Performance and Overhead in a Hybrid Reconfigurable Computer

O. D. Fidanci[1], D. Poznanovic[2], K. Gaj[3],
T. El-Ghazawi[1], N. Alexandridis[1]

[1]George Washington University,
[2]SRC Computers Inc.,
[3]George Mason University

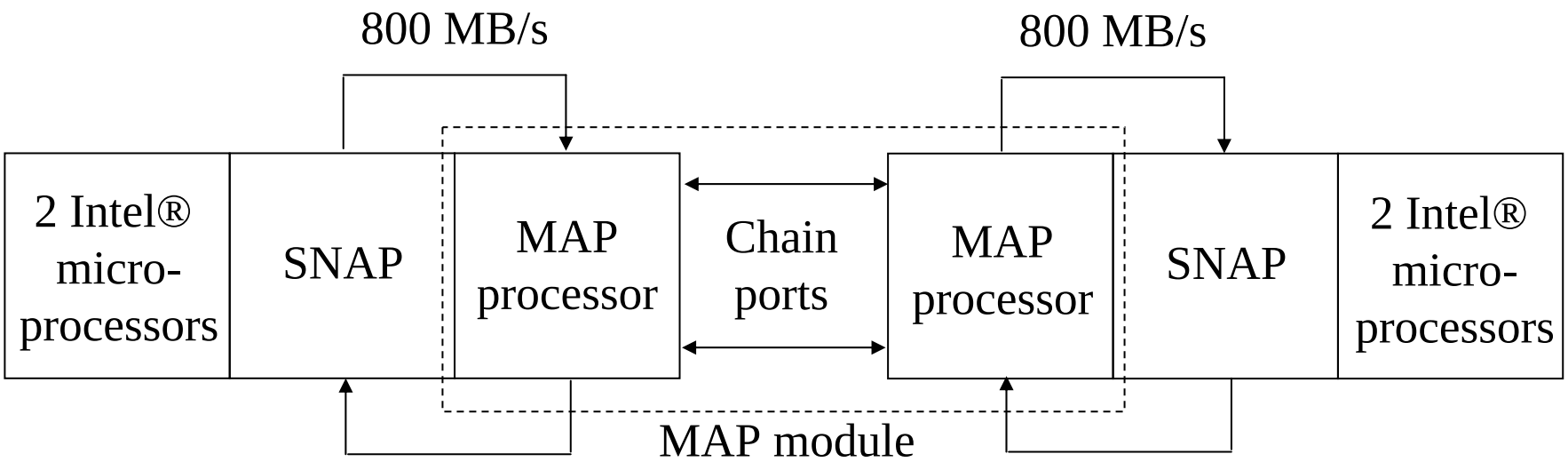
http://cpe02.gmu.edu/rcm/

Features of General-Purpose Reconfigurable Computers

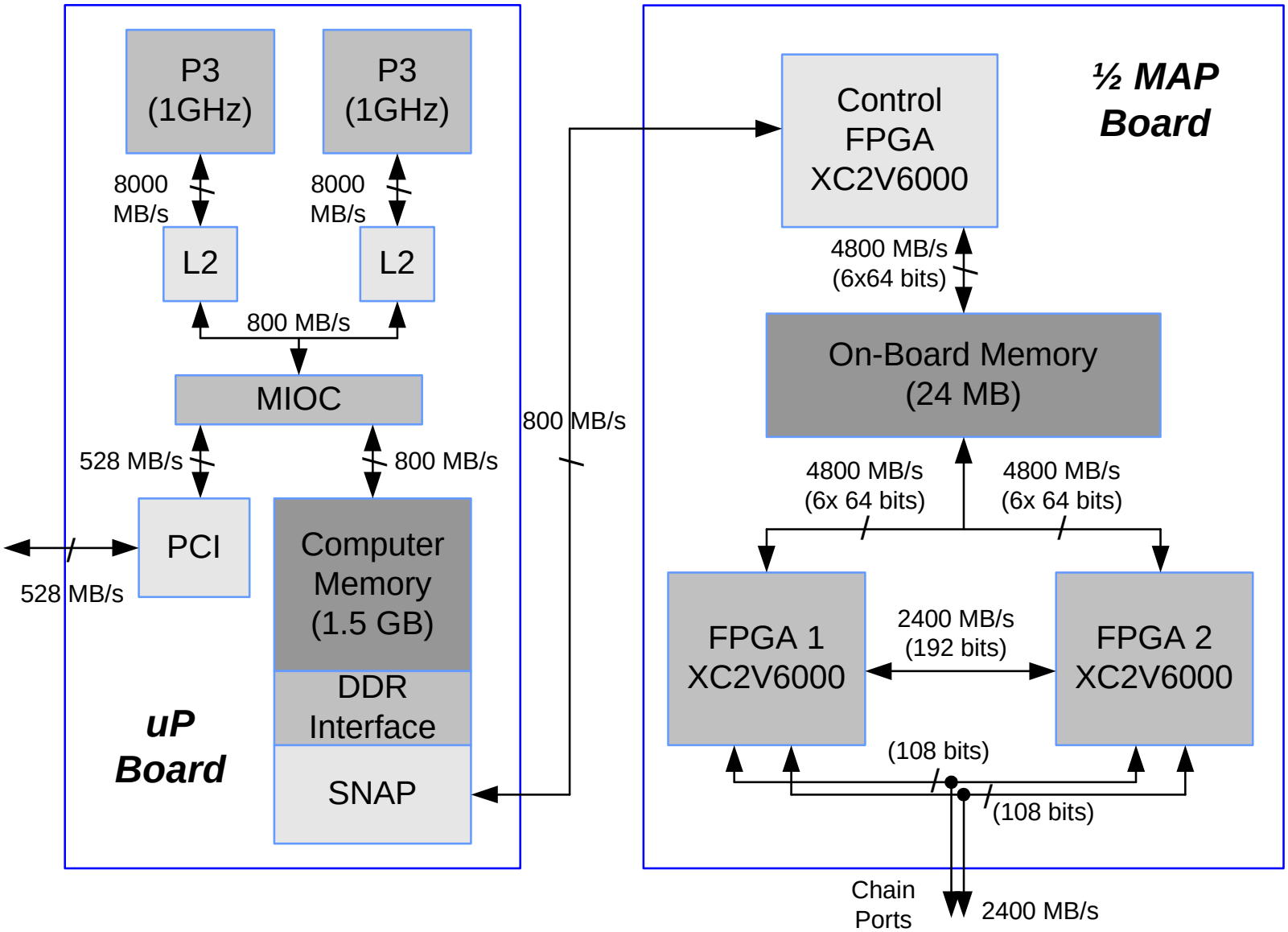
- ✓ composed of traditional microprocessors and Field Programmable Gate Arrays (FPGAs) closely integrated with each other
- ✓ programming does not require knowledge of hardware design
- ✓ permit run-time reconfiguration of FPGAs

Hardware Architecture and Programming Model of SRC-6E

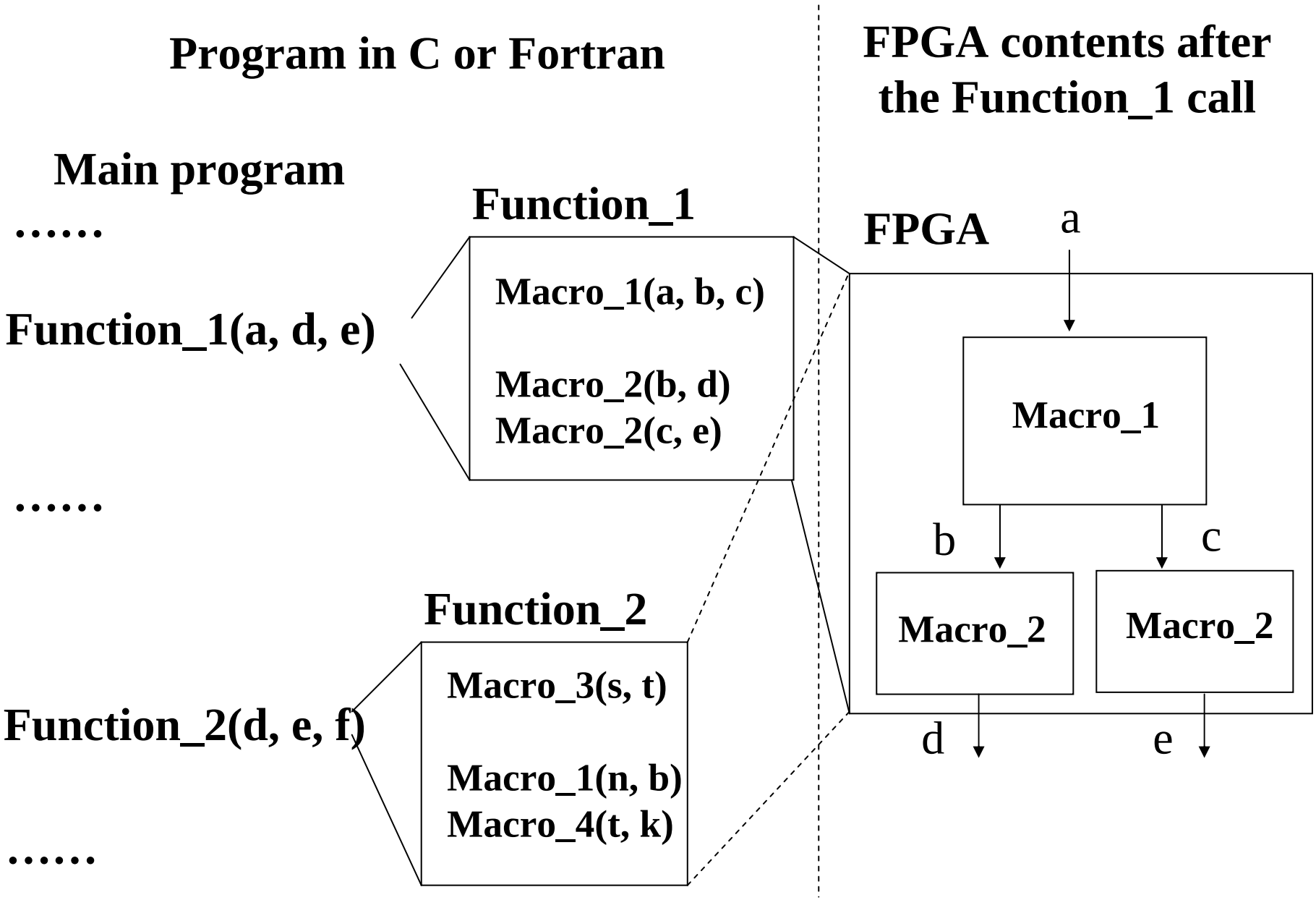
SRC Hardware Architecture



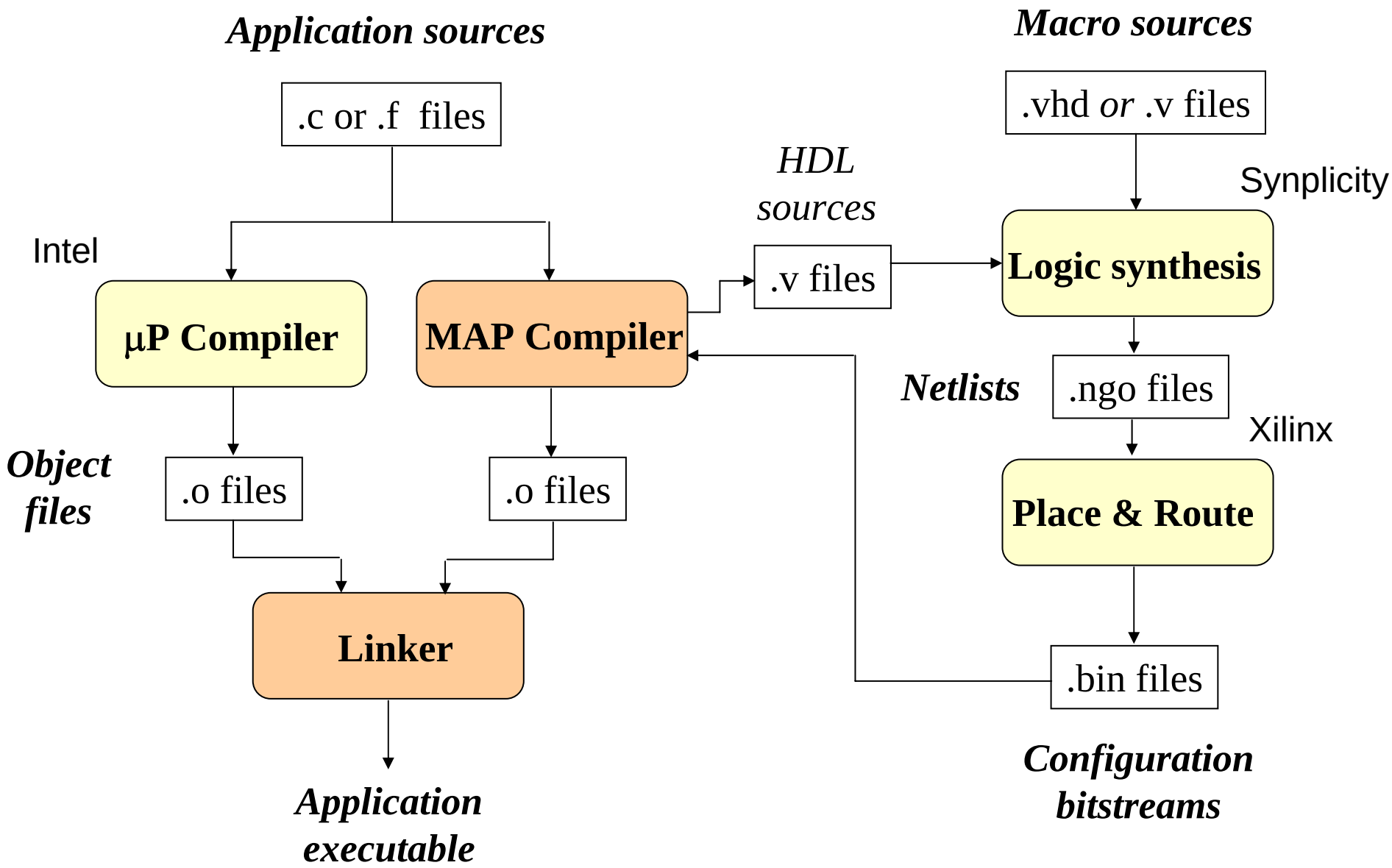
SRC Hardware Architecture – cont.



SRC Programming Model



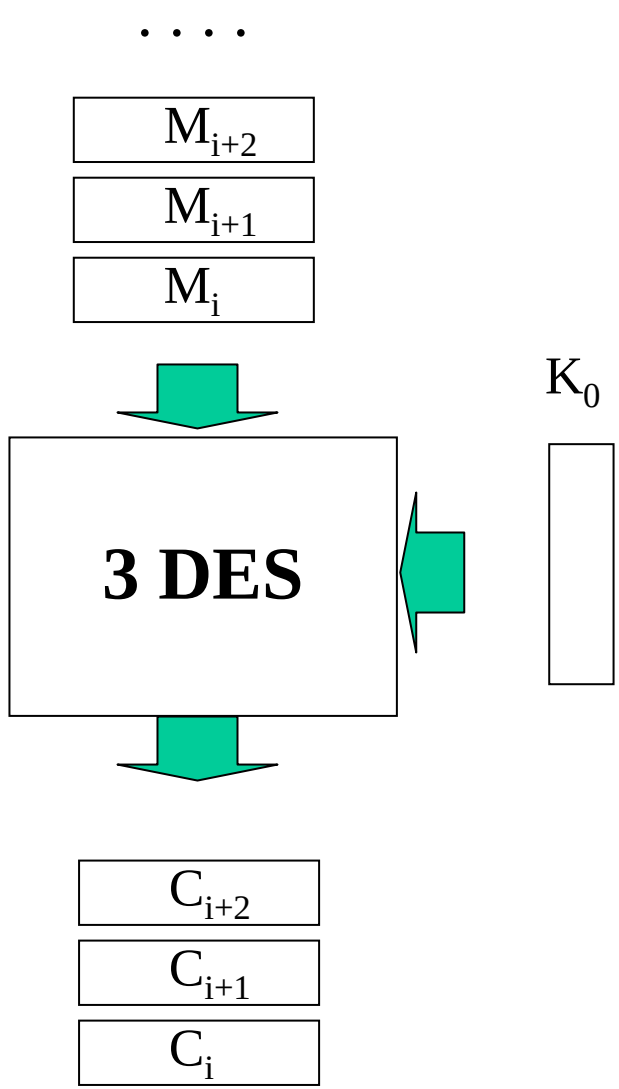
Compilation Process of SRC-6E



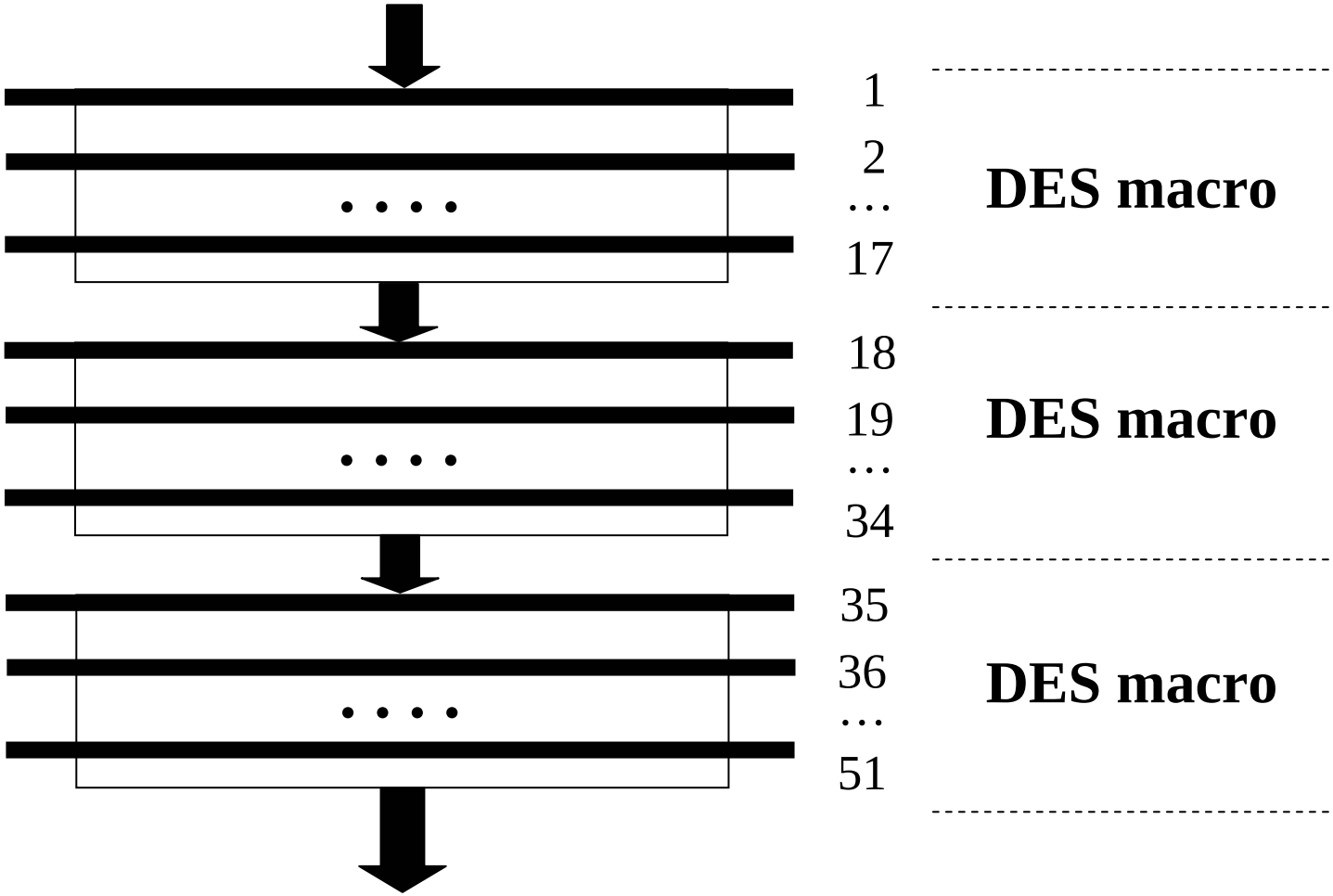
Application Case Study 1

High-throughput Triple DES encryption

High-throughput encryption

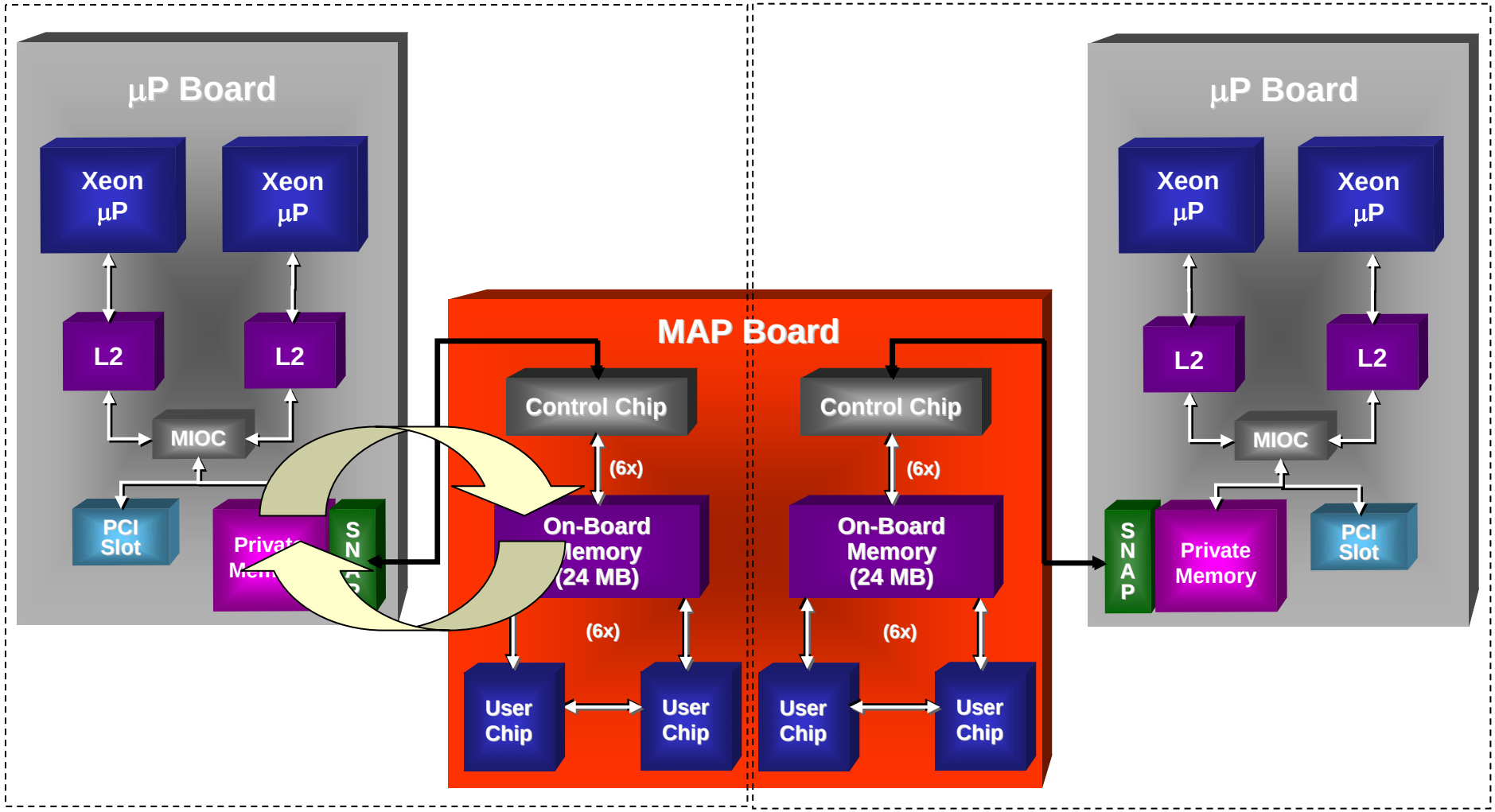


Fully pipelined architecture of Triple DES



- **51 pipeline stages**
- **New input & new output every clock cycle**

Overhead of the data transfer

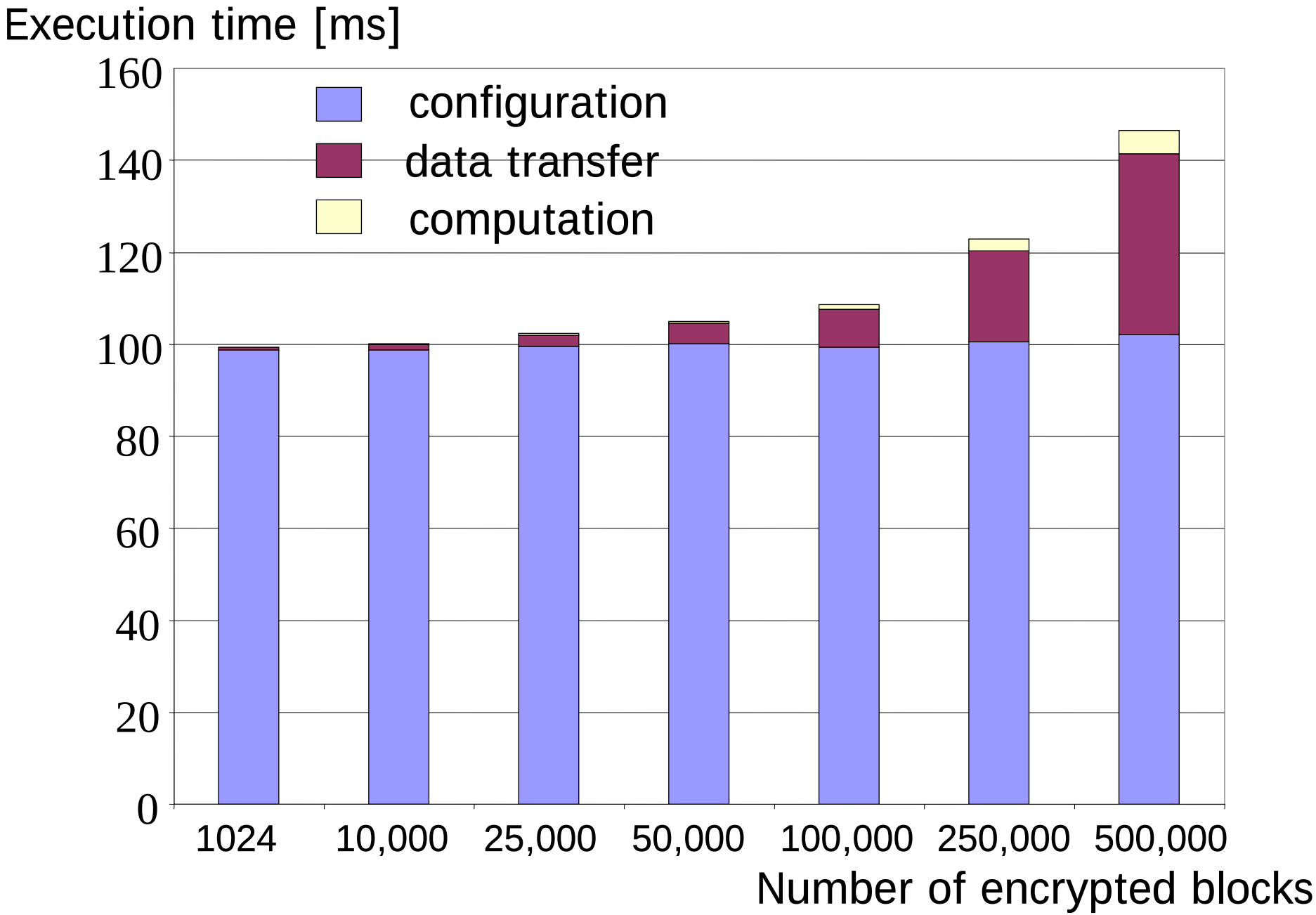


Timing Measurements

Three-level timing measurement scheme has been employed:

1. end-to-end execution time: (wall clock time - HLL Level) includes the configuration, data transfer and data processing times
2. w/o configuration time: (wall clock time - HLL Level) excludes the configuration time but includes data transfer and data processing times
3. MAP Time: (clock counter - Hardware Level) only includes data processing time

Triple DES Encryption



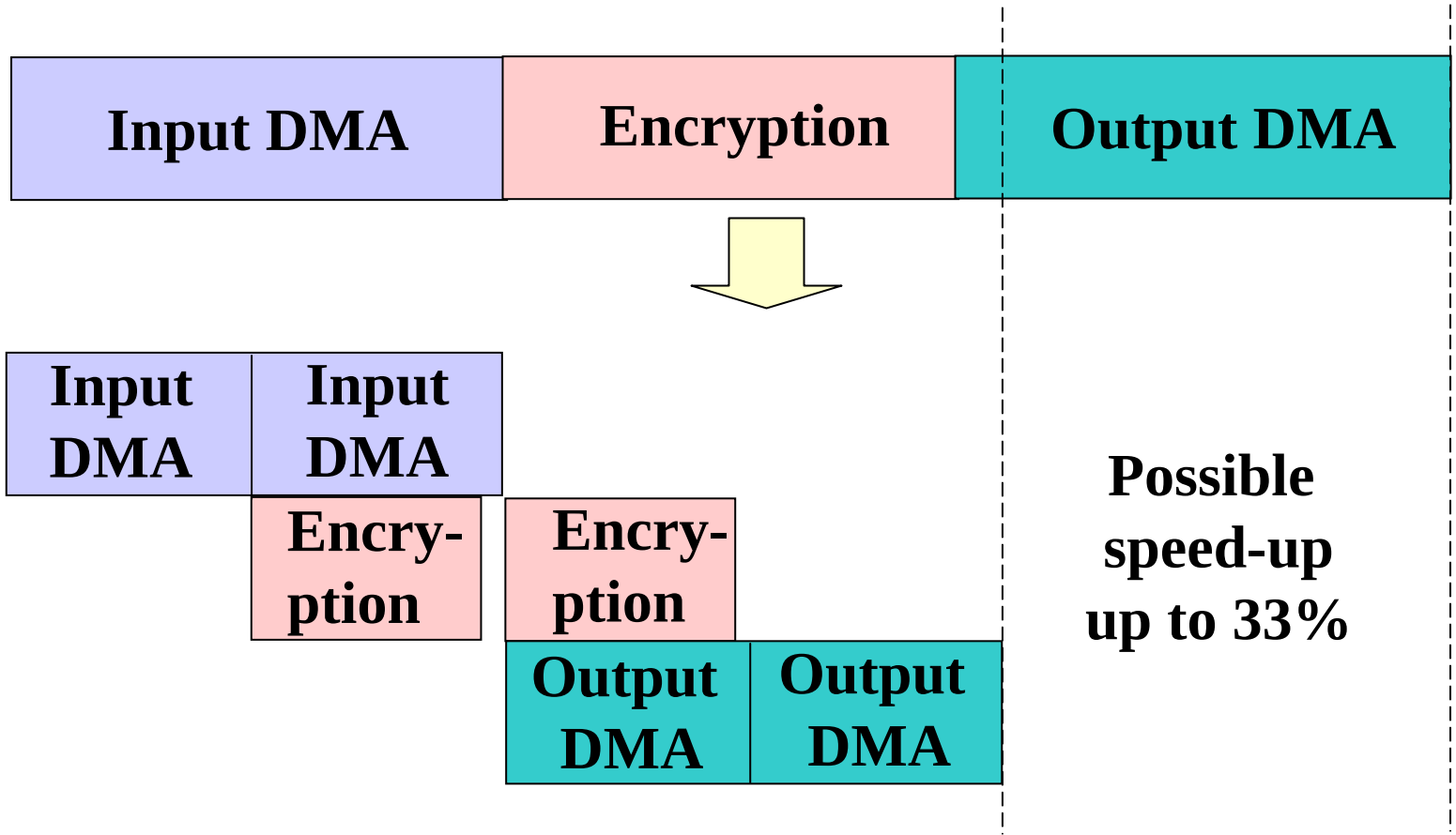
Problems

- execution time dominated by
  - configuration of the MAP FPGA and
  - data transfer between the System Common Memory and On-Board-Memory

- configuration time hiding techniques
  - preloading the configuration before execution
  - flip-flopping FPGAs during reconfiguration

Data transfer hiding techniques

- Data transfer can be hidden by overlapping DMA time with the data processing time



Reference software implementations

Platform:

Pentium 4, 1.8 GHz, 512 kB cache, 1 GB RAM

Software:

Non-optimized:

Public domain code
C only

Intel C++
-O3 optimization

Optimized for encryption (but not for cipher breaking):

Phil Karn's DES code
C and assembly language with look-up table precomputations

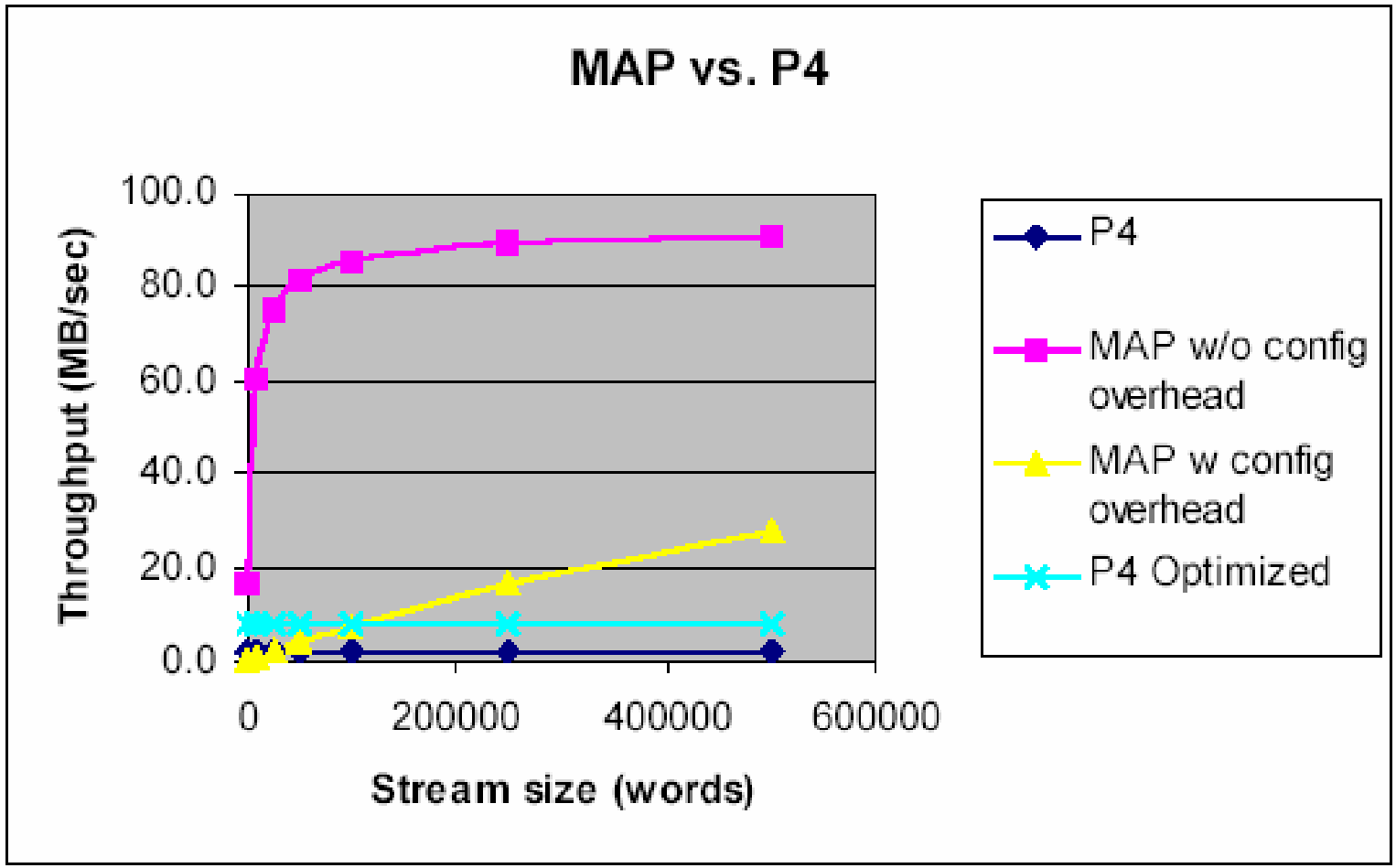
GNU gcc v. 2.96
-O4 optimization

Total execution time of Triple DES for Pentium 4 using optimized and non-optimized code

	P4 non-optimized		P4 optimized	
Length (words)	Total time (sec)	Throu-ghpu (MB/sec)	Total time (sec)	Throu-ghput (MB/sec)
1024	0.00379	2.15920	0.00102	8.06299
10,000	0.03663	2.18400	0.01010	7.92354
25,000	0.09279	2.15540	0.02561	7.80969
50,000	0.18637	2.14627	0.05116	7.81937
100,000	0.37150	2.15343	0.09960	8.03253
250,000	0.91990	2.17415	0.25478	7.84985
500,000	1.83200	2.18341	0.49841	8.02546

$$\frac{\text{Optimized P4 code}}{\text{Non-optimized P4 code}} \approx 4$$

Throughput results for SRC-6E and Pentium 4



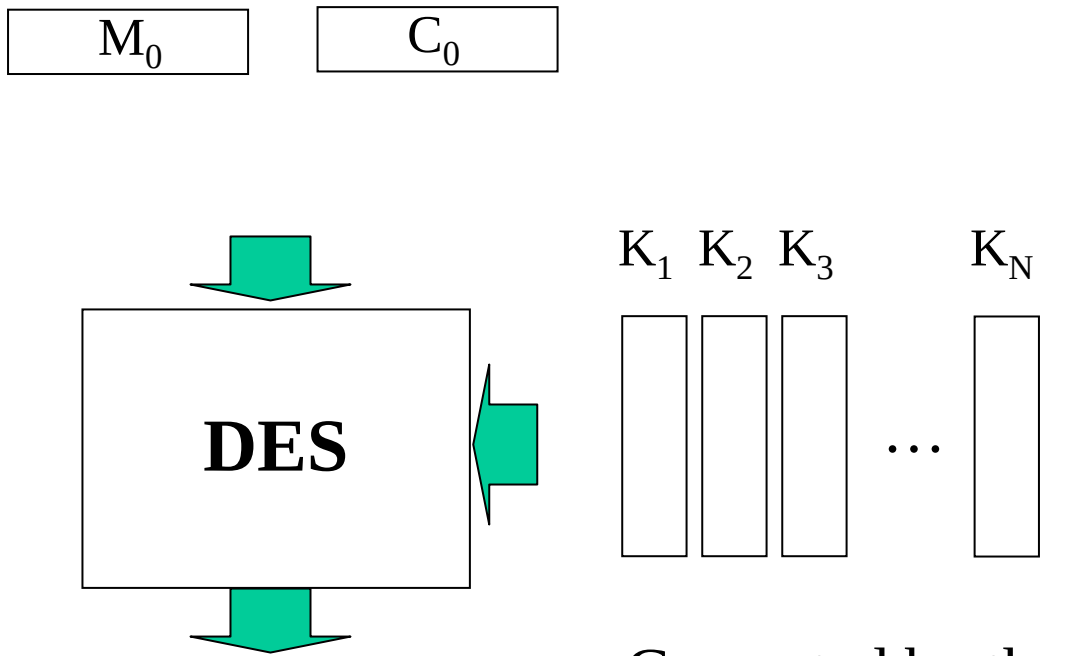
SRC-6E vs. Pentium 4 speed-up

	Non-Optimized P4 / MAP				Optimized P4 / MAP		
Length (Words)	Speedup (Total)	Speedup (Total w/o Config)	Speedup (MAP only)		Speedup (Total)	Speedup (Total w/o Config)	Speedup (MAP only)
1024	0.038	7.54	338.15		0.010	2.02	90.55
10000	0.366	27.62	362.75		0.101	7.61	99.99
25000	0.907	34.88	369.71		0.250	9.63	102.04
50000	1.775	37.88	372.01		0.487	10.40	102.11
100000	3.421	39.86	371.14		0.917	10.69	99.50
250000	7.485	41.29	367.82		2.073	11.43	101.87
500000	12.514	41.44	366.33		3.404	11.27	99.66

Application Case Study 2

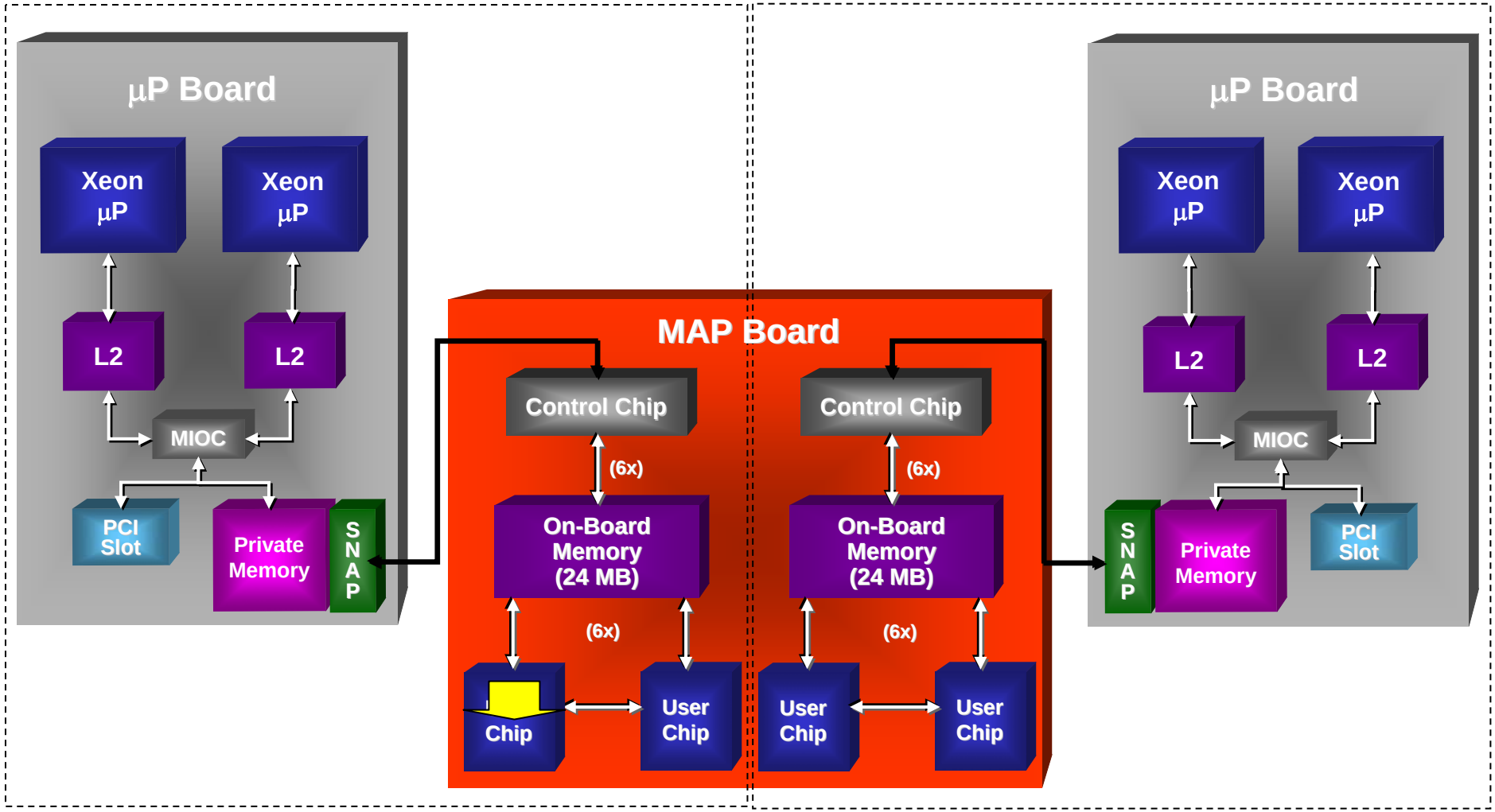
DES cipher breaking

Secret-key breaking

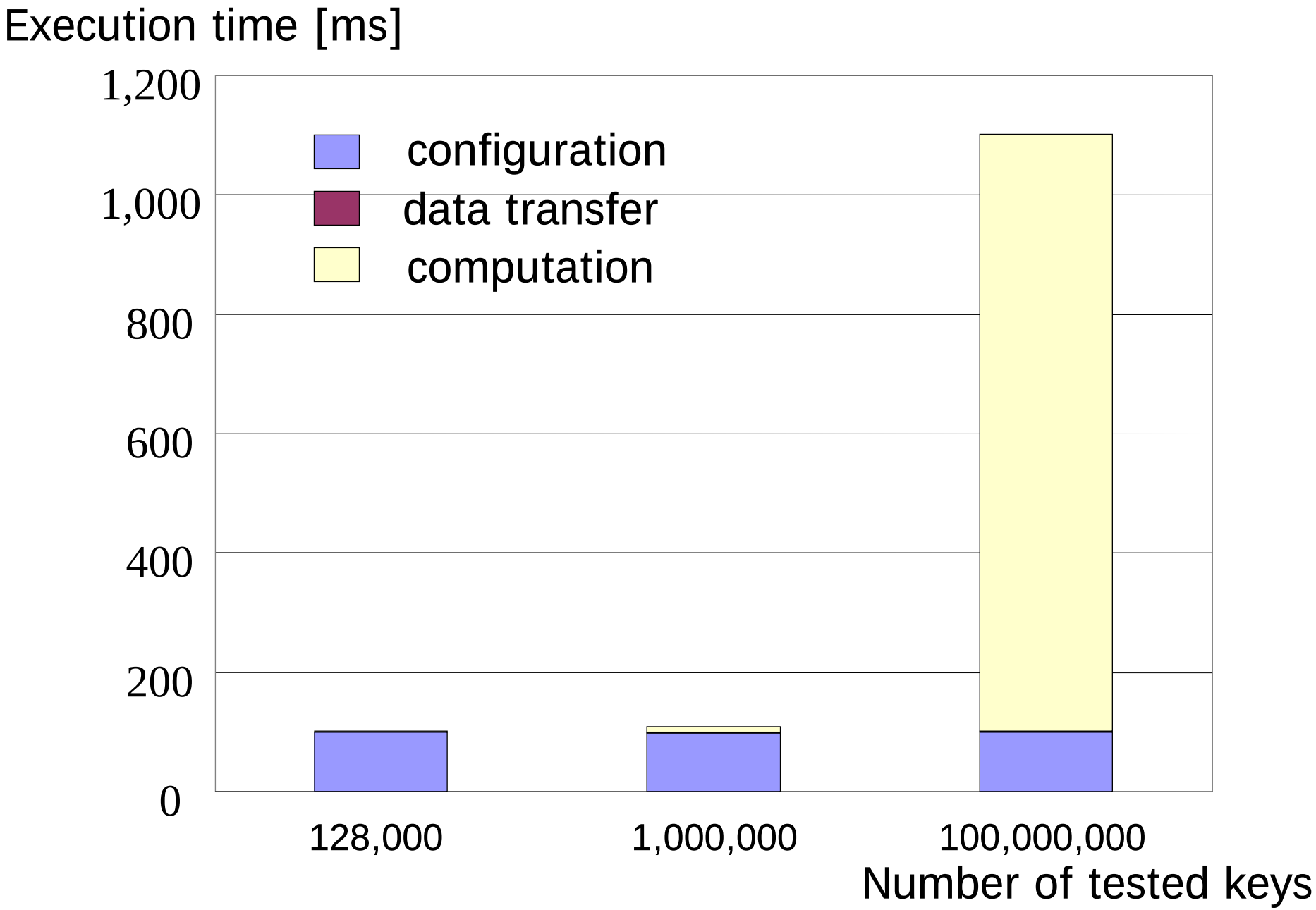


Generated by the DES breaker

Keys generated in the User FPGA



DES breaking machine



SRC-6e vs. Pentium 4 Speed-up

Number of DES units	Search Size (keys)	Speedup Total	Speedup w/o Config.	Speedup MAP only
1 X	128,000	2.5	157.4	194.0
	1,000,000	18.1	191.3	197.3
	100,000,000	180.2	198.3	198.4
2 X	128,000	2.5	265.1	387.8
	1,000,000	18.9	373.0	394.6
	100,000,000	329.4	396.3	396.8
4 X	128,000	2.5	406.7	774.6
	1,000,000	19.3	706.0	789.0
	100,000,000	563.0	792.6	793.6
8 X	128,000	2.6	500.0	1562.5
	1,000,000	20.1	1313.3	1576.0
	100,000,000	893.7	1583.4	1587.2

Conclusions

Two different classes of applications developed and tested for SRC-6E and Pentium 4 PC

- Triple DES encryption: real-time data streaming
- DES breaking: minimal input/output

Conclusions – cont.

Wall-clock speed-ups

3 DES Encryption

3.4 vs. P4 C code
12.5 vs. P4 assembly code

DES Breaking

894 vs. P4 C code
(larger for real-time input sizes)

Speed-ups without reconfiguration

3 DES Encryption

11 vs. P4 C code
41 vs. P4 assembly code

DES Breaking

1583 vs. P4 C code

Informal speed/cost comparison

$$\frac{\text{Cost of the SRC machine}}{\text{Cost of PC}} \approx 100$$

$$\frac{\text{Speed of the SRC machine}}{\text{Speed of PC}} \approx 1600^{*}$$

* with only one out of four FPGAs used in computations

16 x improved speed/cost ratio

Conclusions: Overheads

Reconfiguration time

Most affected applications:

short execution time, large resource requirements, frequent reconfiguration

Minimization techniques:

- **preloading configuration**
- **flip-flopping among multiple FPGAs**

Data transfer time

Most affected applications:

high speed real-time input/output

Minimization techniques:

- **overlapping data transfer with computations**