Ассоциация РусКрипто

РусКрипто 2009

2-5 Апреля 2009 г.

Графические карты как инструмент восстановления паролей

ELCOMSOFT
PROACTIVE SOFTWARE

Почему скорость имеет значение?

Обычные пользователи:
Пароль нужен «вчера»…

Аудит и pentest:
Время = деньги

Графический процессор

намного быстрее

центрального процессора

Почему?

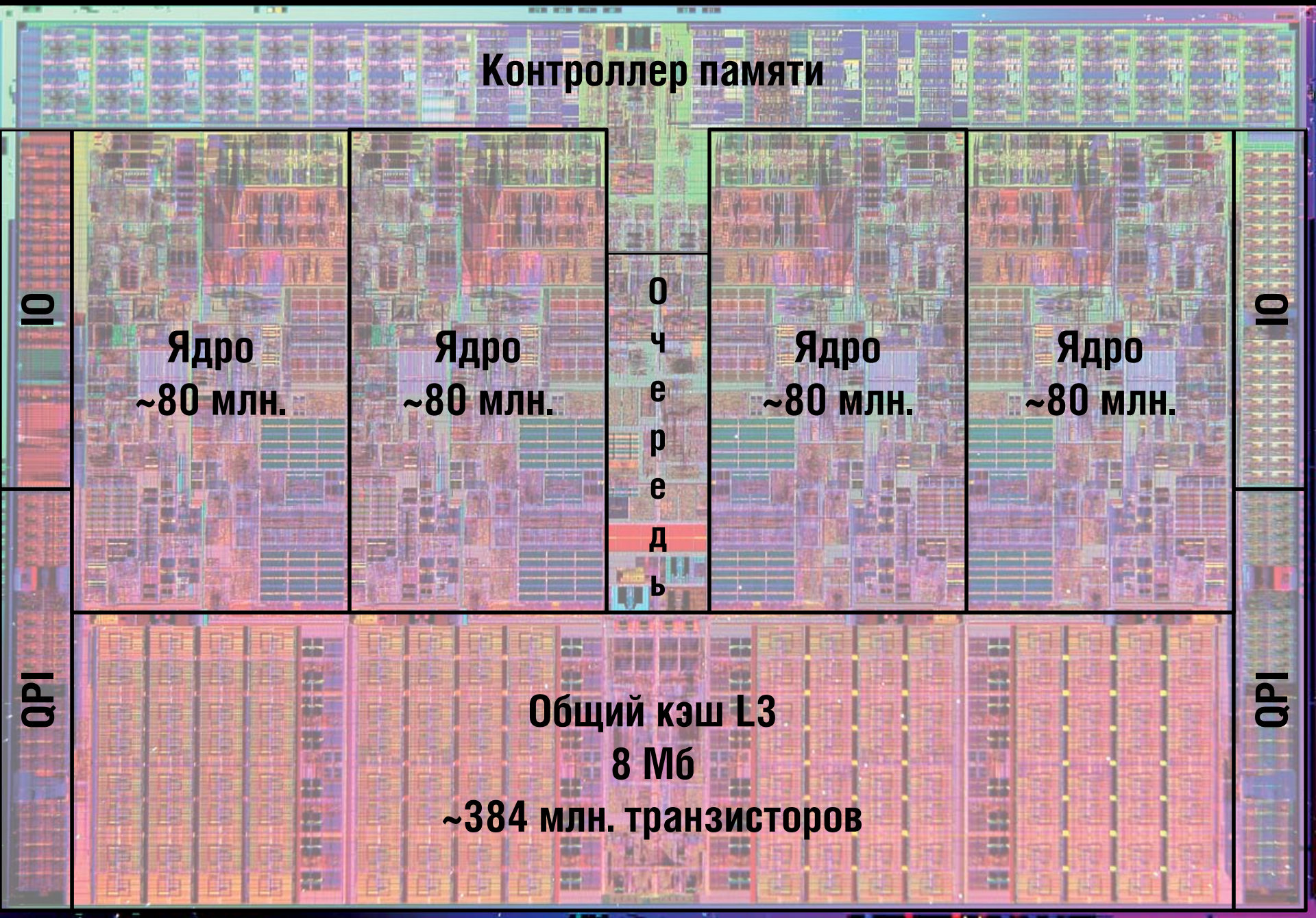
ЦП «заточен» под последовательные вычисления

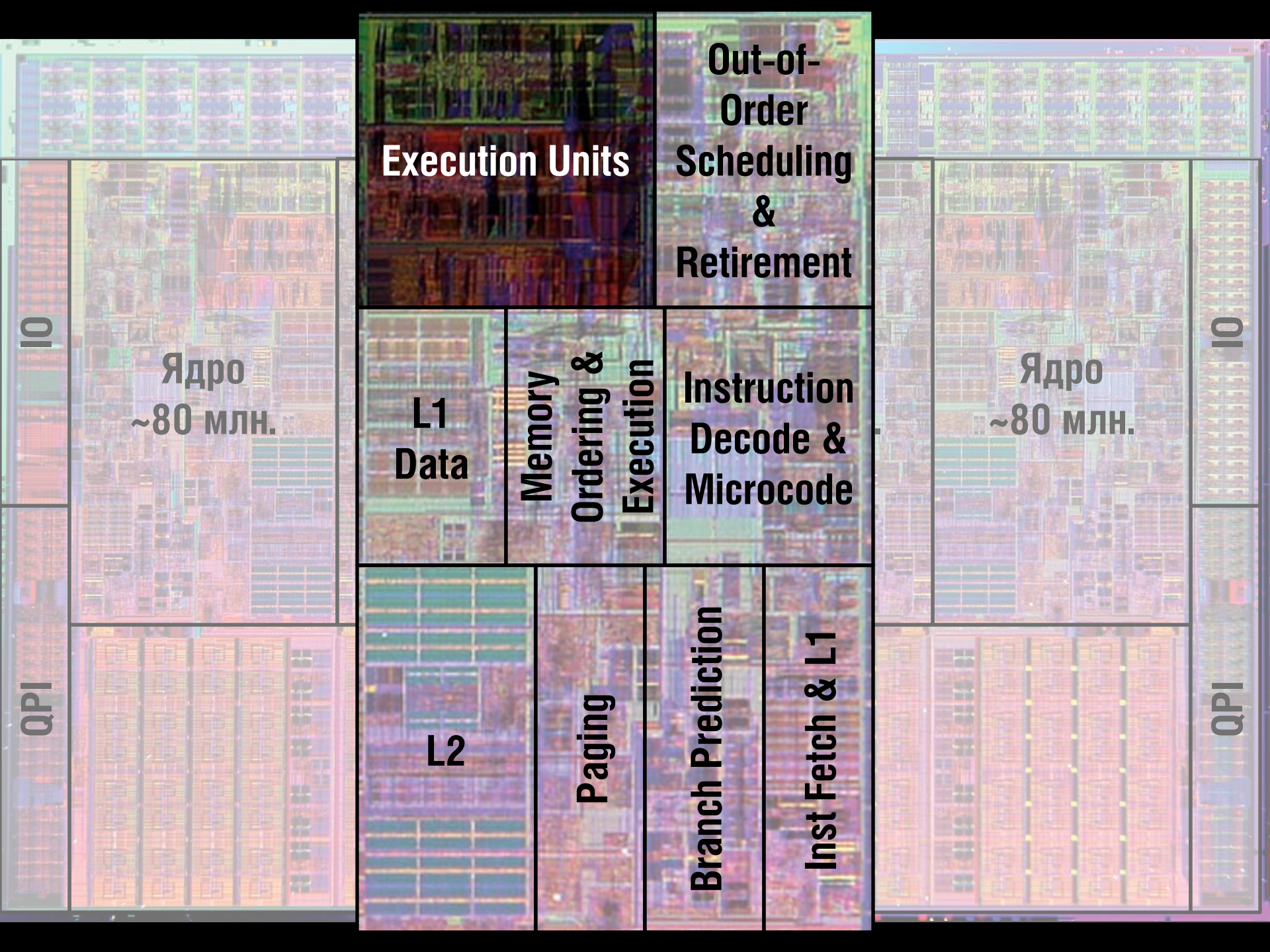
а ГП «заточен» под параллельные

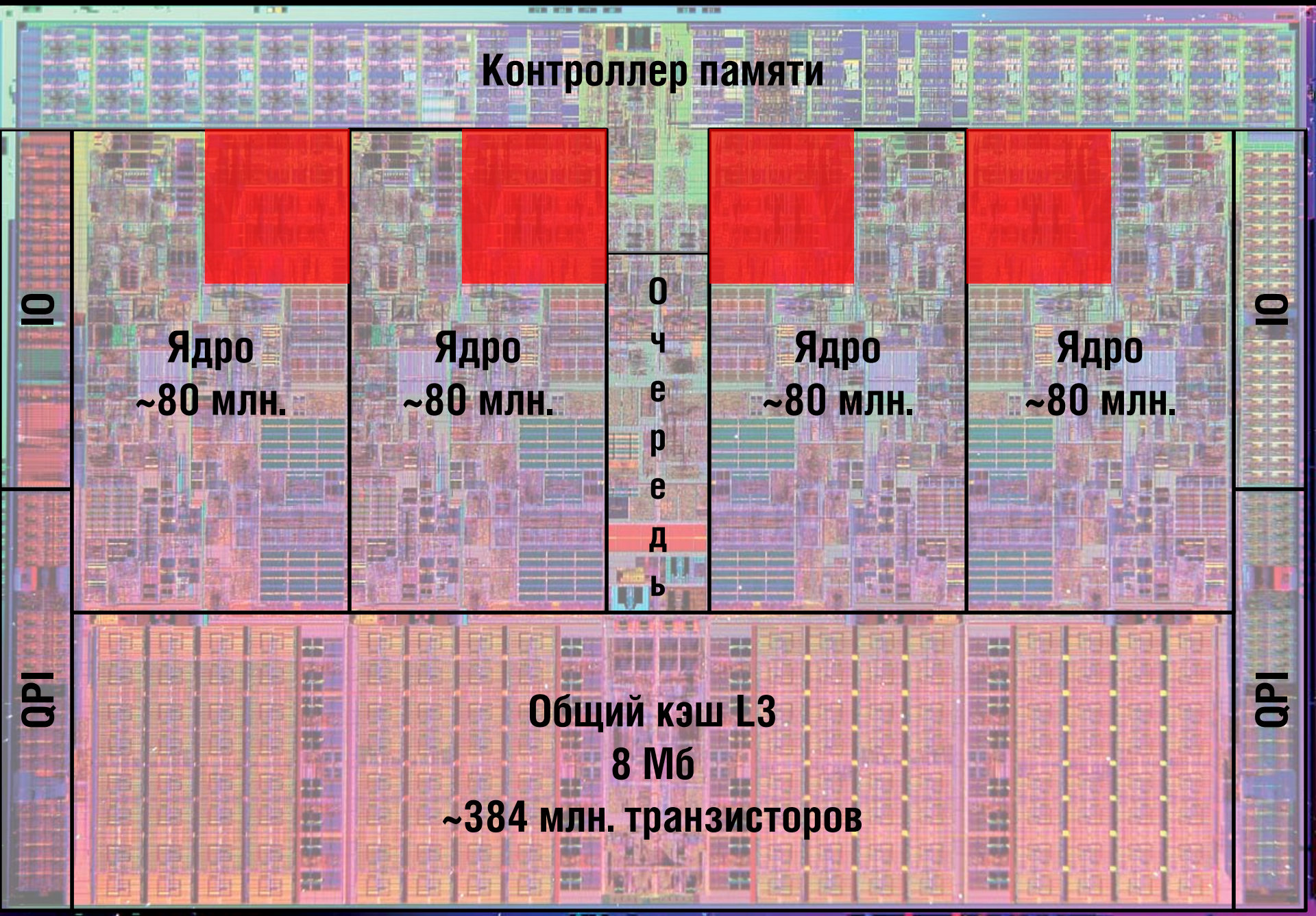
Intel® Core™ i7-965

“Самый производительный процессор для настольных ПК на планете.”

4 ядра
3,2 ГГц
731 млн. транзисторов
263 мм^2


Контроллер памяти
IO
Ядро
~80 млн.
Ядро
~80 млн.
Очередь
Ядро
~80 млн.
Ядро
~80 млн.
IO
QPI
Общий кэш L3
8 Мб
~384 млн. транзисторов
QPI

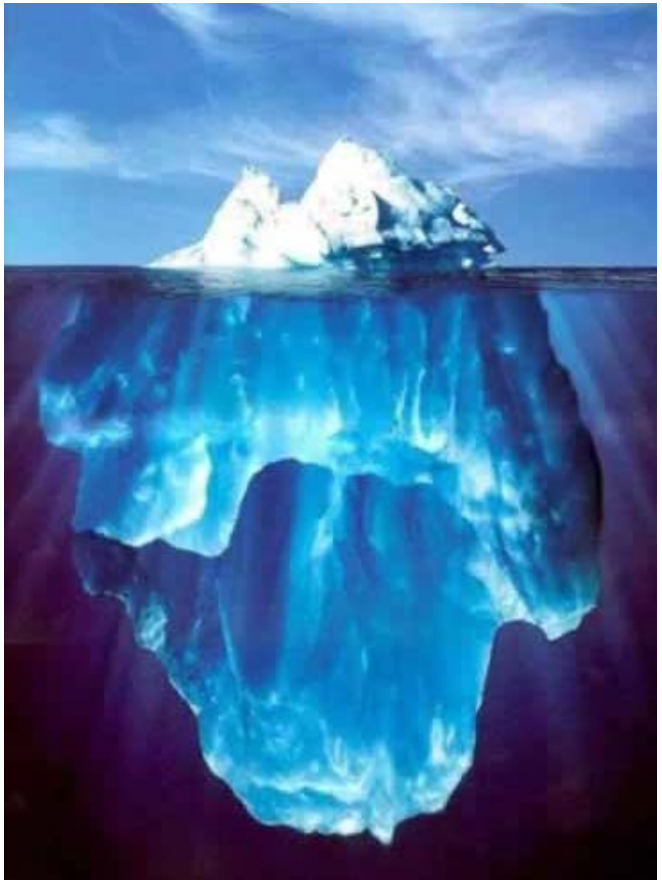

Execution Units
Out-of-Order Scheduling & Retirement
L1 Data
Memory Ordering & Execution
Instruction Decode & Microcode
L2
Paging
Branch Prediction
Inst Fetch & L1
Ядро ~80 млн.
Ядро ~80 млн.
IO
IO
QPI
QPI


Контроллер памяти
IO
Ядро
~80 млн.
Ядро
~80 млн.
Очередь
Ядро
~80 млн.
Ядро
~80 млн.
IO
QPI
Общий кэш L3
8 Мб
~384 млн. транзисторов
QPI

Исполнительные устройства занимают около **10%** процессора!

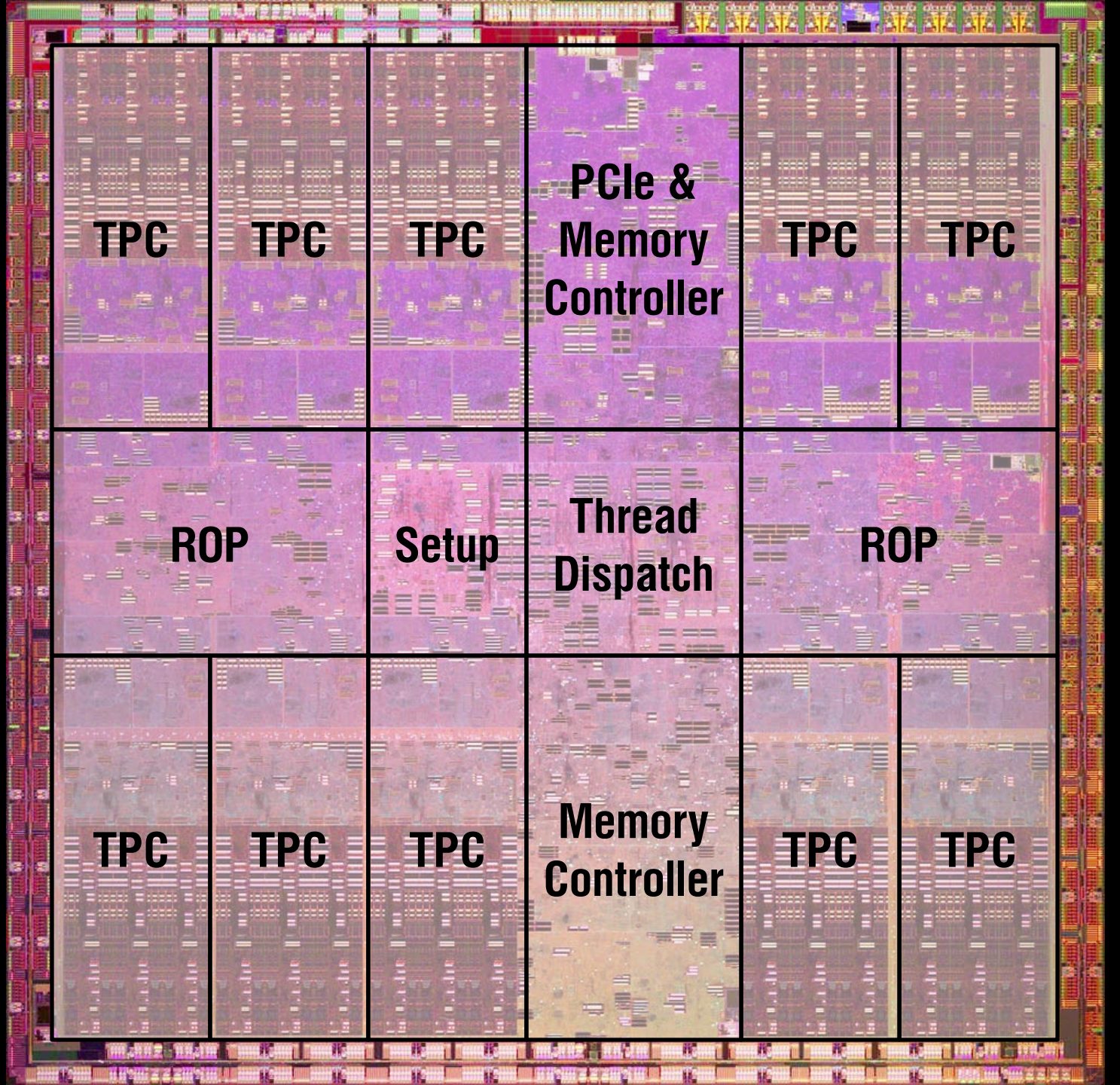
1/10

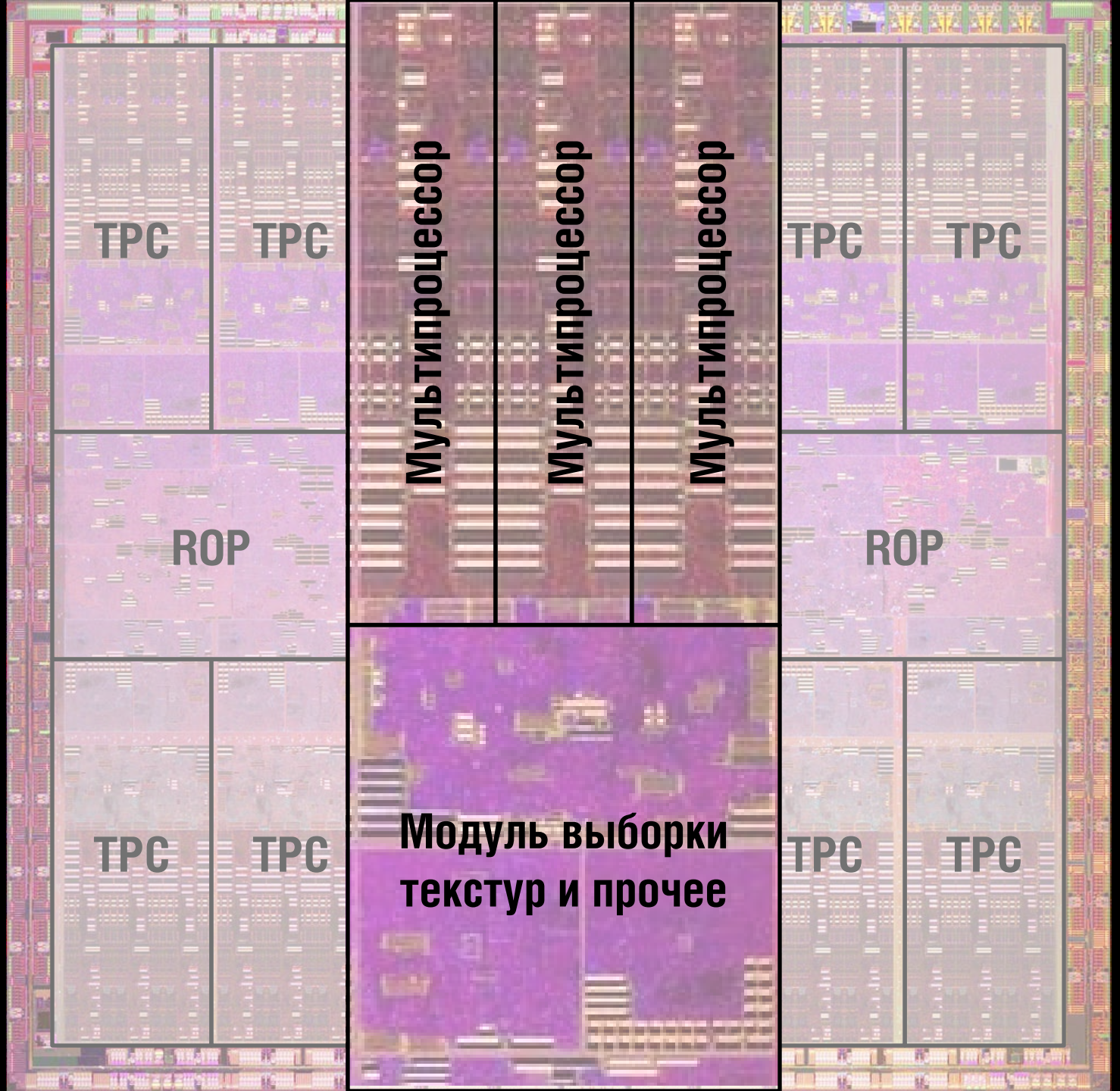
Исполнительные устройства занимают около **10%** процессора!

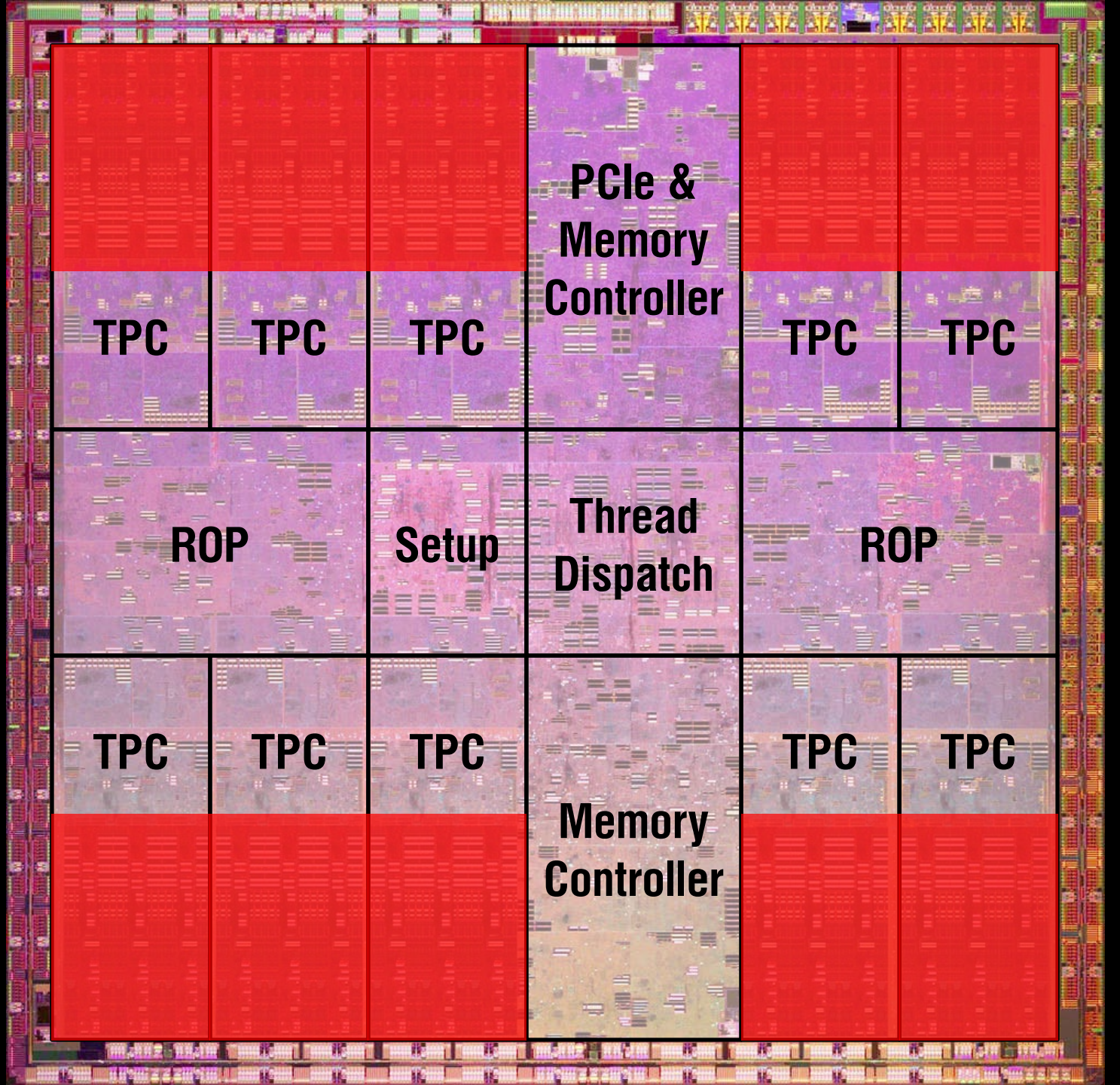


NVIDIA®
GeForce® GTX 285

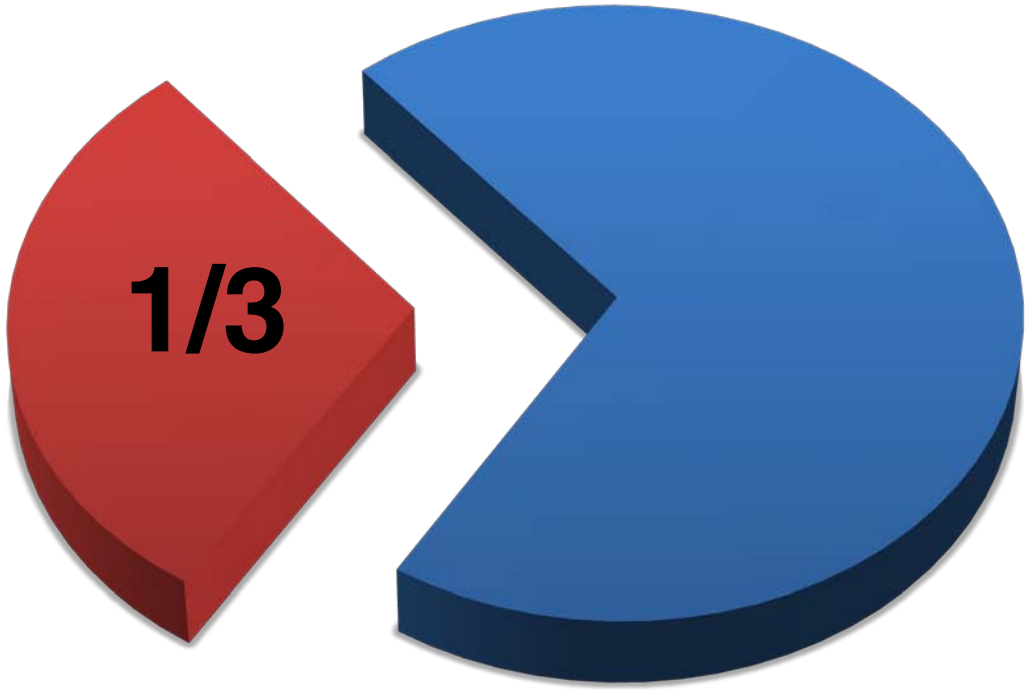
240 ядер
1,476 ГГц
1,4 млрд. транзисторов
470 мм^2


TPC
TPC
TPC
PCIe &
Memory
Controller
TPC
TPC
ROP
Setup
Thread
Dispatch
ROP
TPC
TPC
TPC
Memory
Controller
TPC
TPC

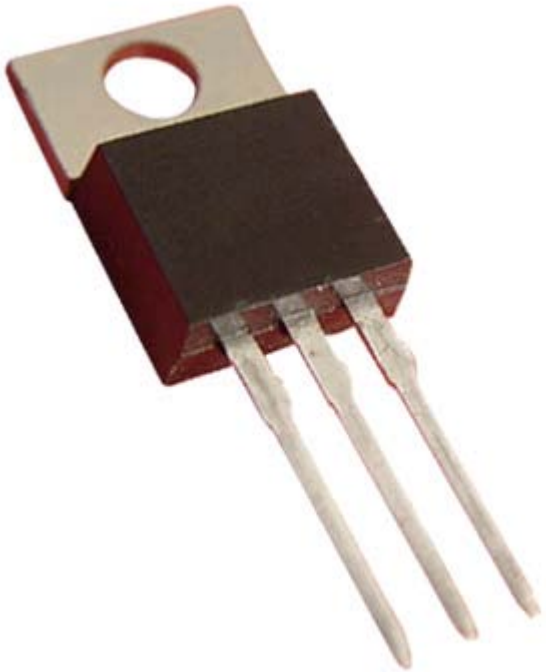

TPC
TPC
TPC
TPC
ROP
ROP
Мультипроцессор
Мультипроцессор
Мультипроцессор
TPC
TPC
TPC
TPC
Модуль выборки текстур и прочее


PCIe &
Memory
Controller
TPC
TPC
TPC
TPC
TPC
ROP
Setup
Thread
Dispatch
ROP
TPC
TPC
TPC
TPC
TPC
Memory
Controller

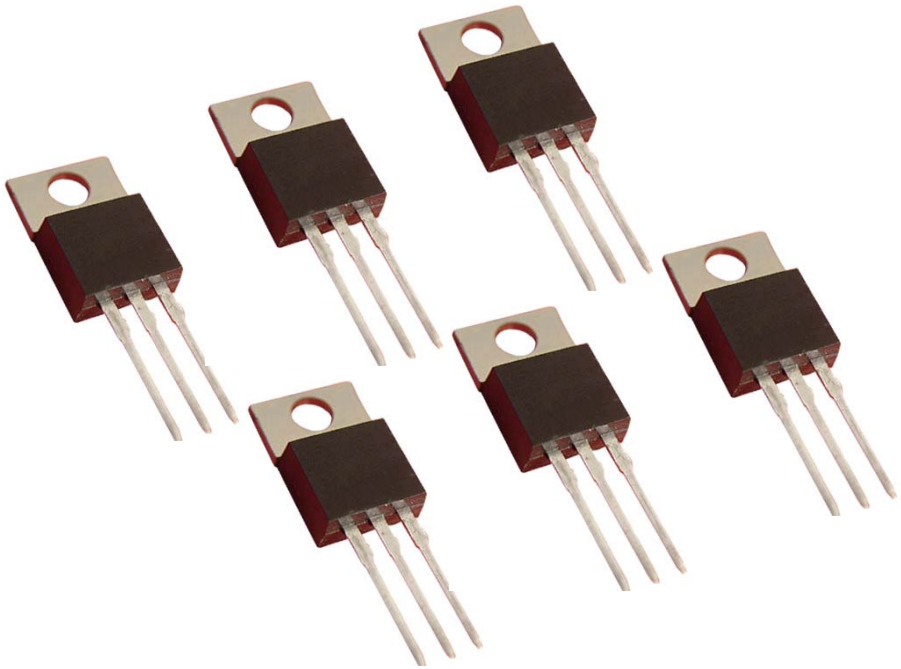
Исполнительные устройства занимают около **30%** процессора!

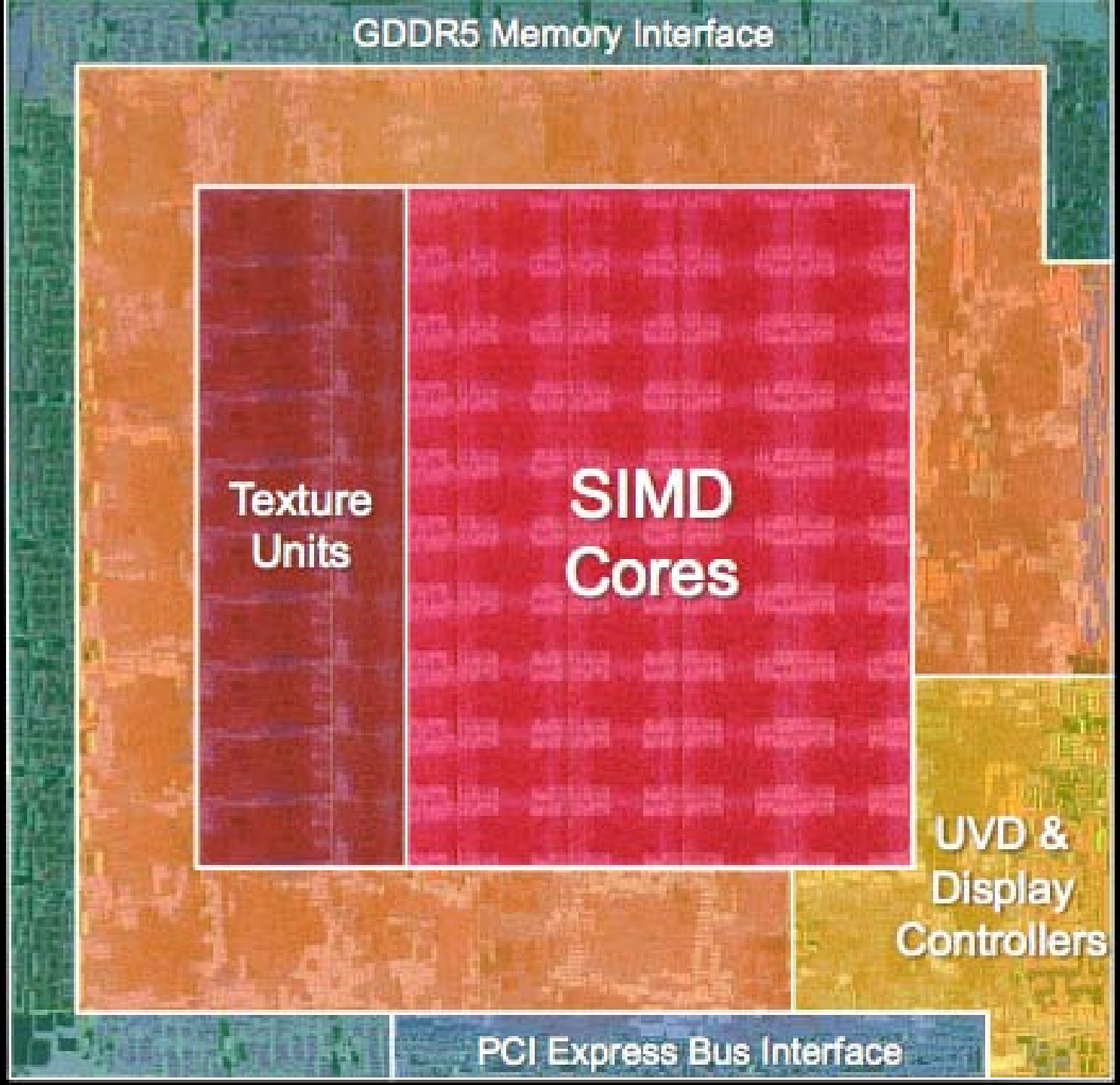


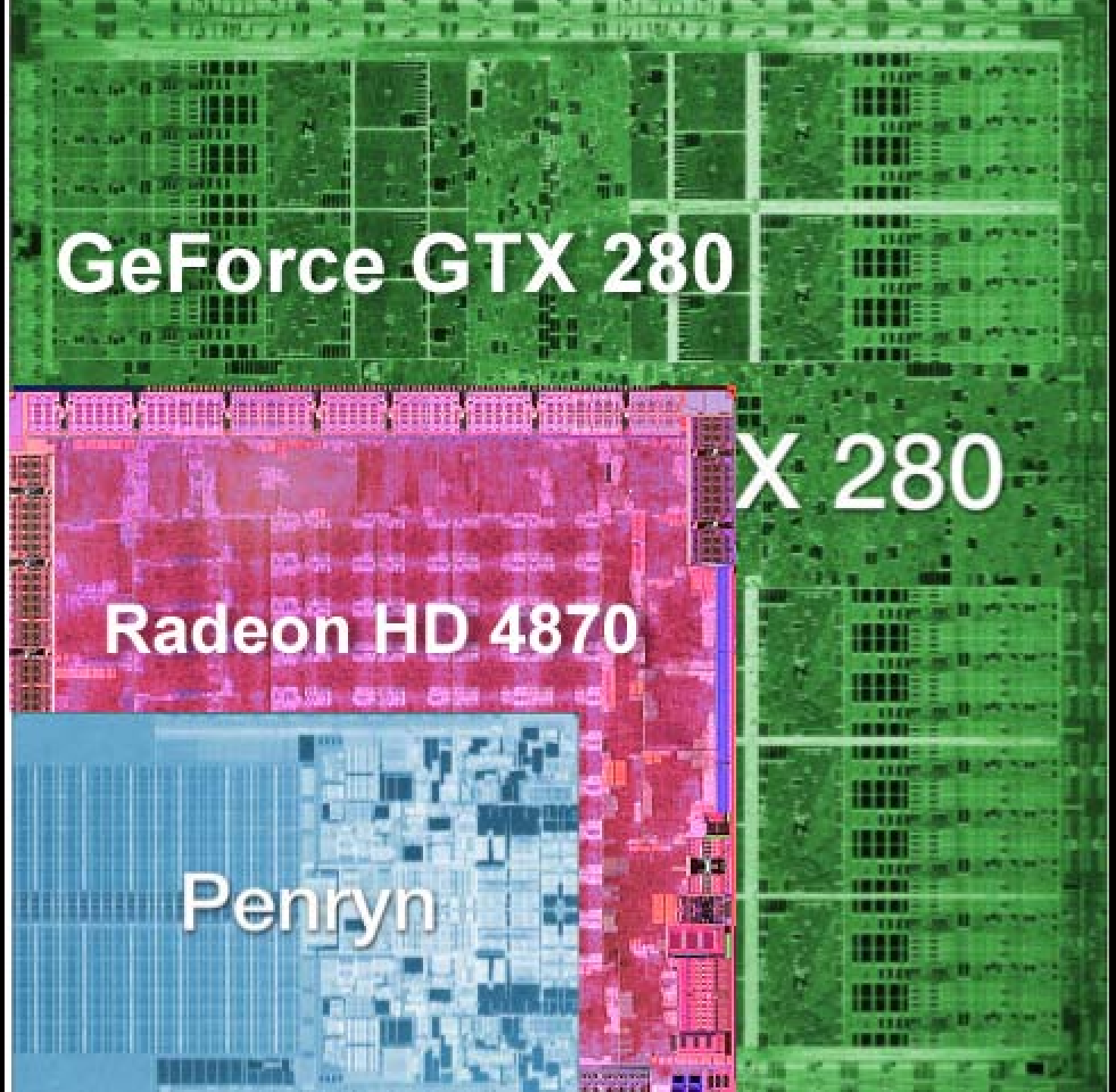
Исполнительным устройствам в ГП отведено **в 6 раз** больше ресурсов!



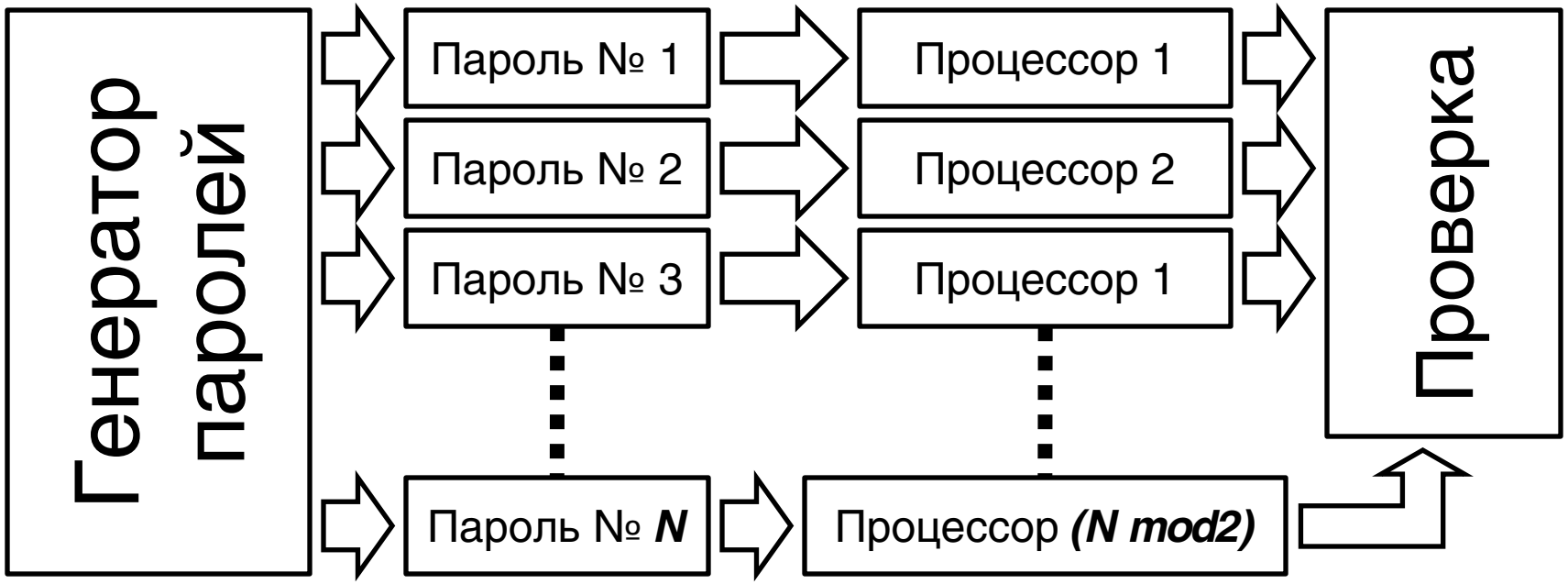
Исполнительным устройствам в ГП отведено **в 6 раз** больше ресурсов!



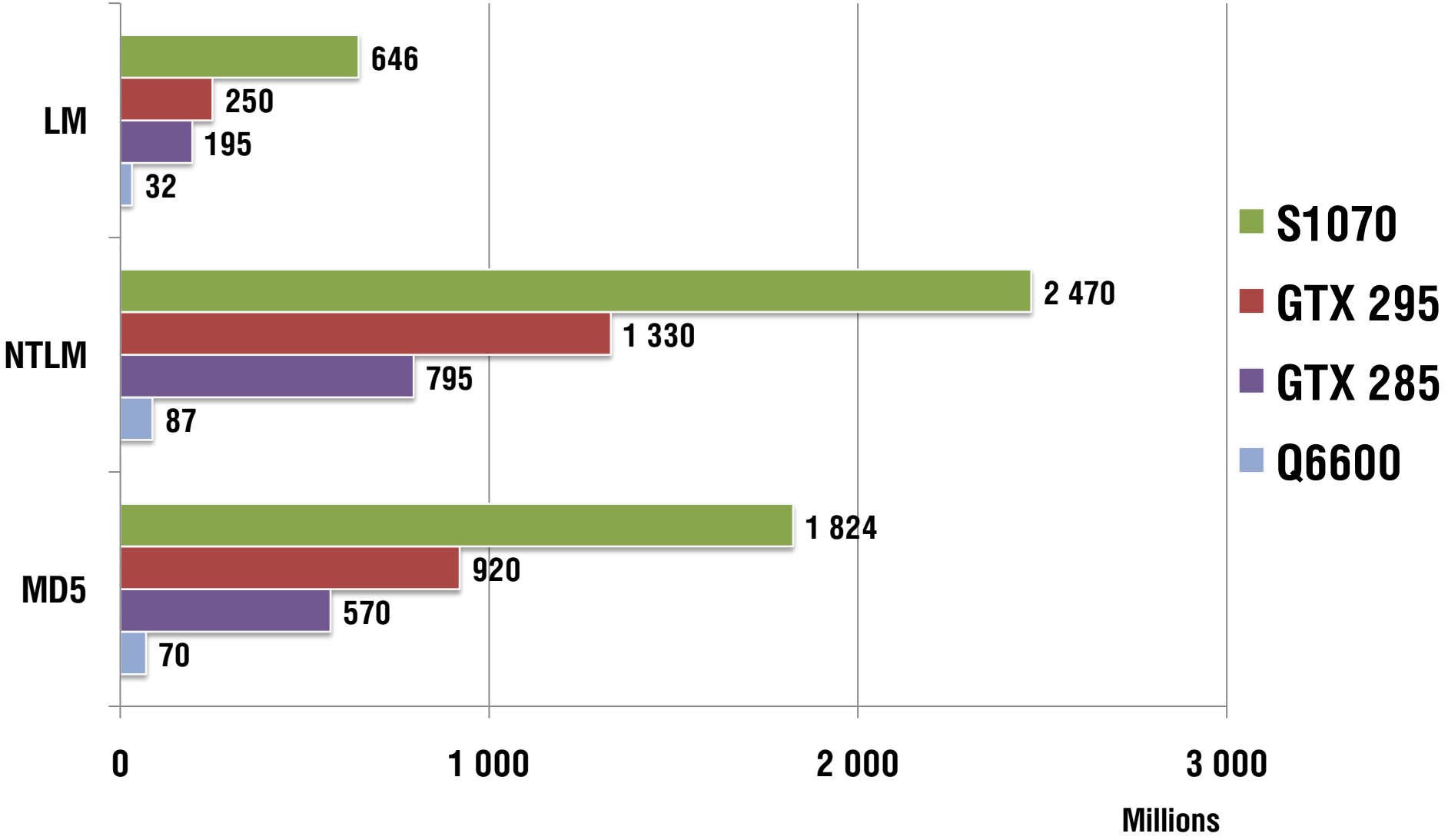

GDDR5 Memory Interface
Texture Units
SIMD Cores
UVD & Display Controllers
PCI Express Bus Interface


GeForce GTX 280
X 280
Radeon HD 4870
Penryn

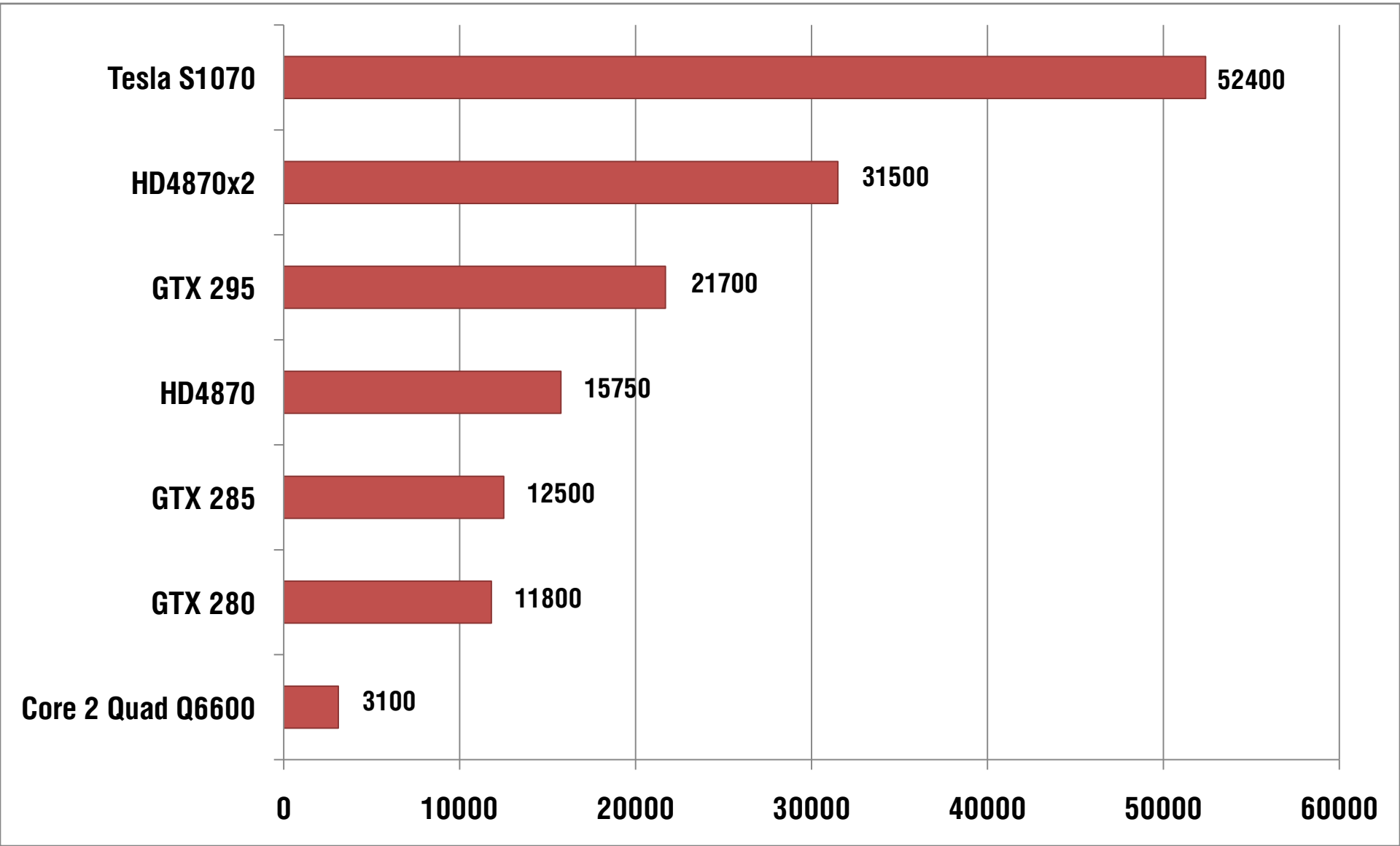
Перебор паролей распараллеливается тривиально



Результаты


LM
646
250
195
32
NTLM
2 470
1 330
795
87
MD5
1 824
920
570
70
S1070
GTX 295
GTX 285
Q6600
0
1 000
2 000
3 000
Millions

Результаты


Tesla S1070
52400
HD4870x2
31500
GTX 295
21700
HD4870
15750
GTX 285
12500
GTX 280
11800
Core 2 Quad Q6600
3100
0
10000
20000
30000
40000
50000
60000

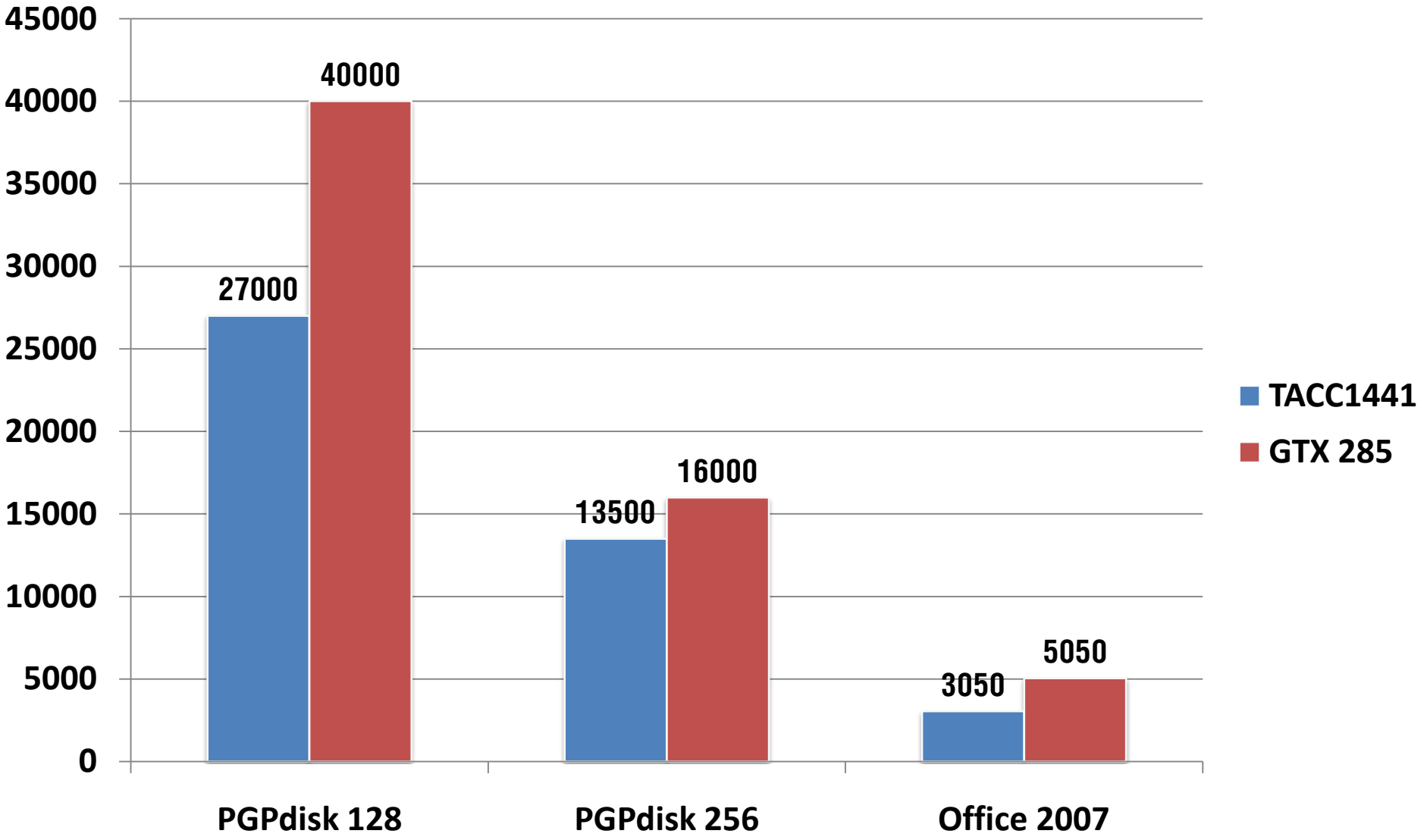
Альтернативы?

Tableau TACC1441

Реализован на ПЛИС (Xilinx)
FireWire
Закрытый SDK

US $3’995

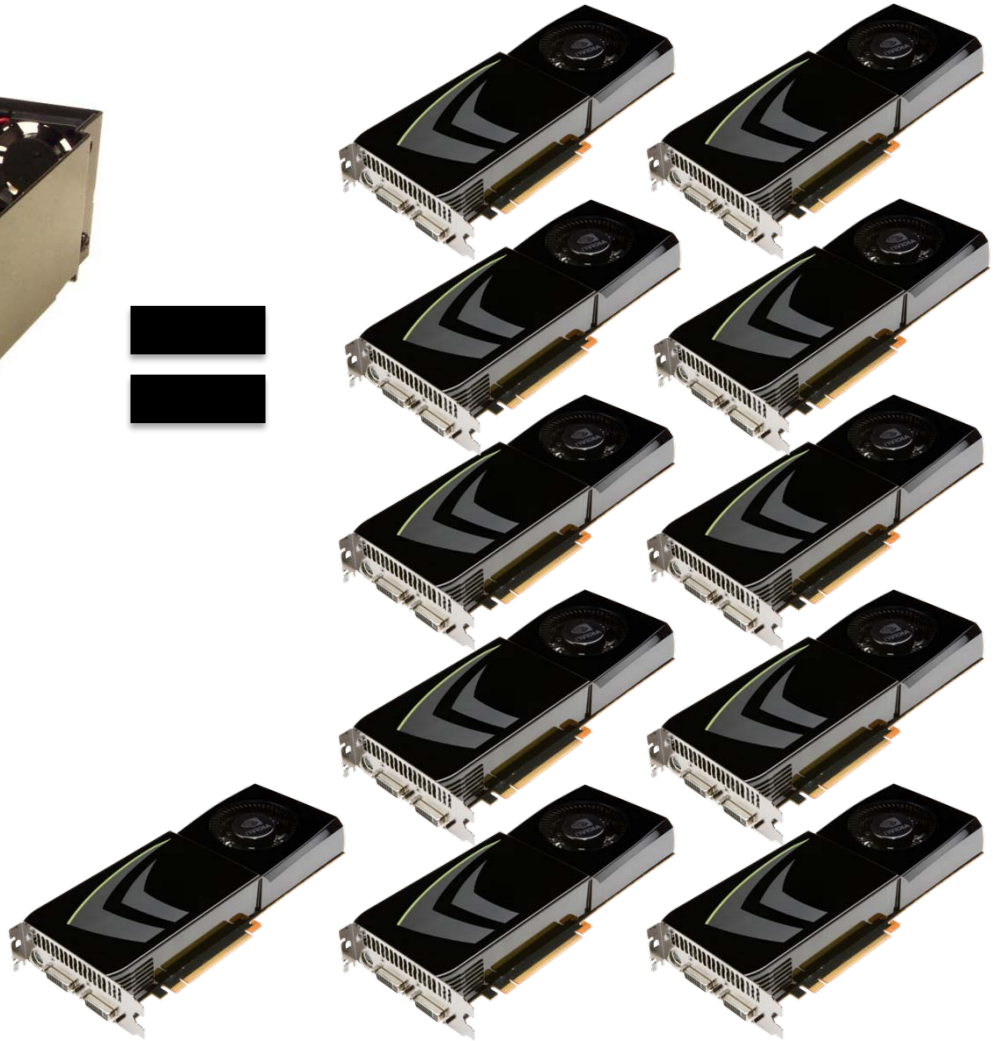
Сравнение


45000
40000
35000
30000
25000
20000
15000
10000
5000
0
40000
27000
16000
13500
5050
3050
PGPdisk 128
PGPdisk 256
Office 2007
TACC1441
GTX 285

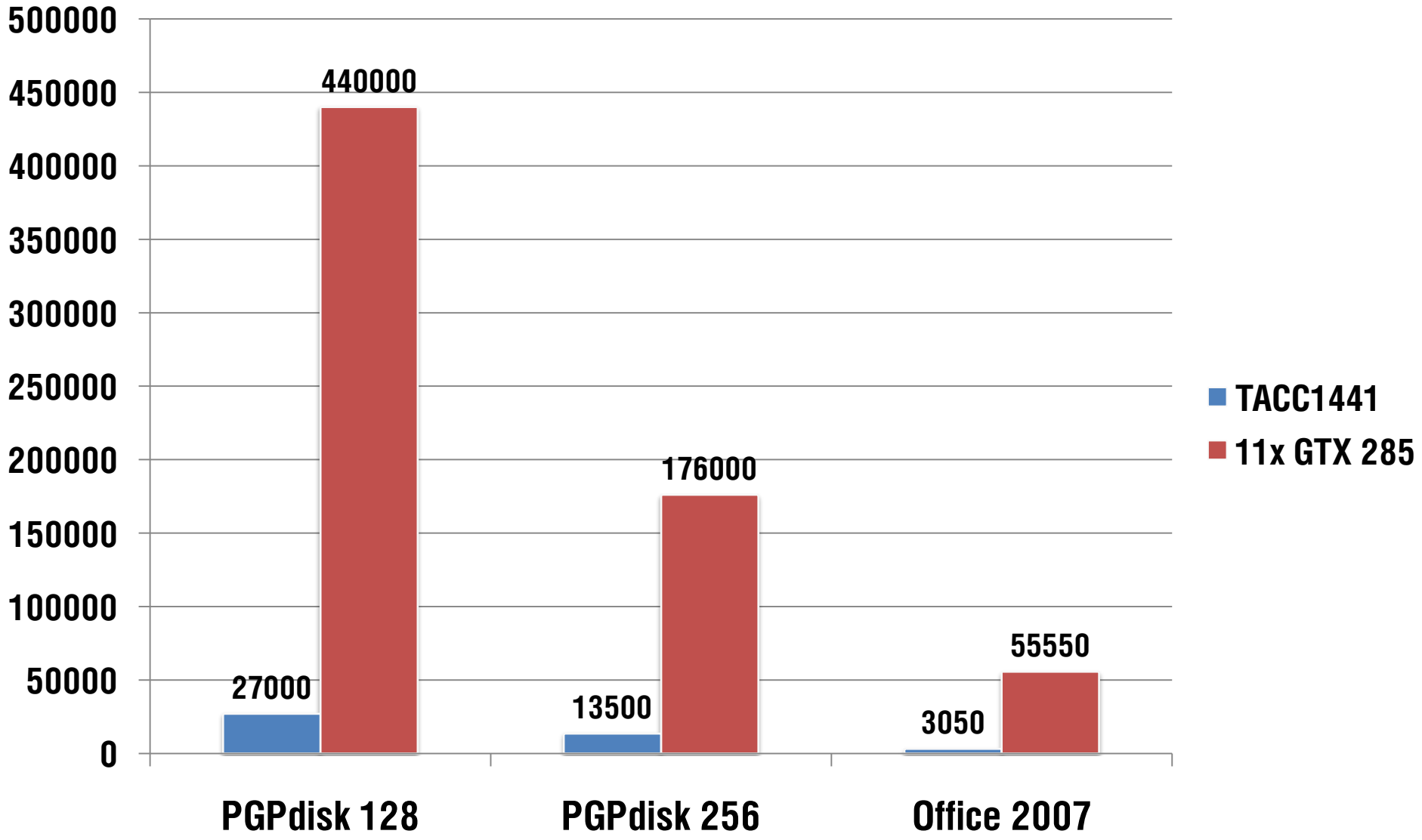
Сравнение


TABLEAU
Menu
Enter
Hardware Accelerator
Model TACC1441
Power
Host Det
Busy

=



Сравнение


500000
450000
400000
350000
300000
250000
200000
150000
100000
50000
0
440000
27000
176000
13500
55550
3050
PGPdisk 128
PGPdisk 256
Office 2007
TACC1441
11x GTX 285

Спасибо!

Андрей Беленко
a.belenko@elcomsoft.com