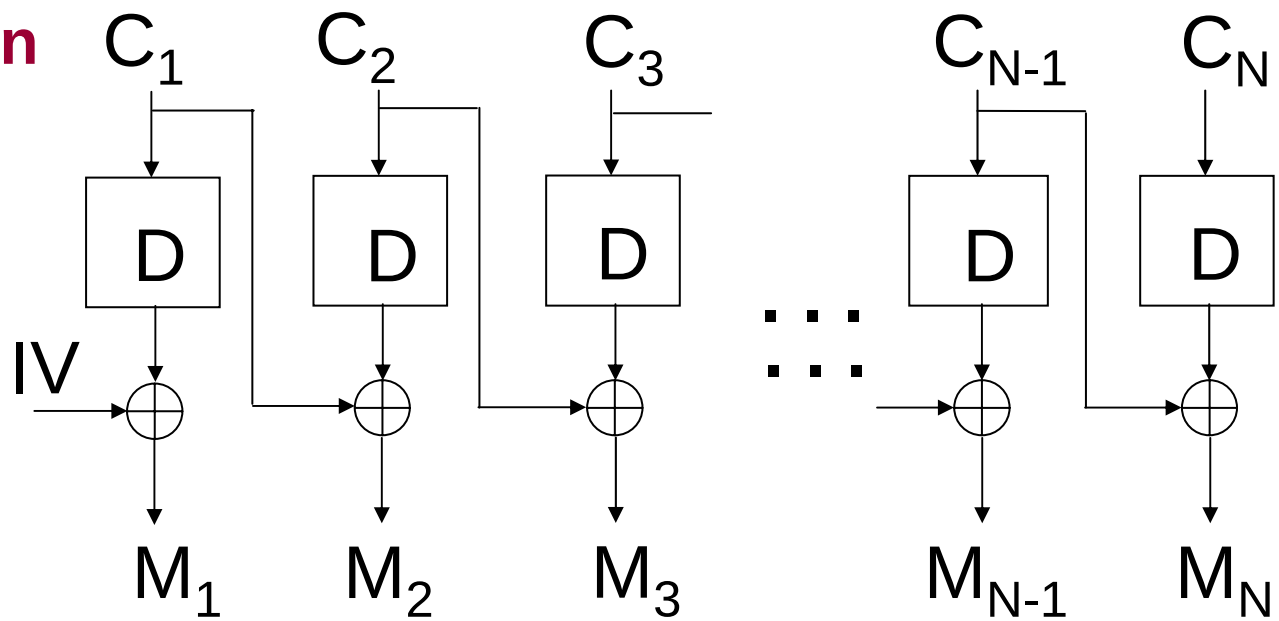
Modes of operation: CBC

RFC 2405

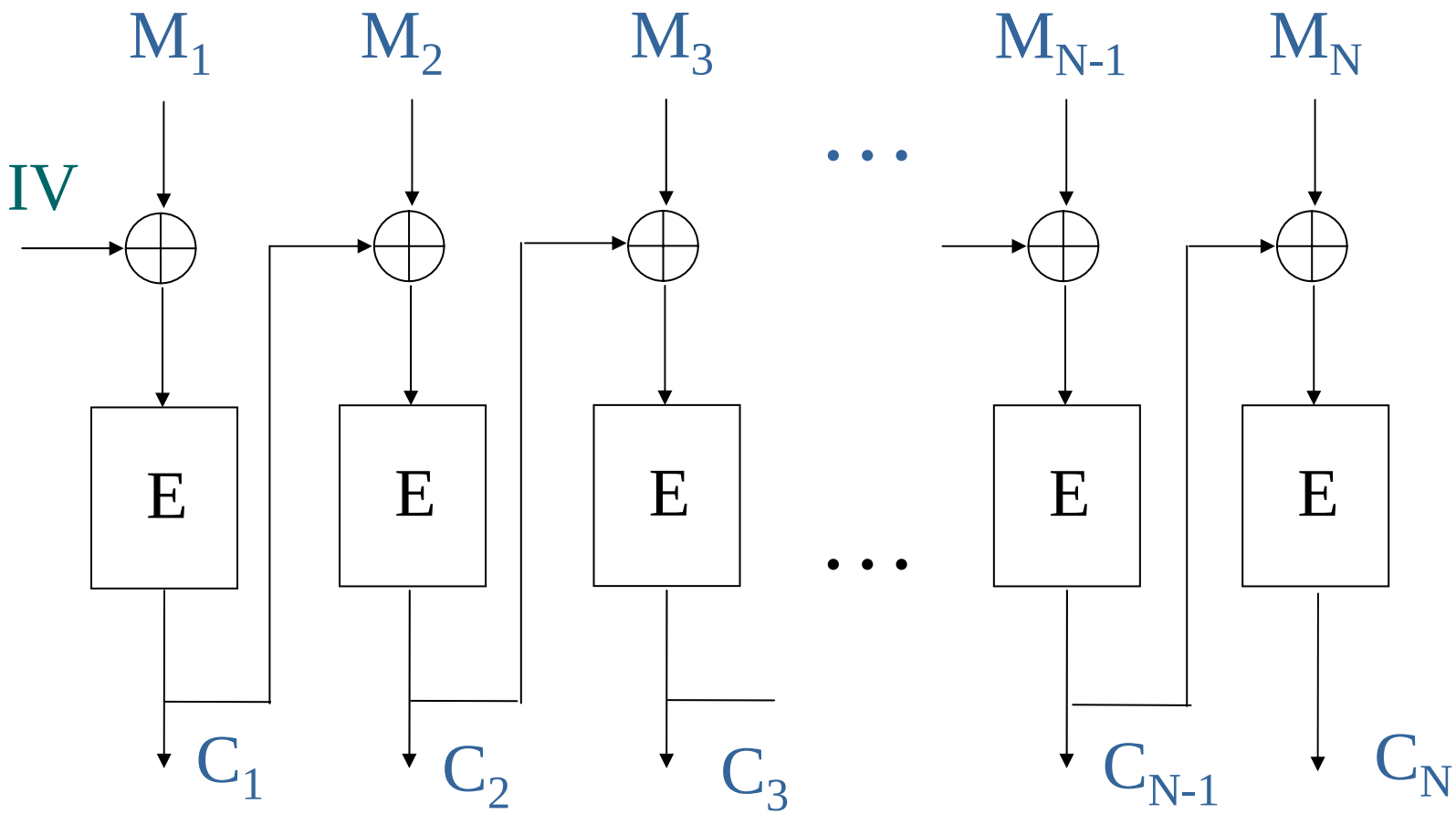
Encryption



Decryption



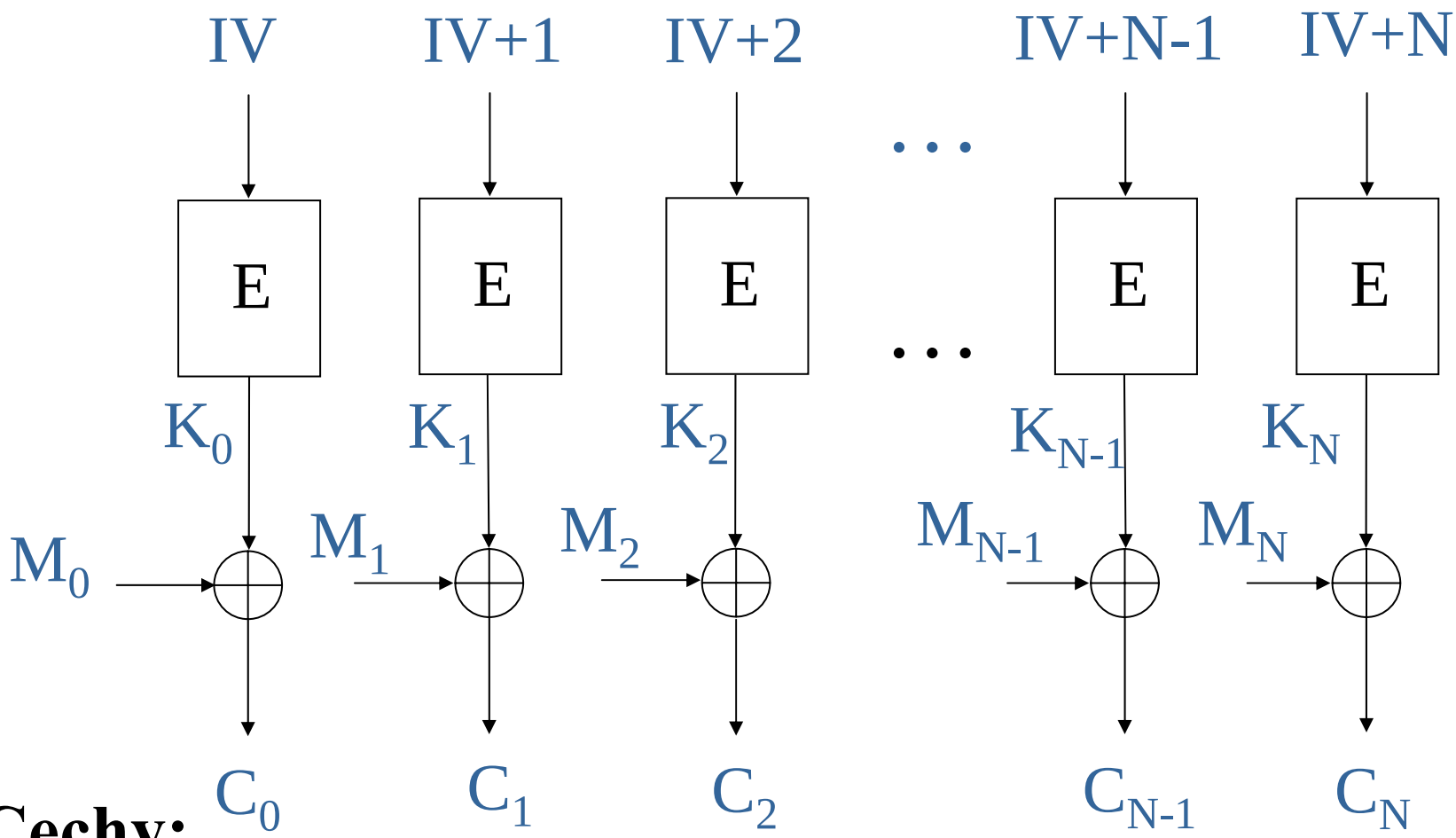
Modes of operation: Current standard - CBC



Problems:

- **No parallel processing of blocks from the same packet**
- **No speed-up by preprocessing**
- **No integrity or authentication**

Counter mode



Cechy:

+ Potential for parallel processing

+ Speed-up by preprocessing

- No integrity or authentication

Operating Modes Contest

4 Old Modes
(CBC, CFB, OFB, ECB)

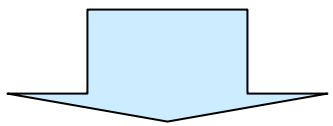
April 2001

---

10 New Candidates
from Egypt, Estonia, Norway,
Sweden, Thailand, USA

Counter mode

Summer 2001



5 Standard Modes

2002

New Standard Modes

IPSec: Why reconfigurable hardware?

Frequently changing algorithms and their parameters

- AES
- new modes of operation
- new hash functions
- parameters of public key cryptosystems

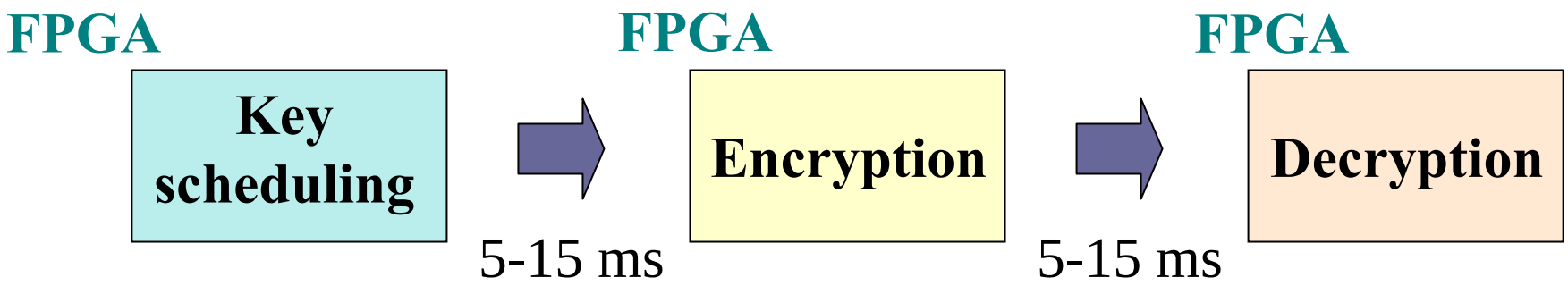
Capability for reconfiguration =

- algorithm agility
- scalable security
- flexible architecture
- remote error correction

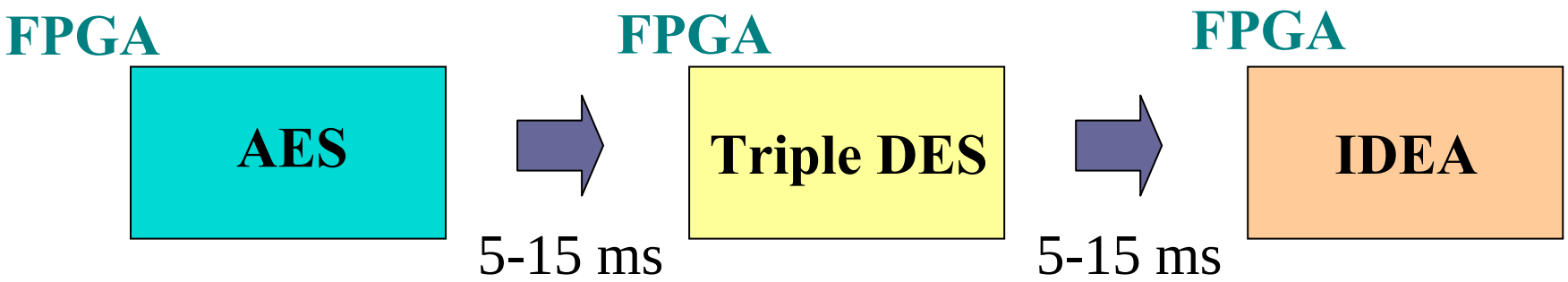
Reconfigurability

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

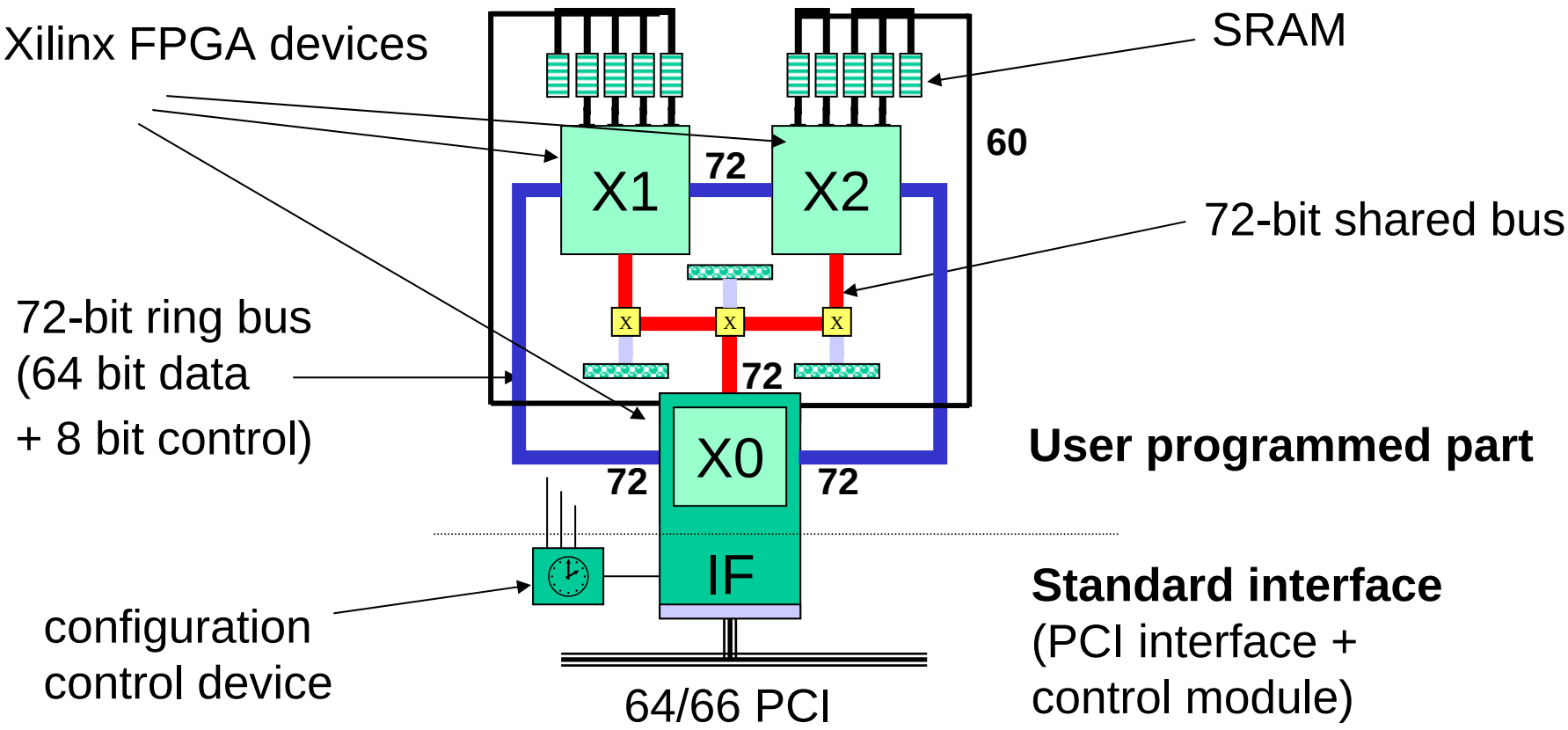
Encryption vs. decryption vs. key scheduling



Various algorithms

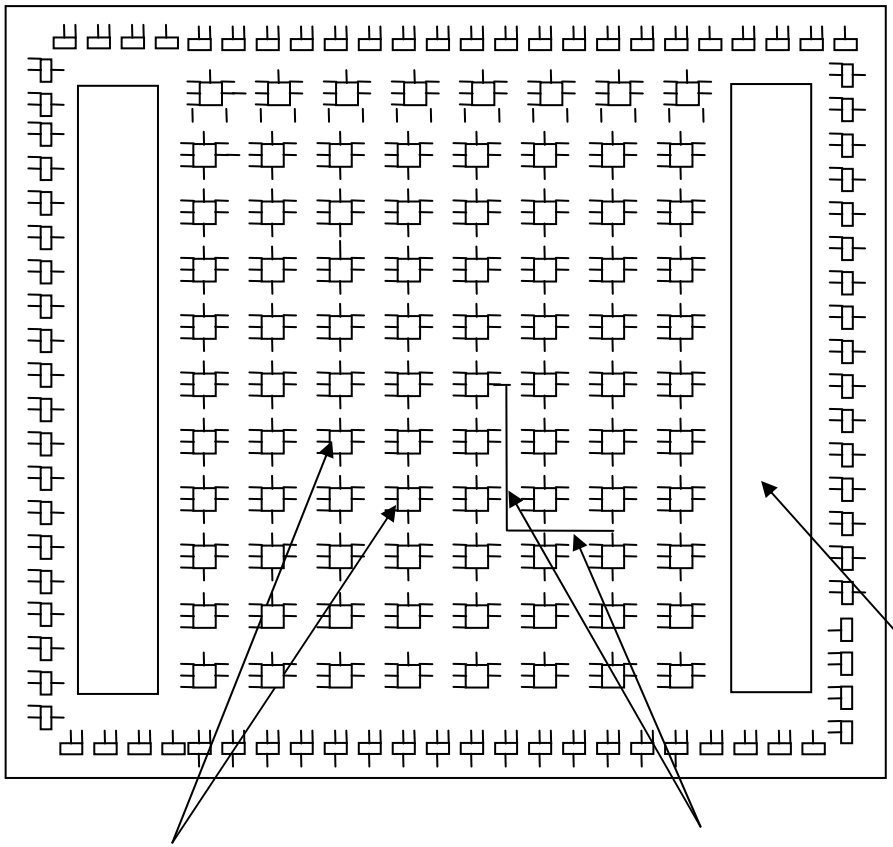


SLAAC-1V


Xilinx FPGA devices
SRAM
60
X1
72
X2
72-bit shared bus
72-bit ring bus
(64 bit data
+ 8 bit control)
X
X
X
72
X0
72
72
User programmed part
IF
configuration
control device
64/66 PCI
Standard interface
(PCI interface +
control module)

Target FPGA devices

Xilinx Virtex - XCV 1000



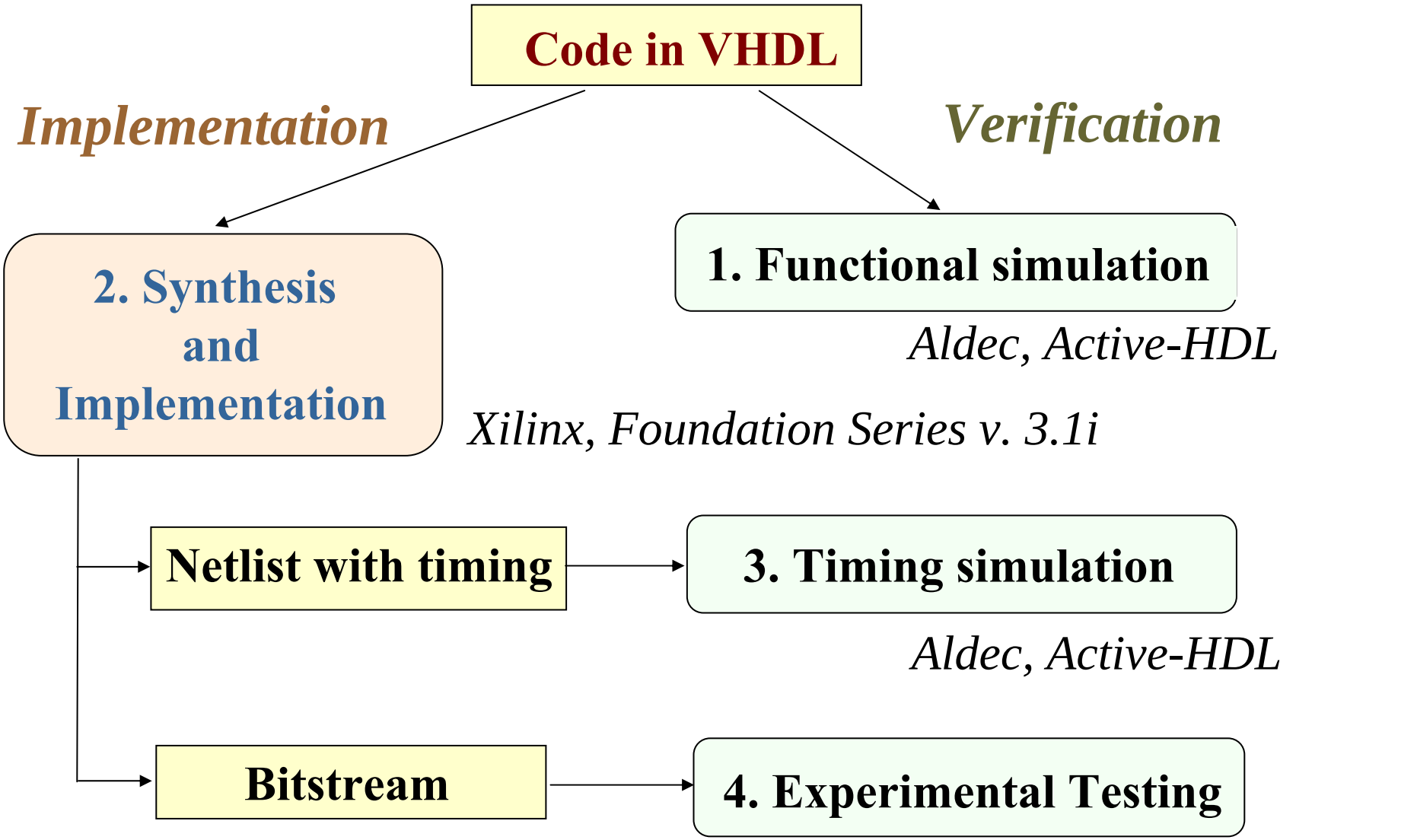
- 0.22 μm CMOS process
- 12 288 CLB slices
- 10 4-kbit block RAMs
- 1 mln equivalent logic gates
- Up to 200 MHz clock

Block RAMs

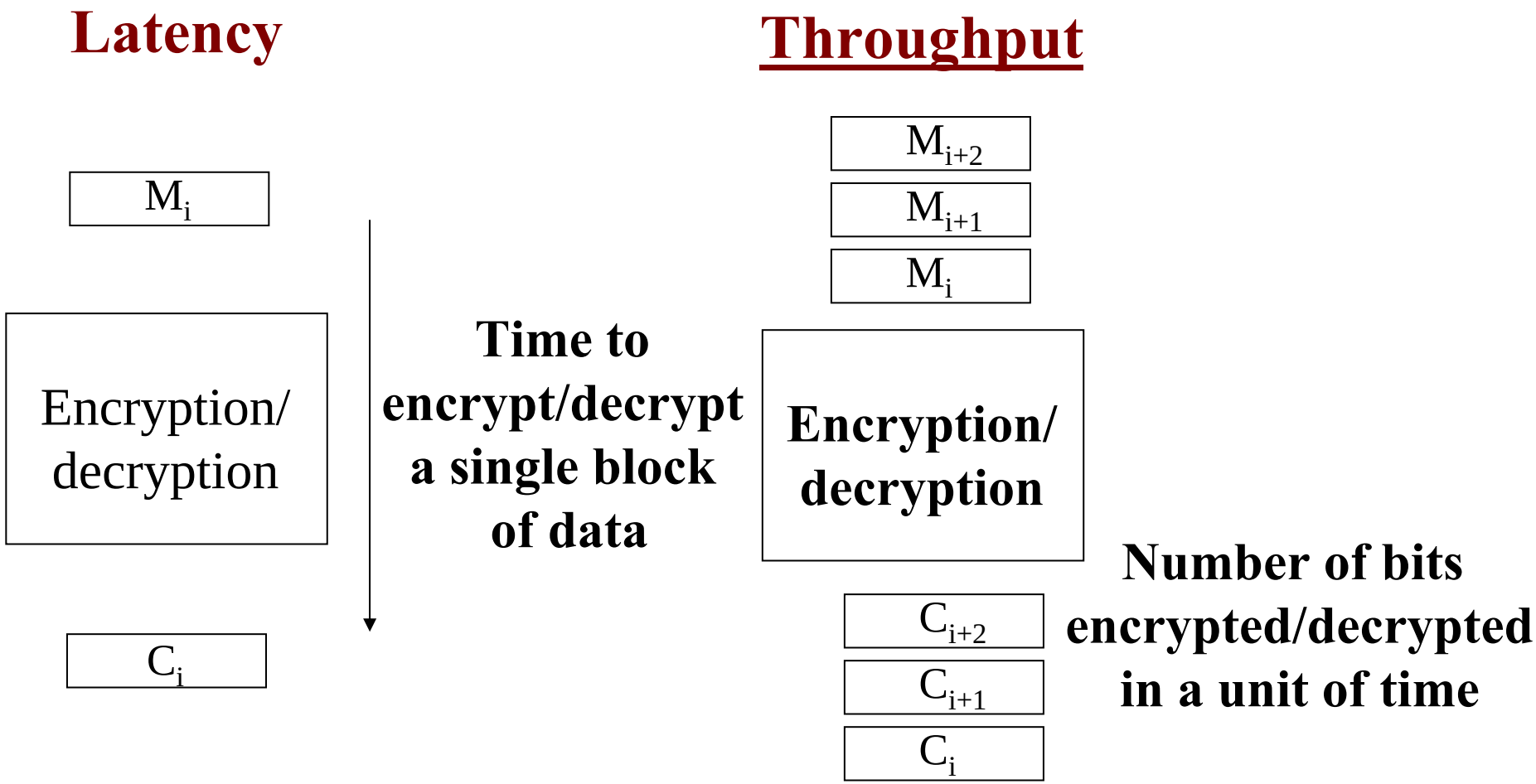
Configurable Logic Block slices (CLB slices)

Programmable Interconnects

Methodology and Tools

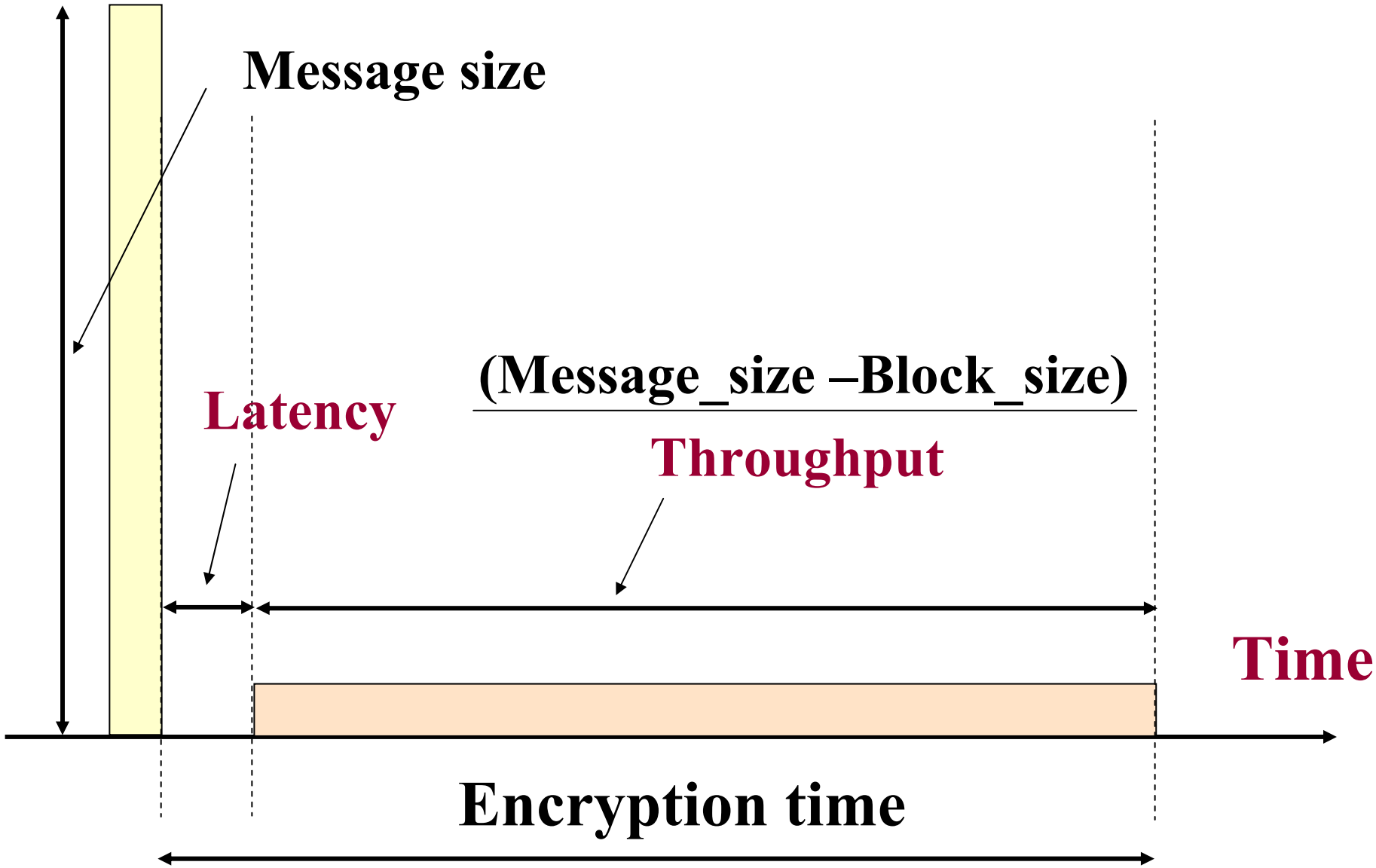


Primary parameters of hardware implementations for secret-key block ciphers

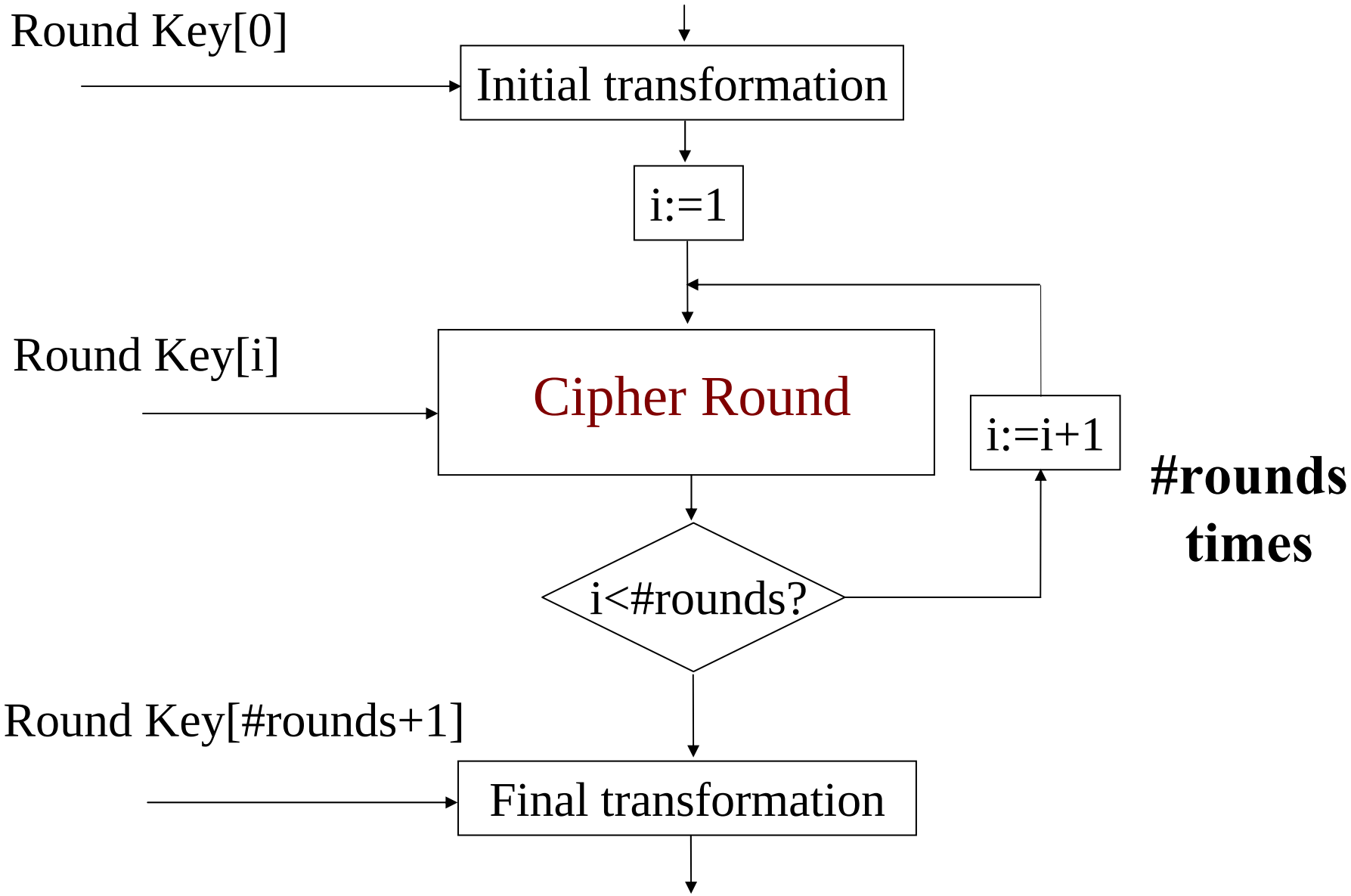


$$\text{Throughput} = \frac{\text{Block\_size} \cdot \text{Number\_of\_blocks\_processed\_simultaneously}}{\text{Latency}}$$

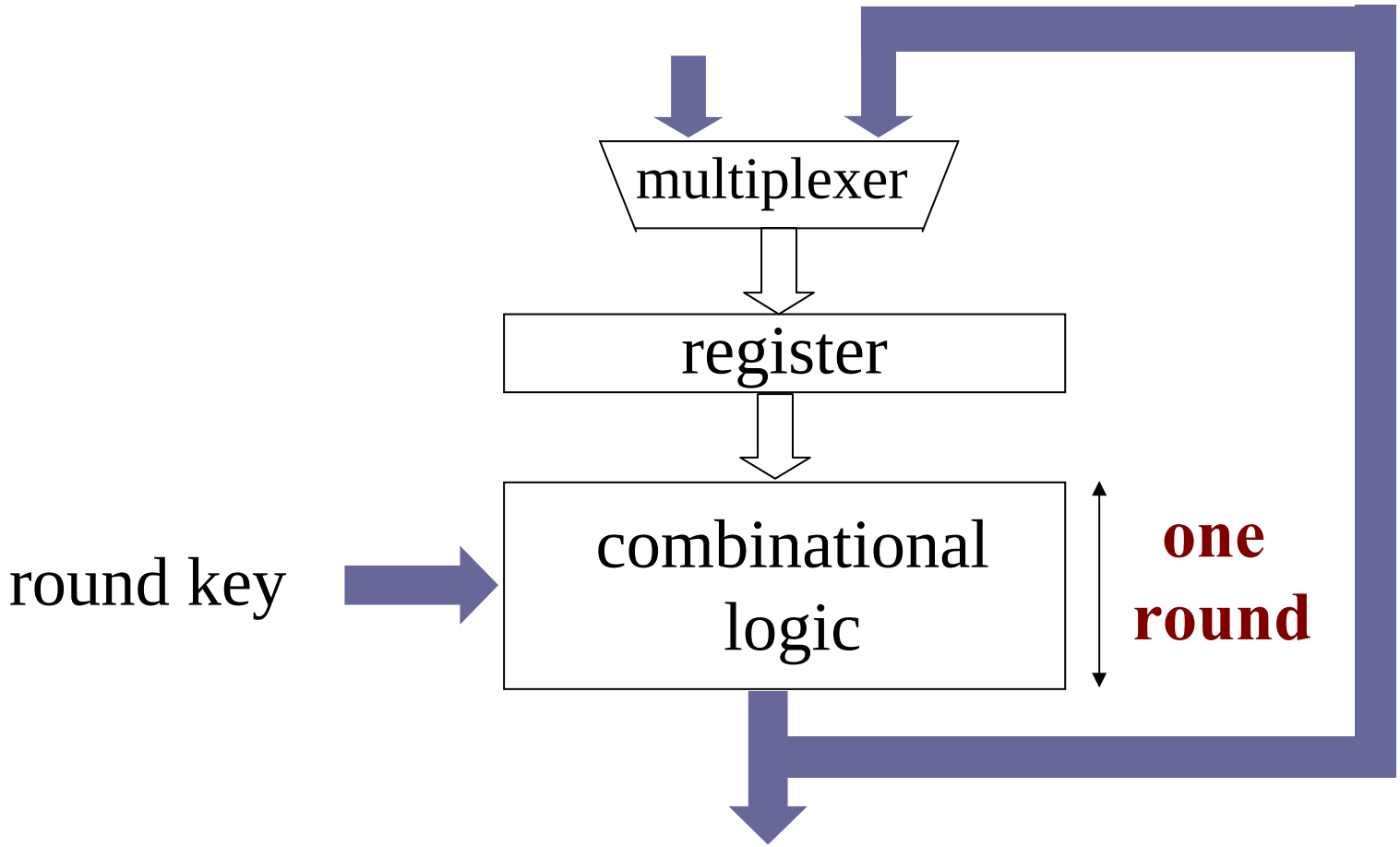
Dependence of the encryption time on latency and throughput



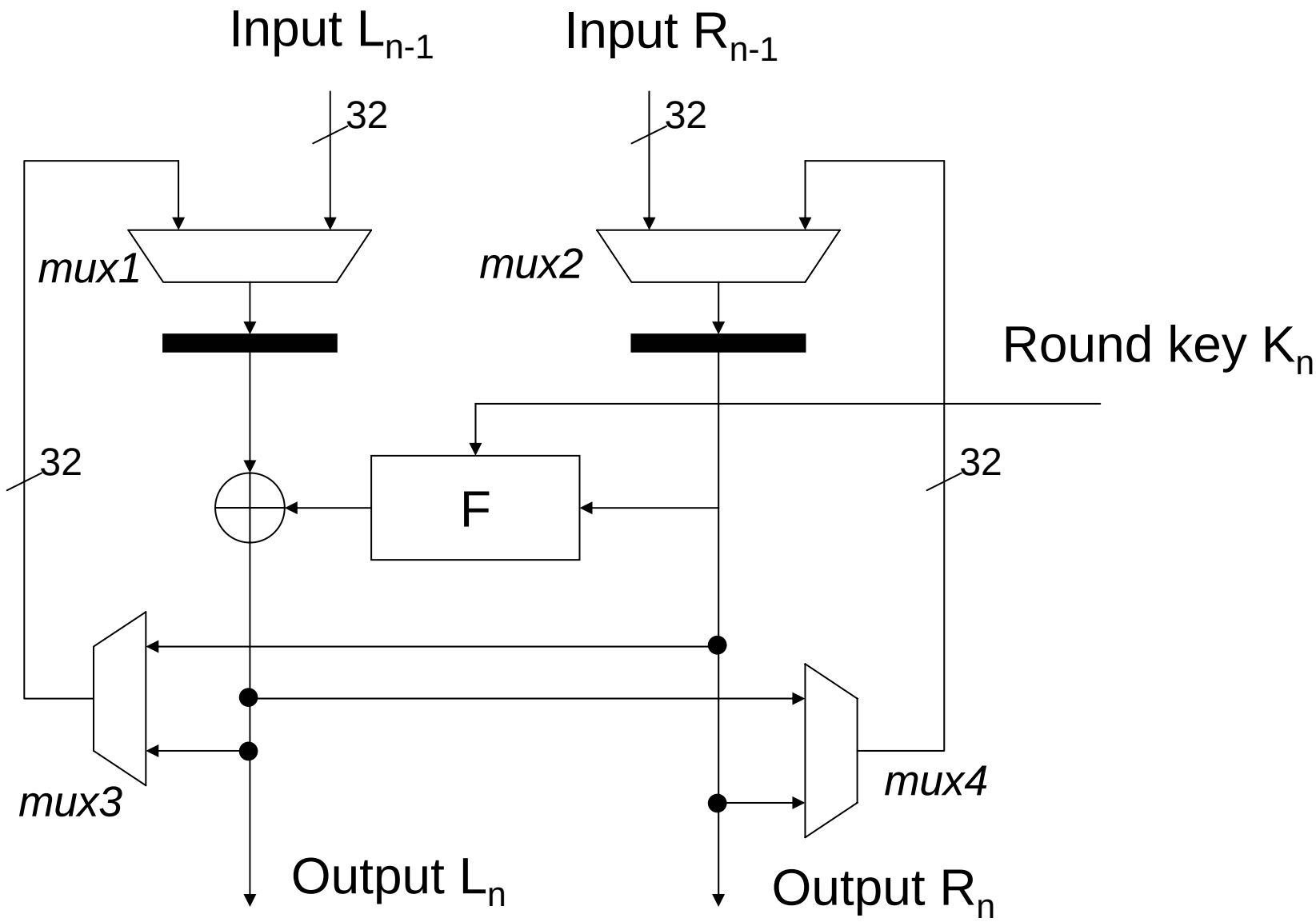
Typical Flow Diagram of a Secret-Key Block Cipher



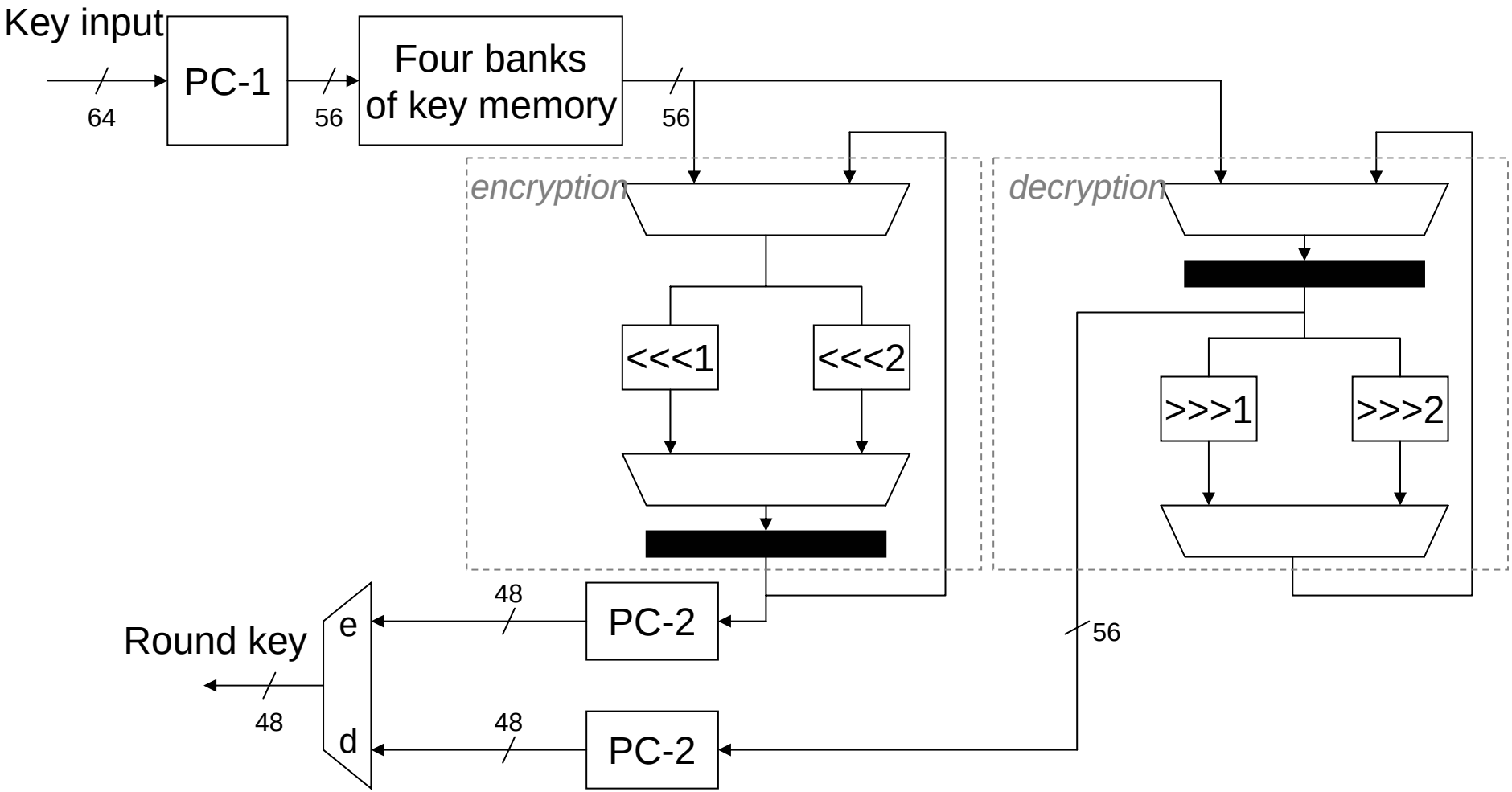
Basic iterative architecture



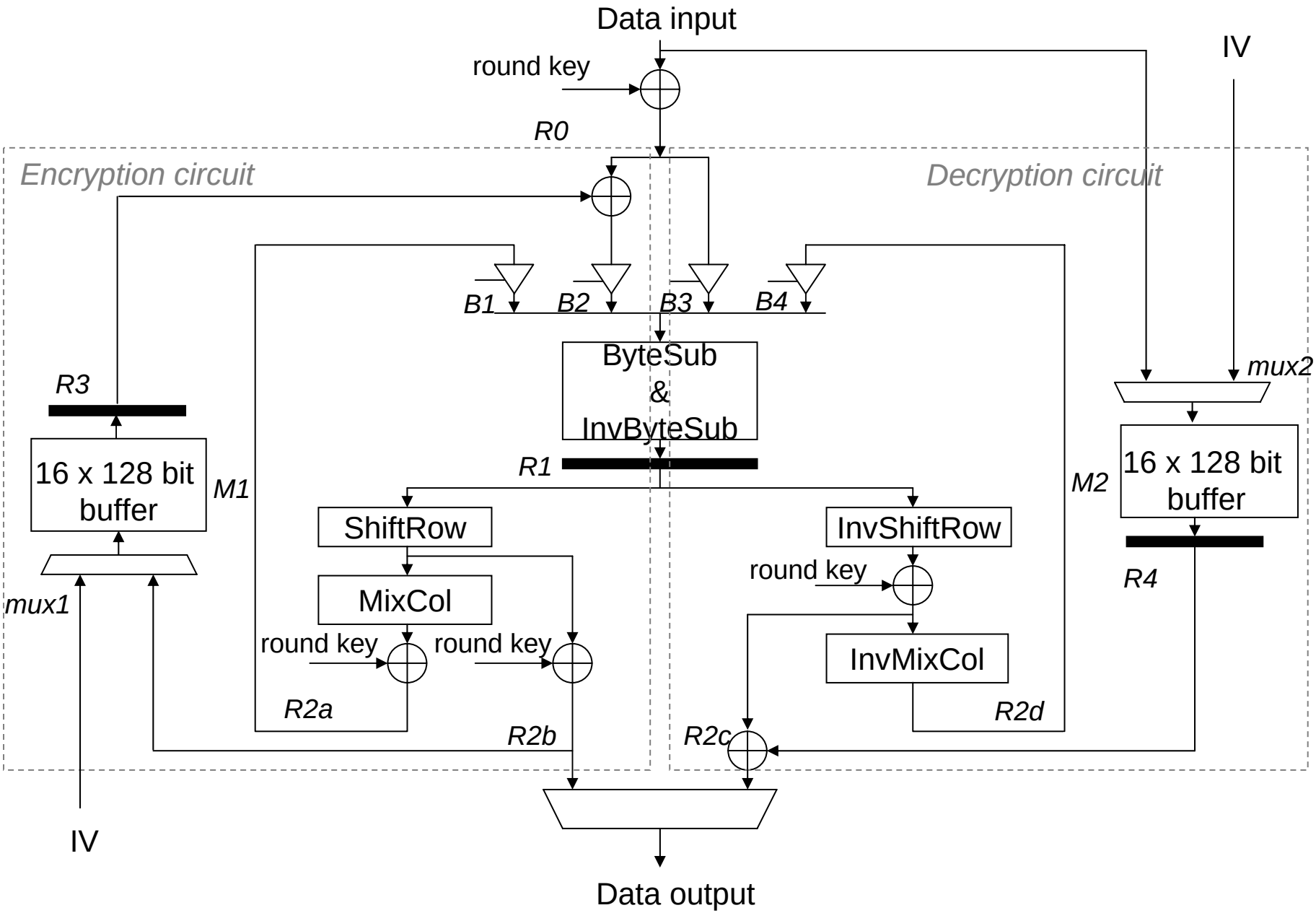
Triple DES: Basic Architecture
Encryption/Decryption Core



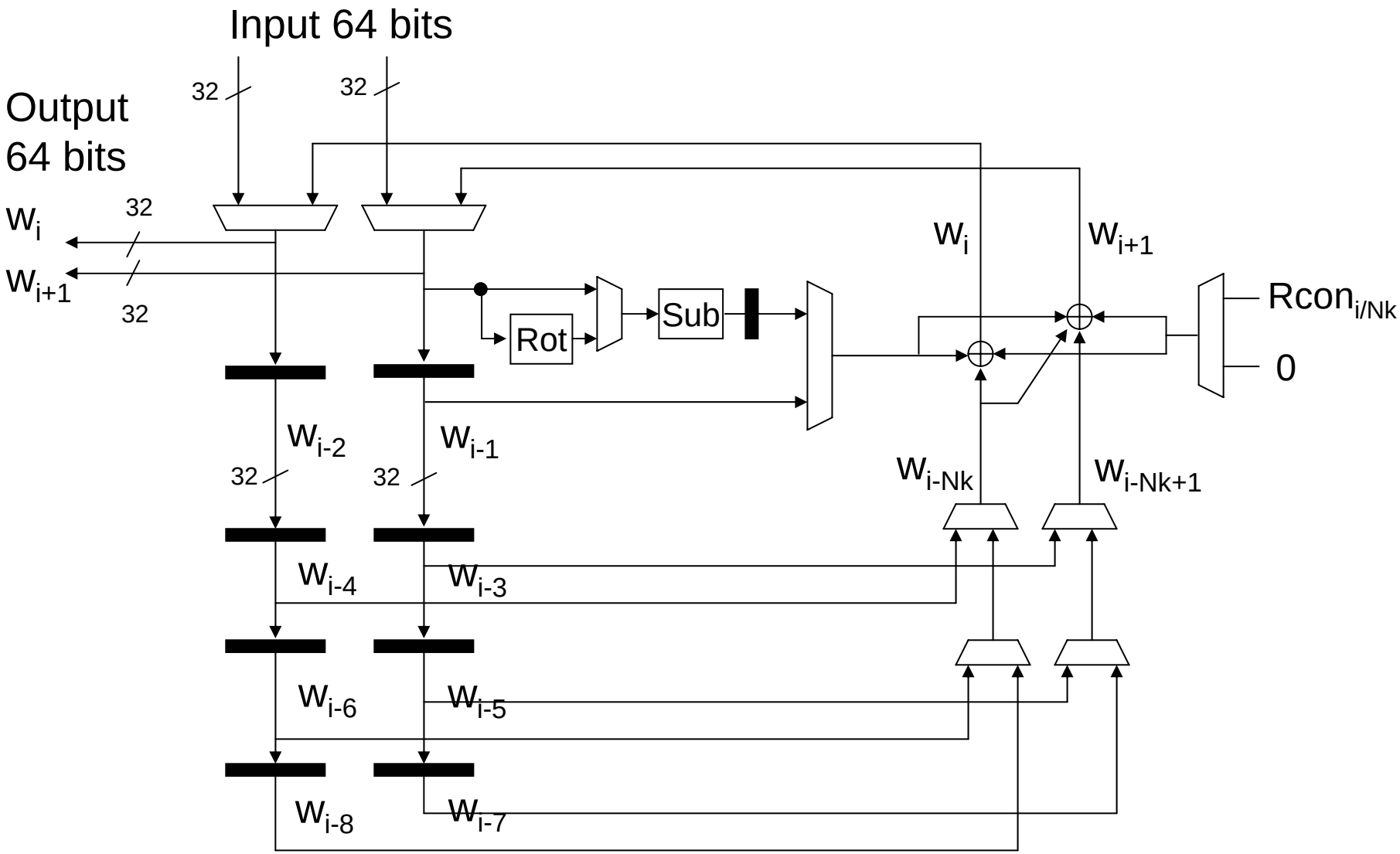
Triple DES: Basic Architecture
Key scheduling



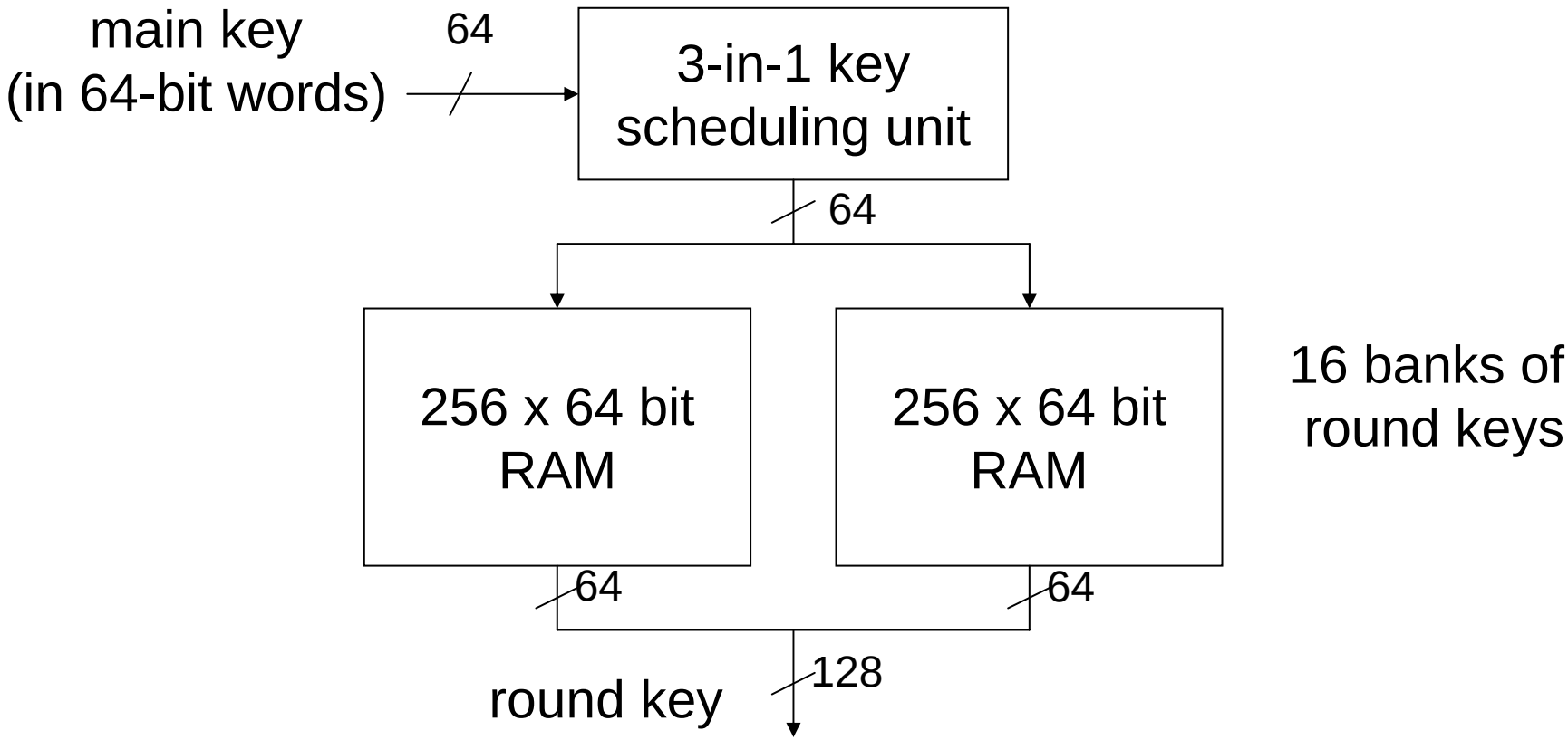
AES -Rijndael: Basic Architecture



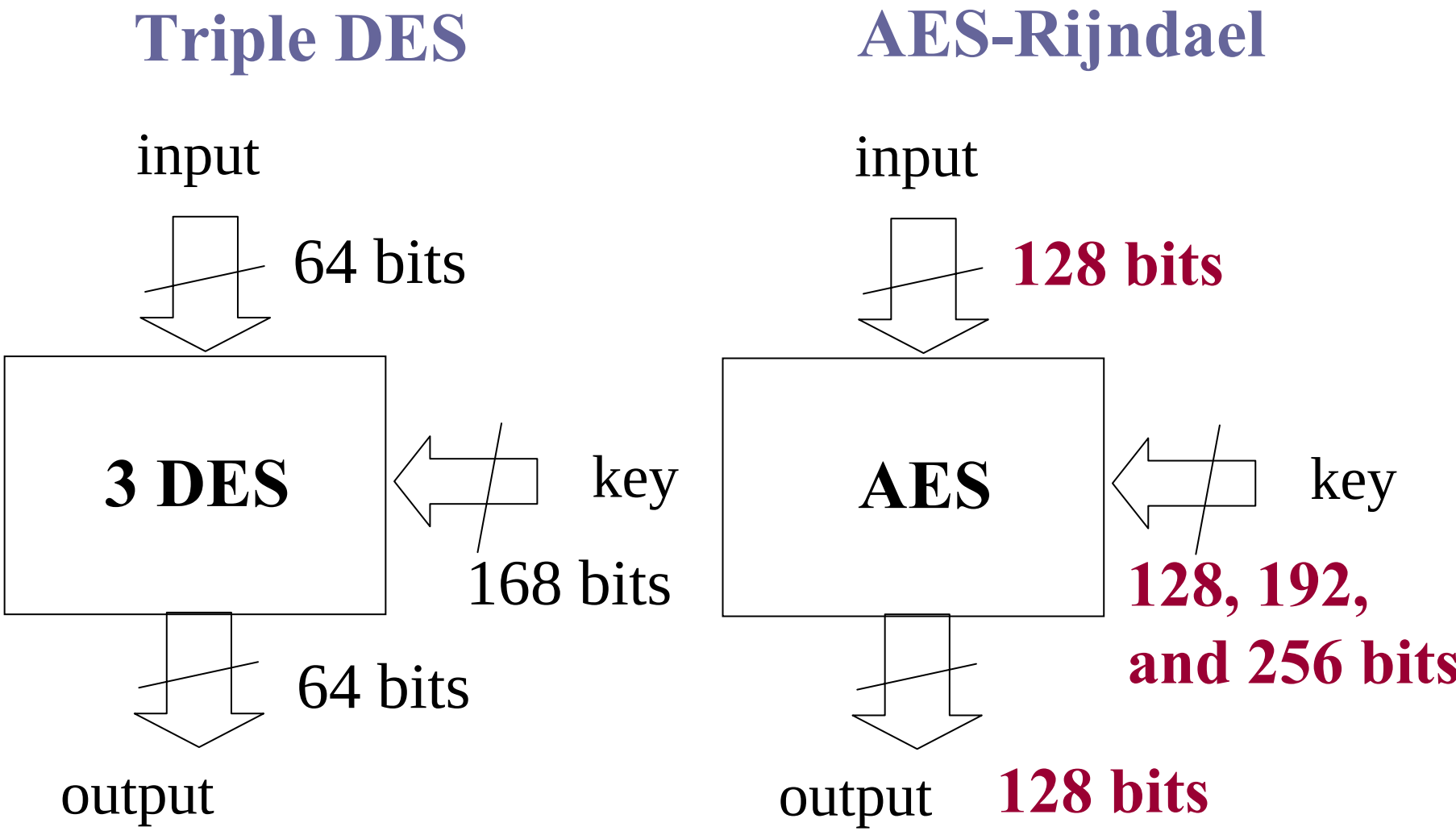
AES - Rijndael: 3-in-1 Key Scheduling Unit



Banks of round keys



Rijndael vs. Triple DES
External differences



Rijndael vs. Triple DES
Internal differences

Triple DES

Feistel network

Internal operations optimized for hardware

- the same circuit used for encryption and decryption
- compact design
- the same speed for encryption and decryption

Rijndael

Substitution-Linear Transformation Network

Internal operations optimized for software and hardware

- separate encryption and decryption units
- larger area
- different maximum encryption and decryption speeds

Rijndael vs. Triple DES
Functional differences

Triple DES

Round keys generated from the main key
- in arbitrary order
- one round key per clock cycle

Round keys can be computed on the fly

Rijndael

Round keys generated from the main key
- in only one order
- 1/4 th or 1/2 nd of a round key per clock cycle

Round keys need to be precomputed and stored in internal memory

Testing Procedure

1. Functional testing

Tests based on NIST Special Publication 800-20

- Known Answer Tests
- Monte Carlo Test

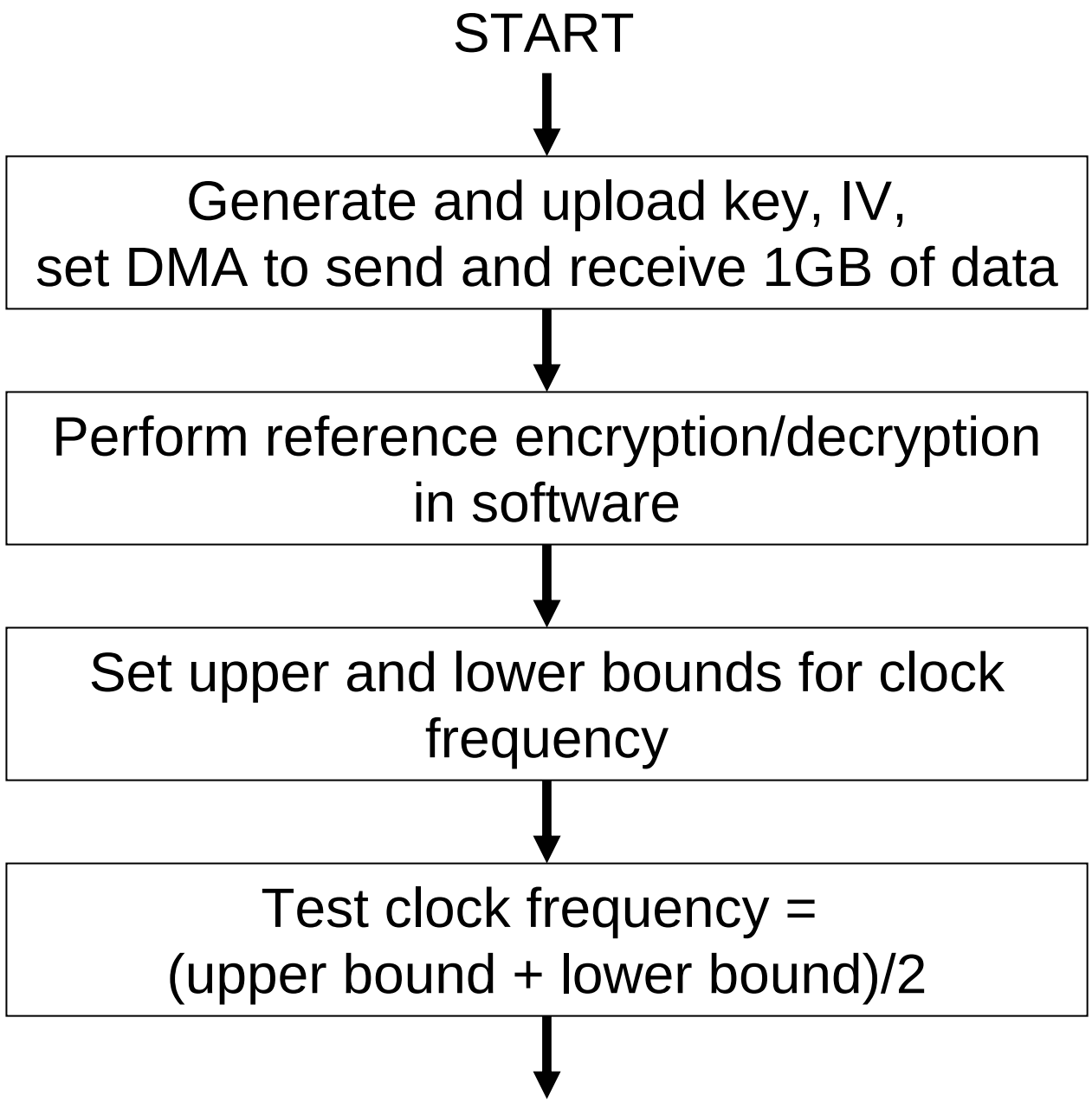
2. Maximum clock frequency test

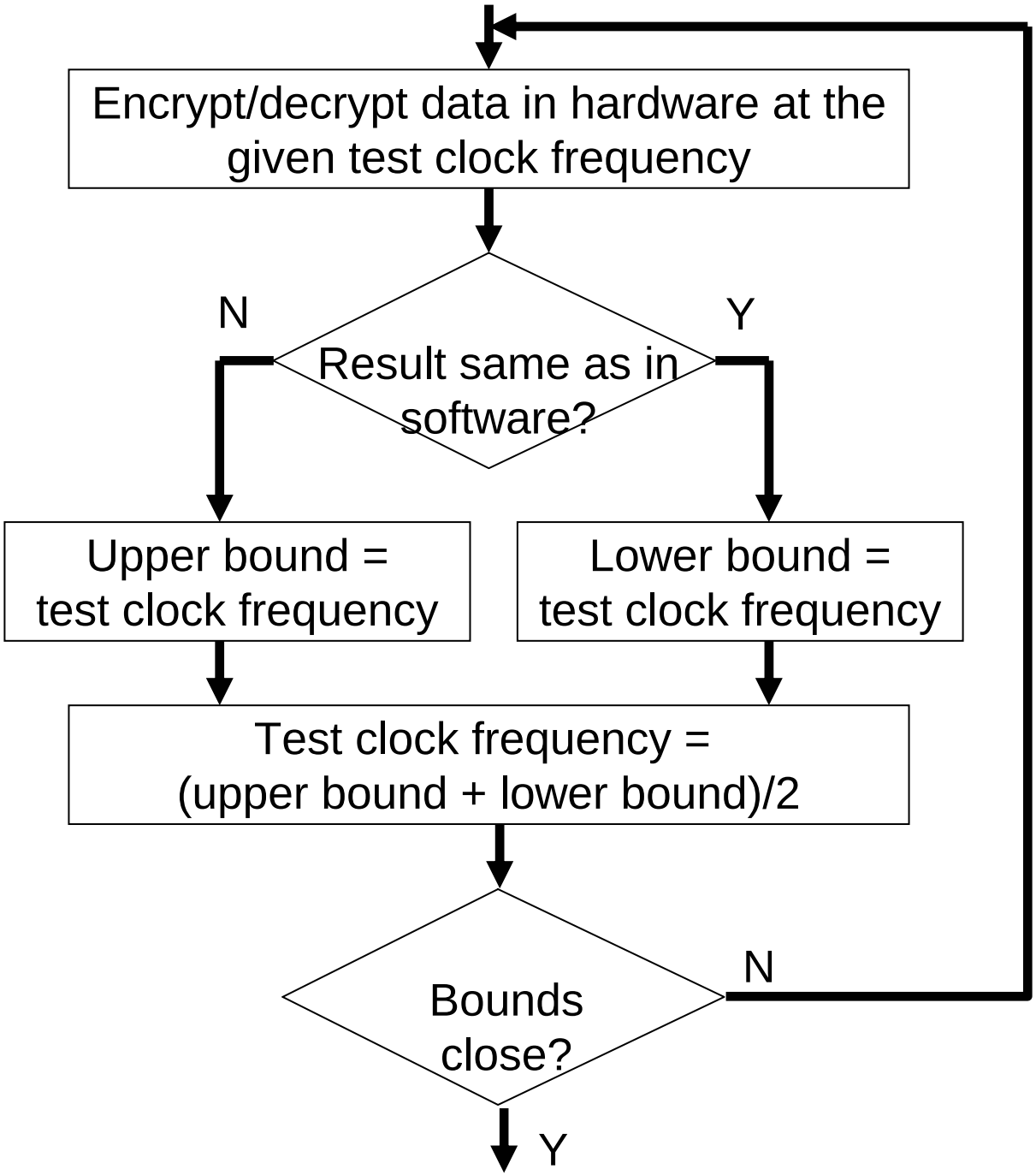
- clock frequency varied using binary search
- 1 GB of data encrypted or decrypted in the CBC mode
- results compared with results from software implementation

3. Maximum encryption/decryption throughput test

- maximum clock frequency
- 4 GB of data encrypted or decrypted in the CBC mode
- time necessary to complete all operations determined

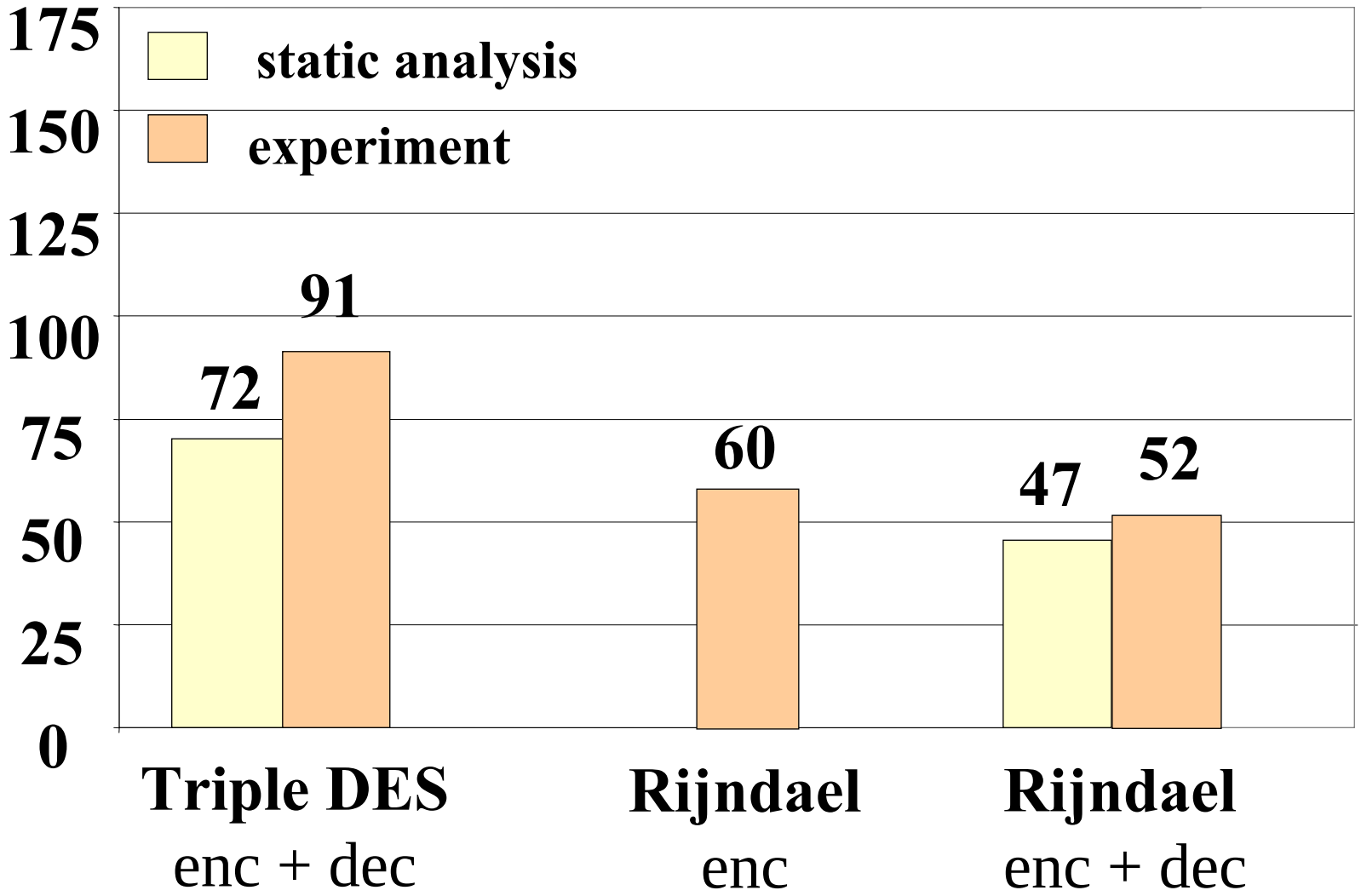
Maximum Clock Frequency Test (1)



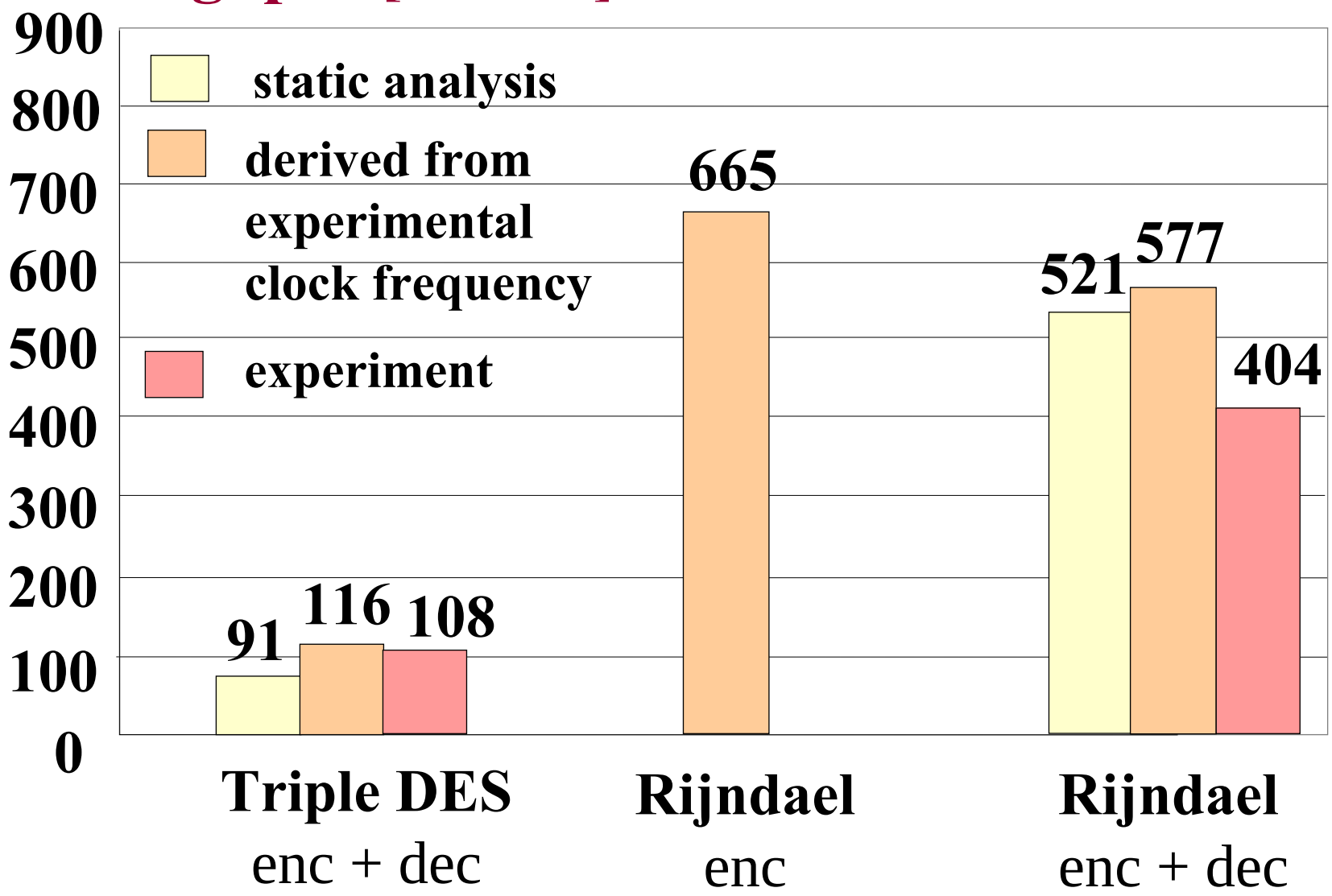

Encrypt/decrypt data in hardware at the given test clock frequency
Result same as in software?
N
Y
Upper bound = test clock frequency
Lower bound = test clock frequency
Test clock frequency = (upper bound + lower bound)/2
Bounds close?
N
Y

Results for basic architectures

Maximum clock frequency [MHz]

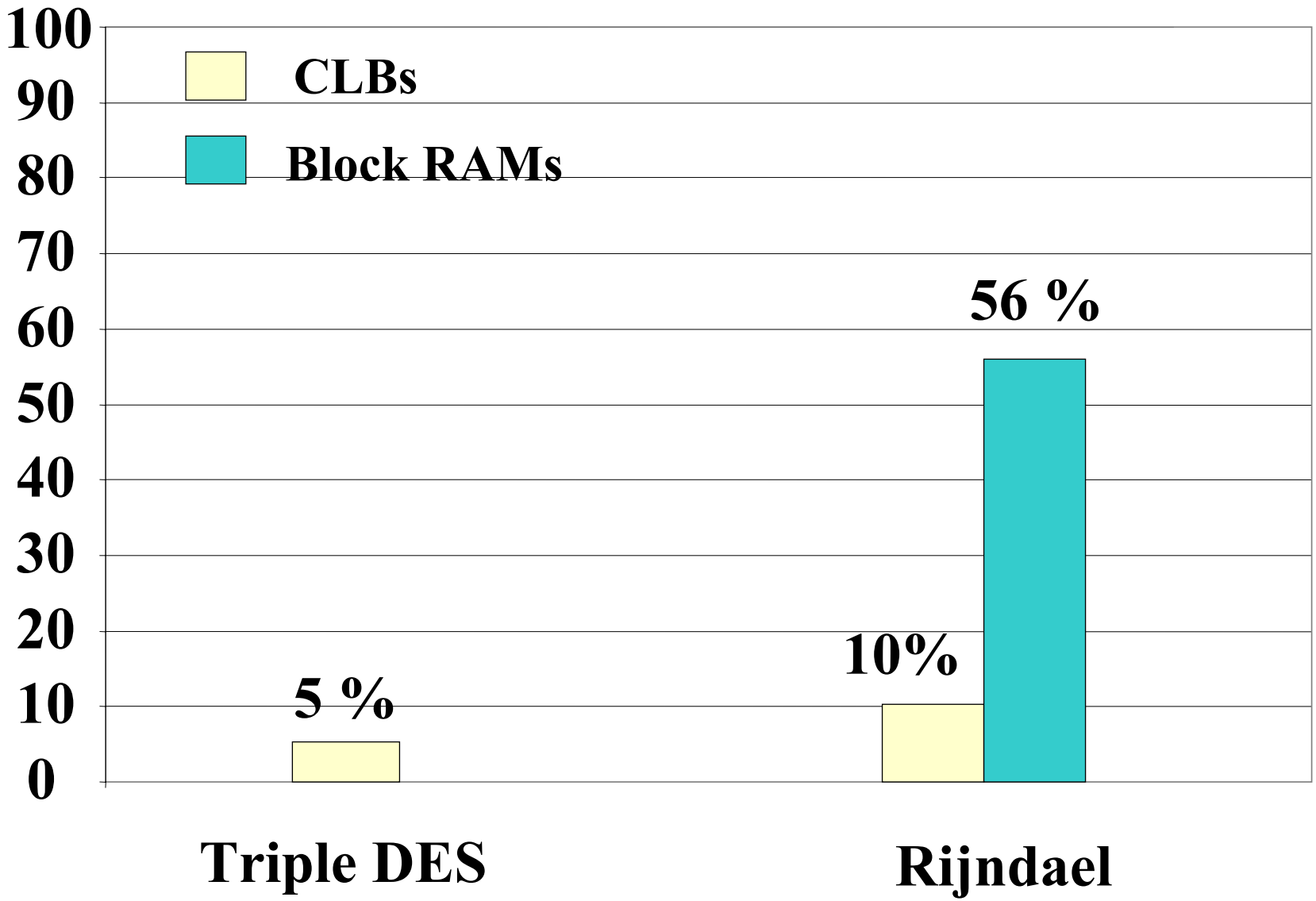


Corresponding circuit throughputs

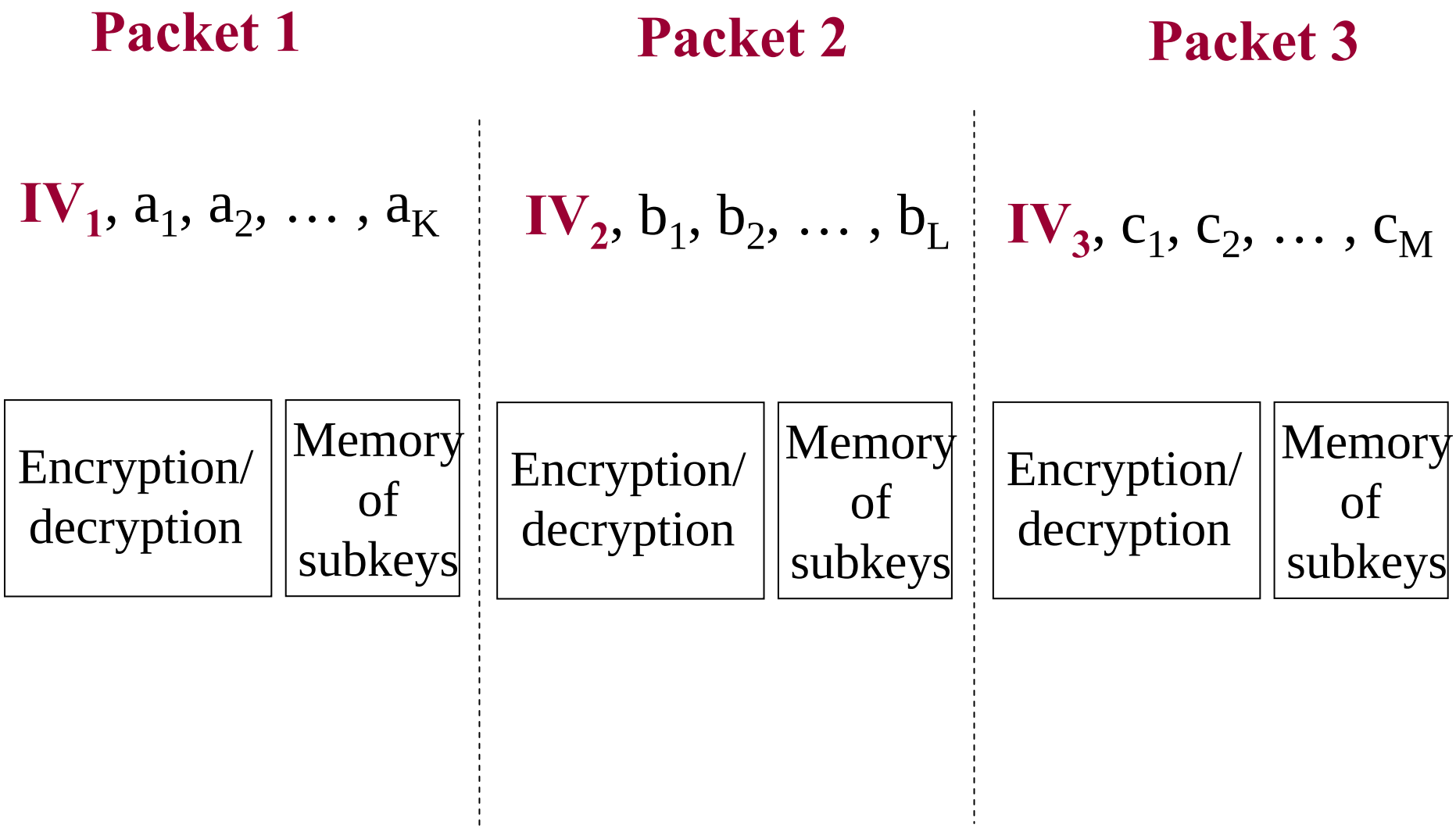


Use of resources: basic architecture

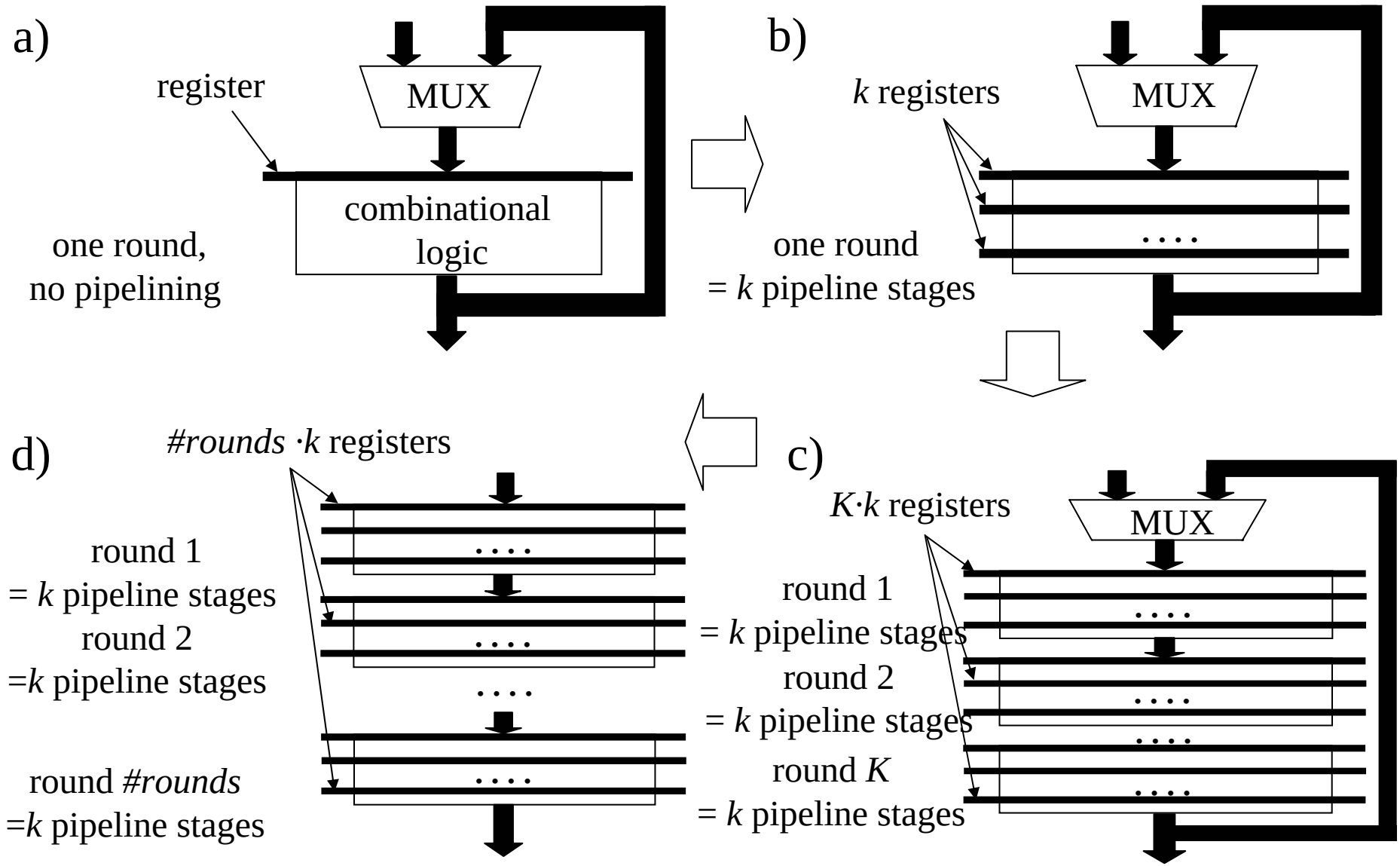
Percentage of the Virtex 1000 device resources



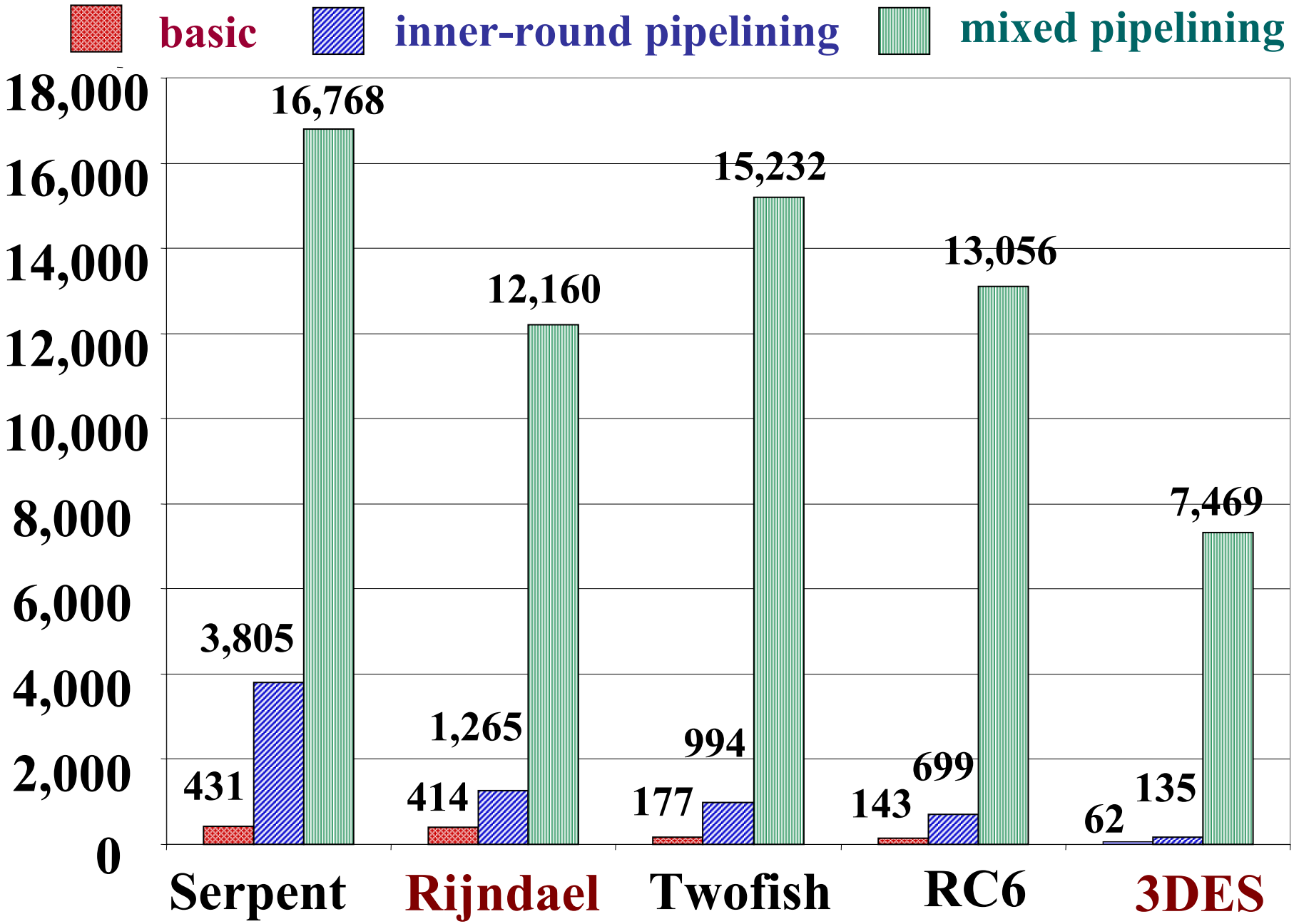
Increasing throughput using parallel processing



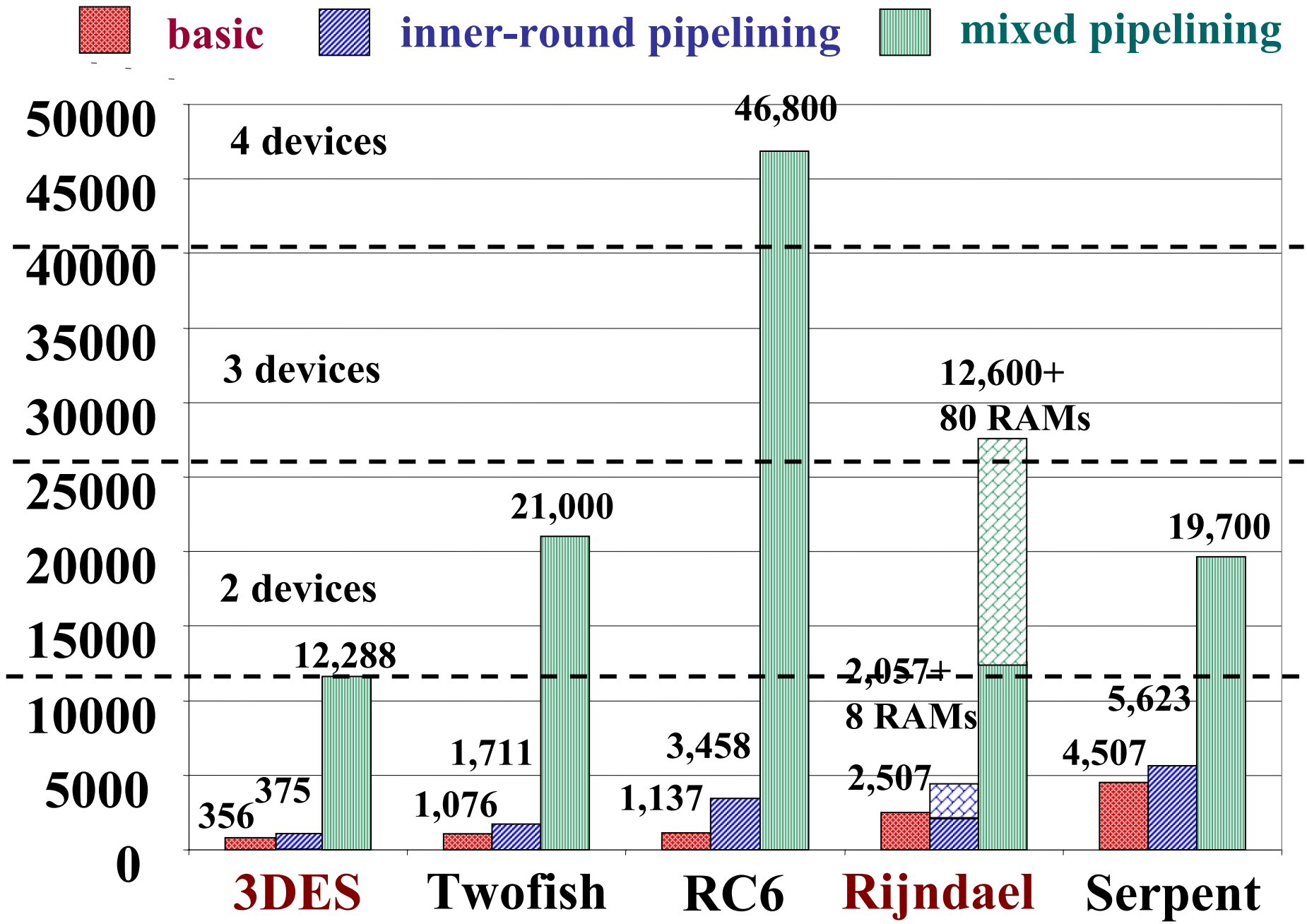
Increasing throughput using pipelining



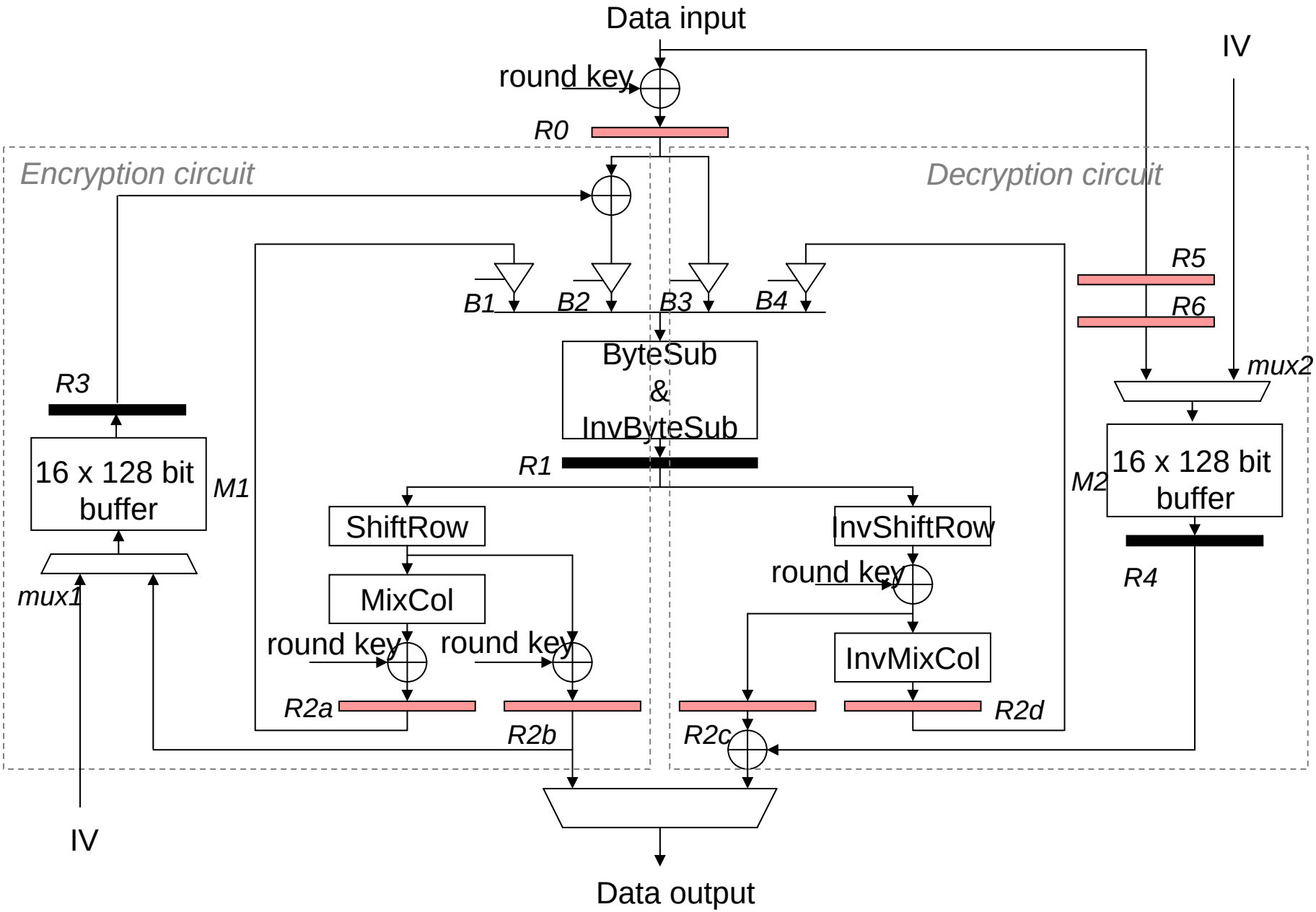
Throughput [Mbit/s]



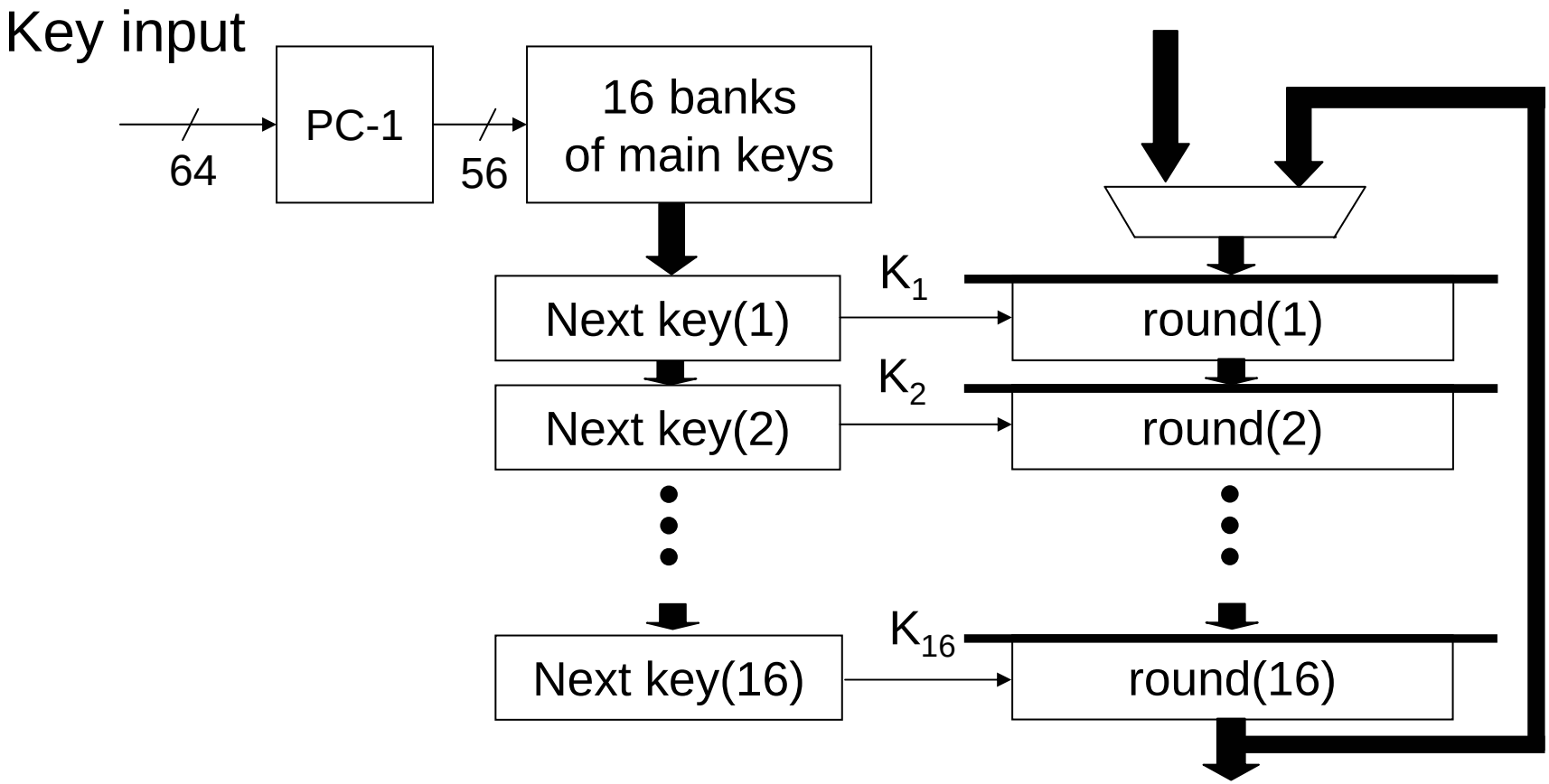
Area [CLB slices]



AES -Rijndael: Extended Architecture

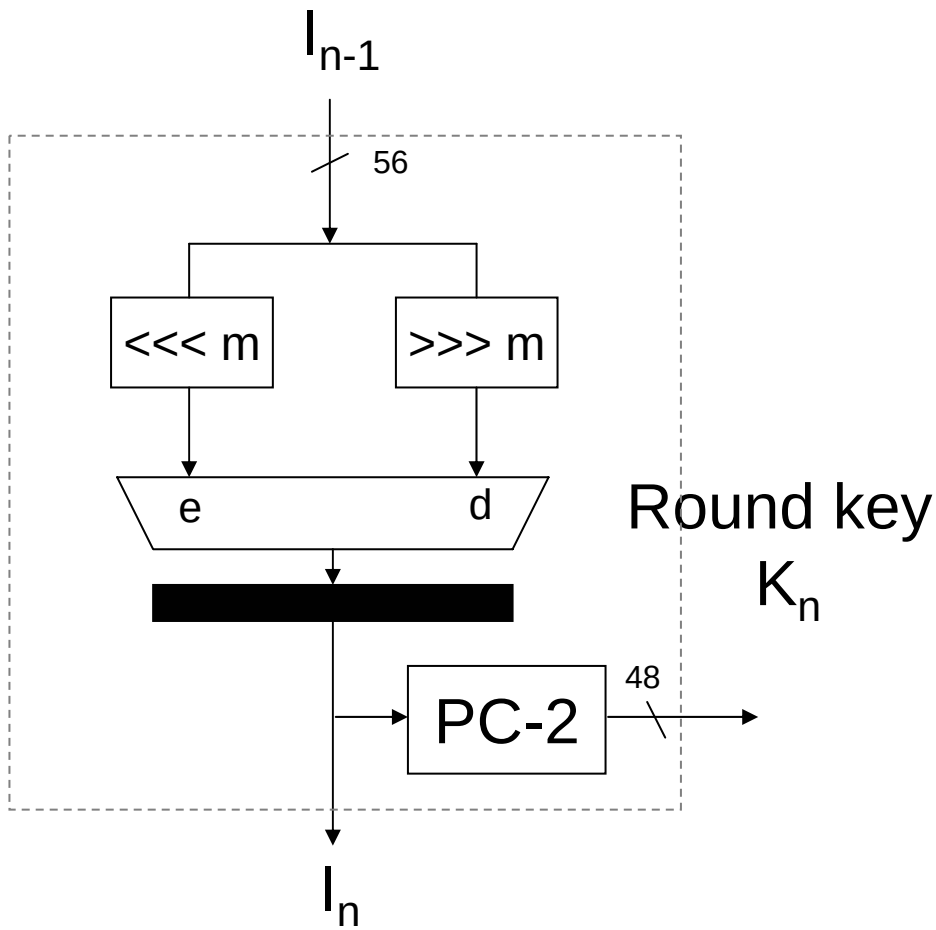


Triple DES: Extended Architecture

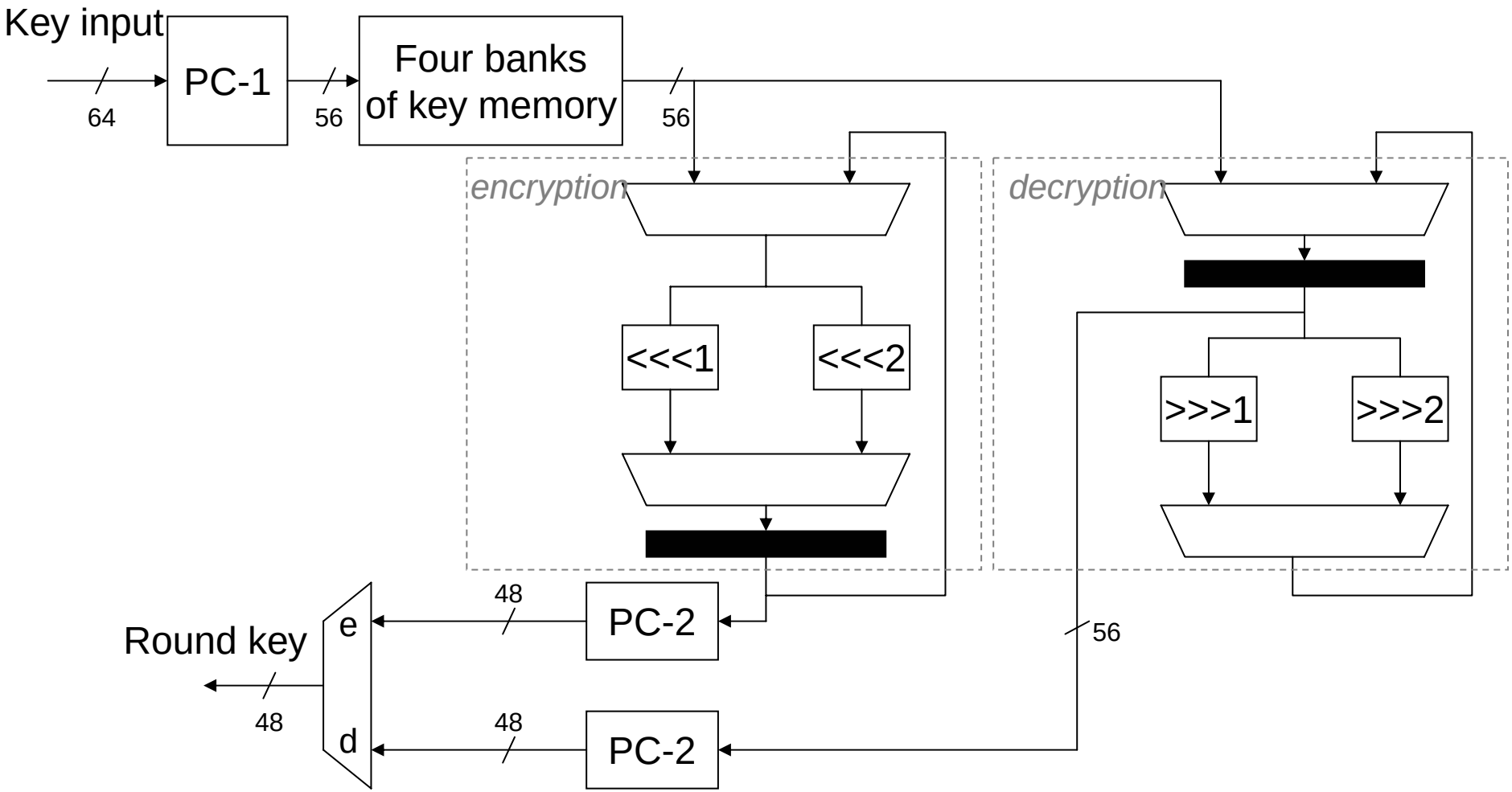


Simplification of the key scheduling unit: extended architecture

Next key(n)

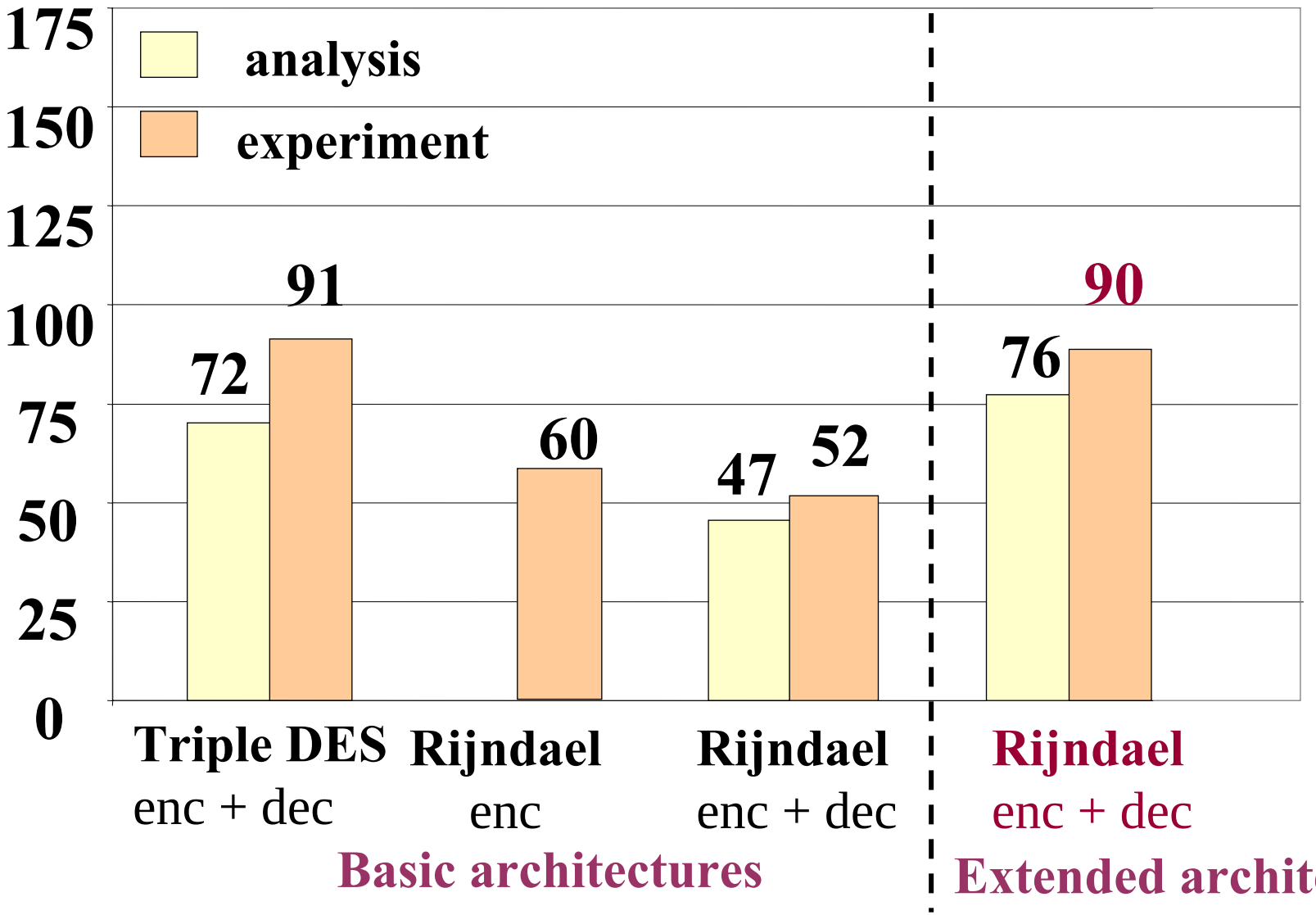


Triple DES: Key scheduling in basic architecture

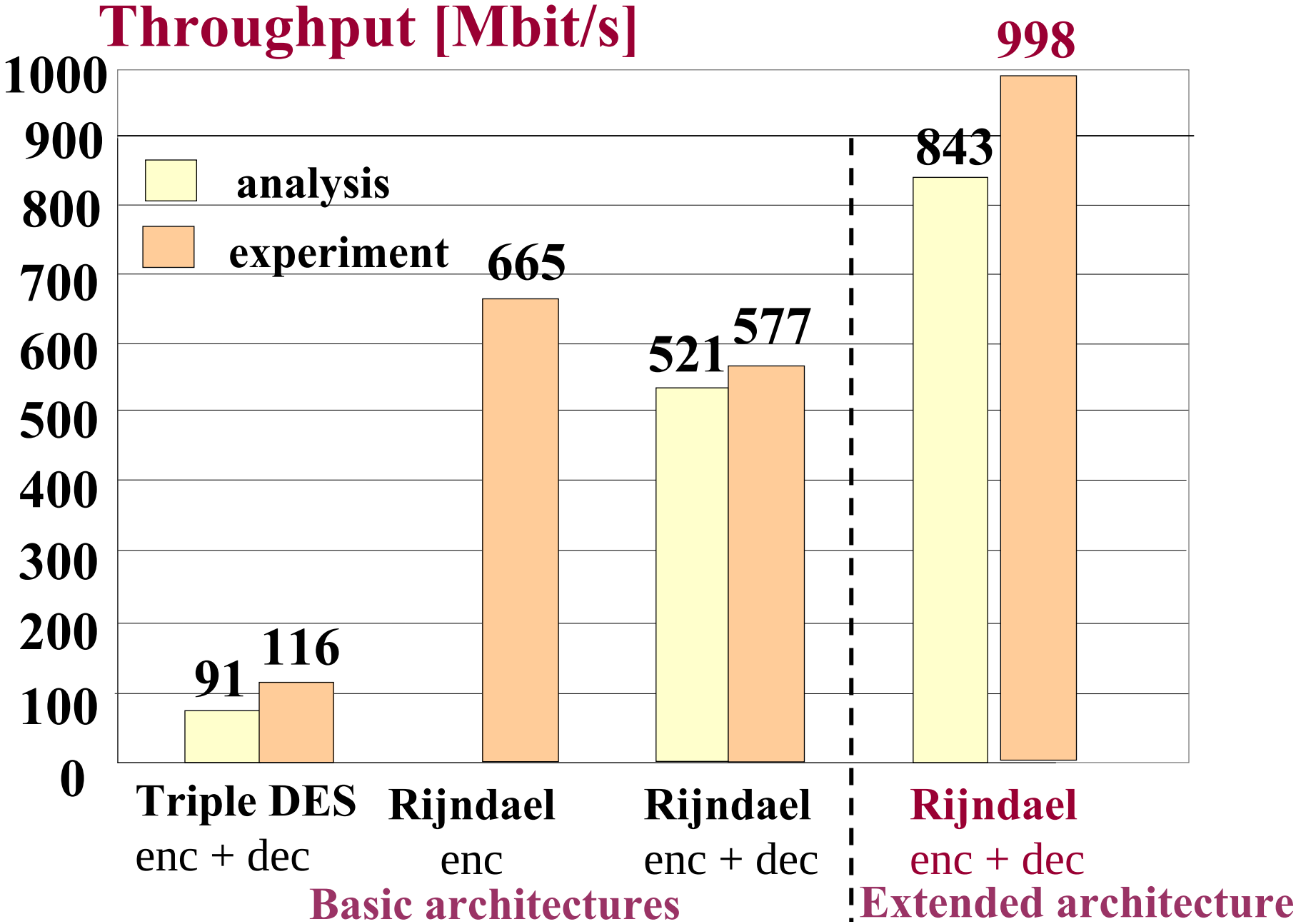


Tentative results for extended architecture

Maximum clock frequency [MHz]

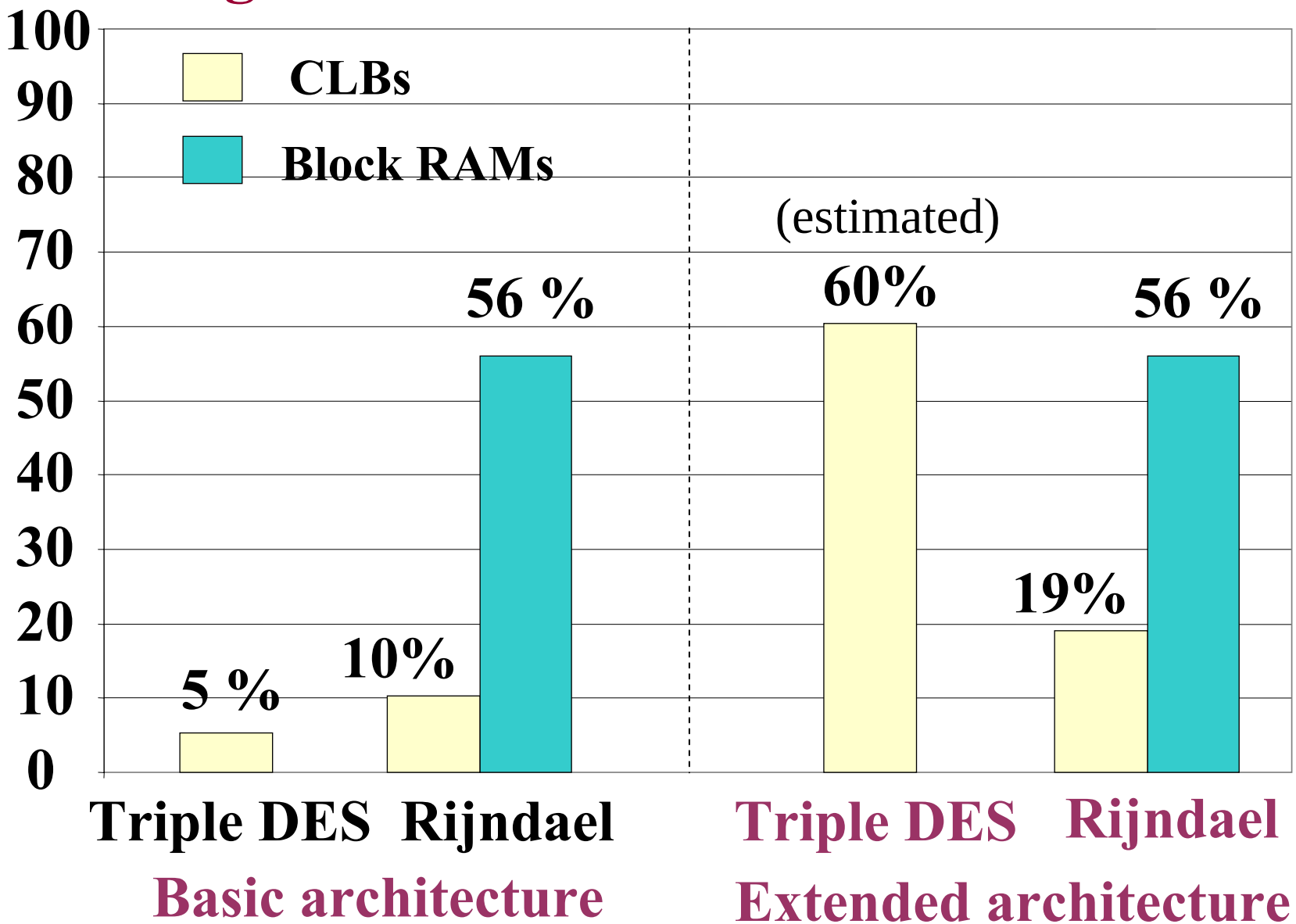


Corresponding circuit throughputs



Use of resources by extended architectures

Percentage of the Virtex device resources



Conclusions

- High-speed **IPSEC-compliant implementations of Rijndael and Triple DES** developed and tested experimentally using the SLAAC-1V FPGA accelerator board

- Encryption and decryption throughputs of Rijndael in the range of **1 Gbit/s** (998 Mbit/s) demonstrated experimentally

- Integrated 1 Gbit/s implementation of Rijndael and Triple DES shown to require only **80% of resources of a single FPGA** device Virtex XCV-1000

- **SLAAC-1V** accelerator board capable of supporting encryption & decryption throughputs in the range of **3 Gbit/s**