TROOPERS 09

get skilled, or get owned

GPU-Assisted Password Cracking

ELCOMSOFT
PROACTIVE SOFTWARE

Who may need Password Recovery?

- Ordinary users (own passwords)
- IT Departments (employee's passwords)
- Security auditors, consultants and penetration testers
- Law enforcement & government

- **Hackers usually don't!**

Why speed counts?

Users and IT Departments:
«We needed those passwords yesterday»

Auditors, consultants and pentesters:
«Time is Money»

How to increase speed?

Traditional way is to network together many computers to form a cluster

- Communication overhead
- Difficult to manage
- Not power-efficient

Any other options?

Yes!

For many HPC applications GPUs **are many times faster** than CPUs

But they're not only faster, they are **greener**!

Why?

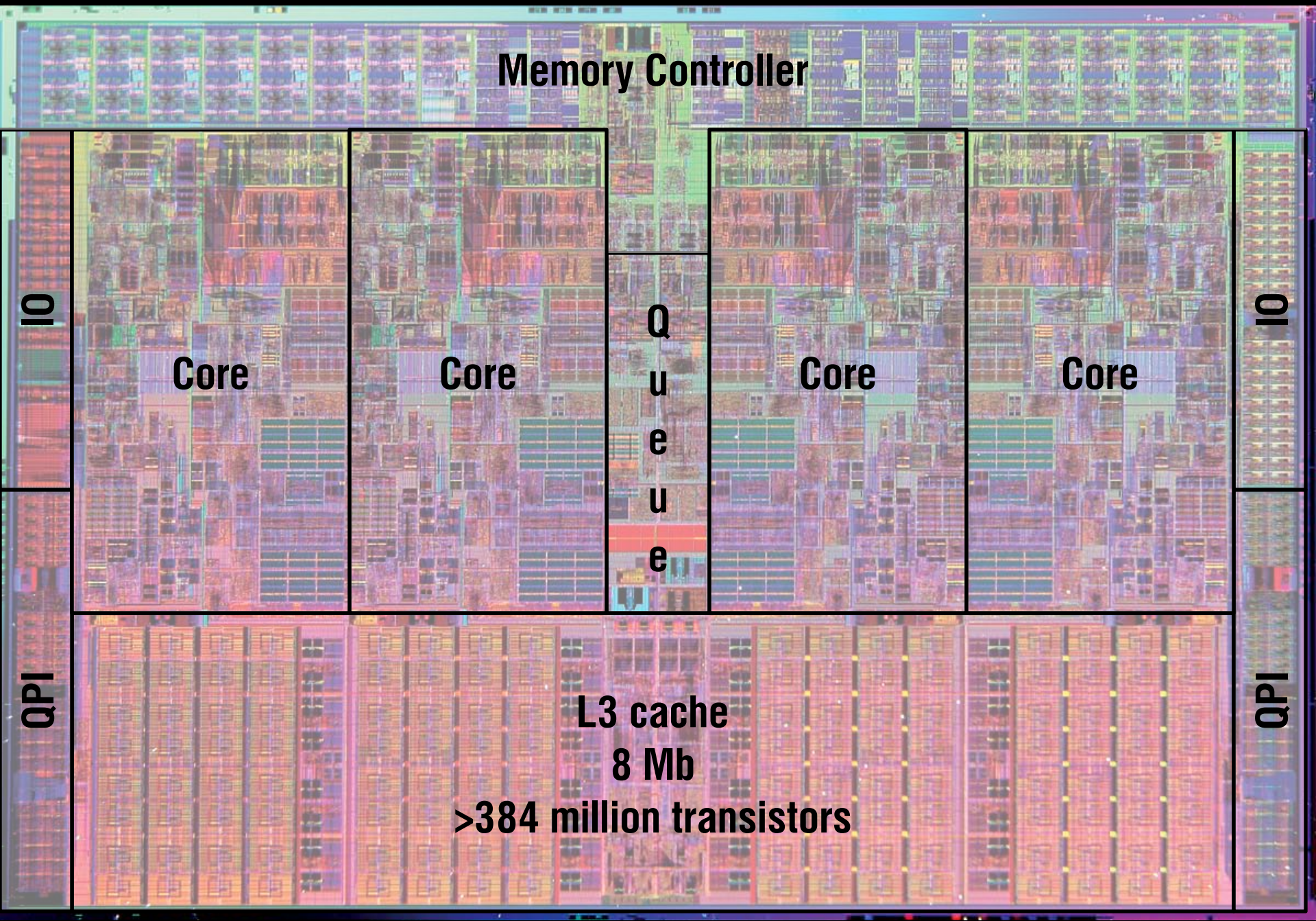
CPUs are designed to be efficient at serial computing…

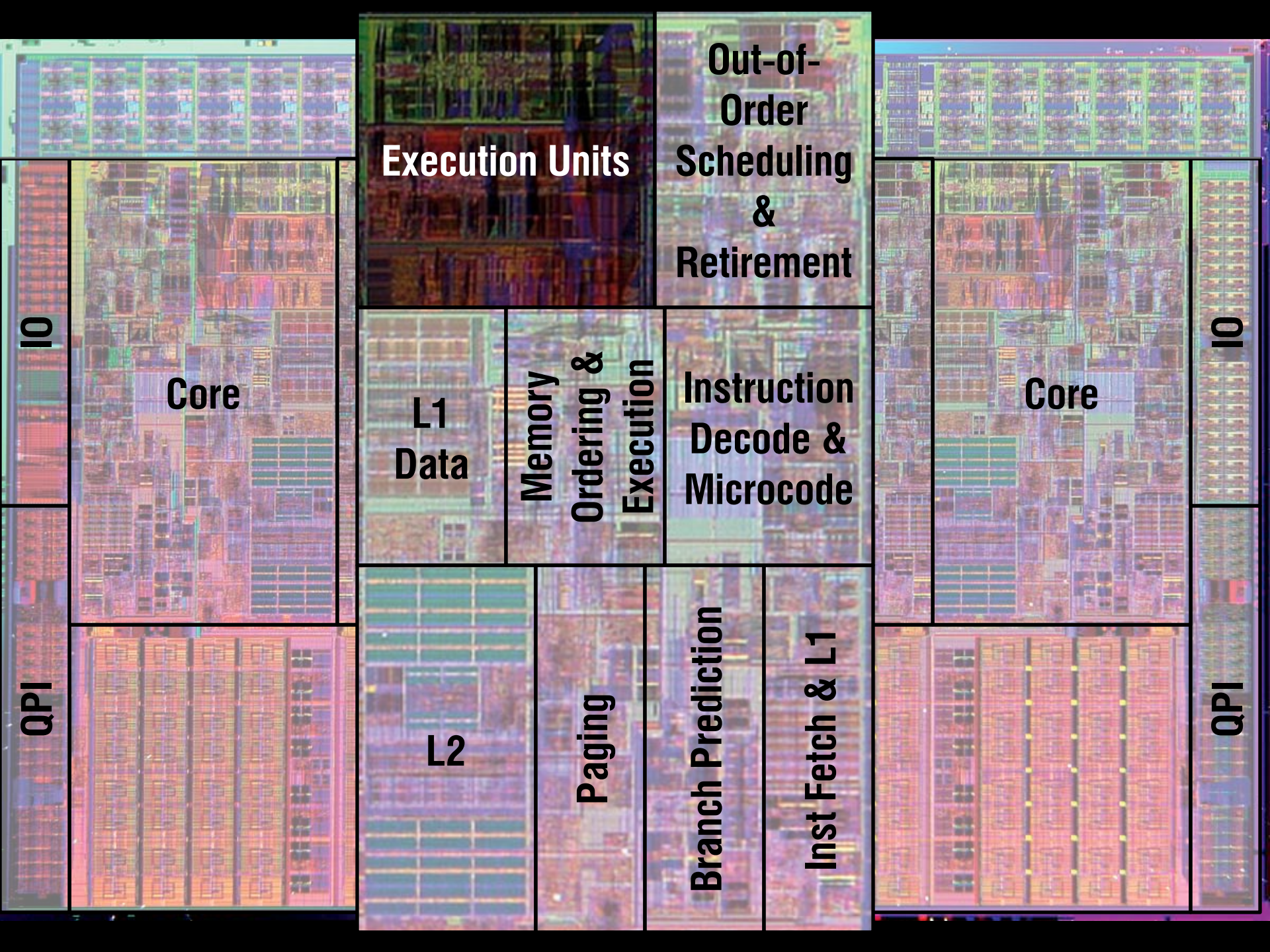
…while GPU's main concern is parallel computing

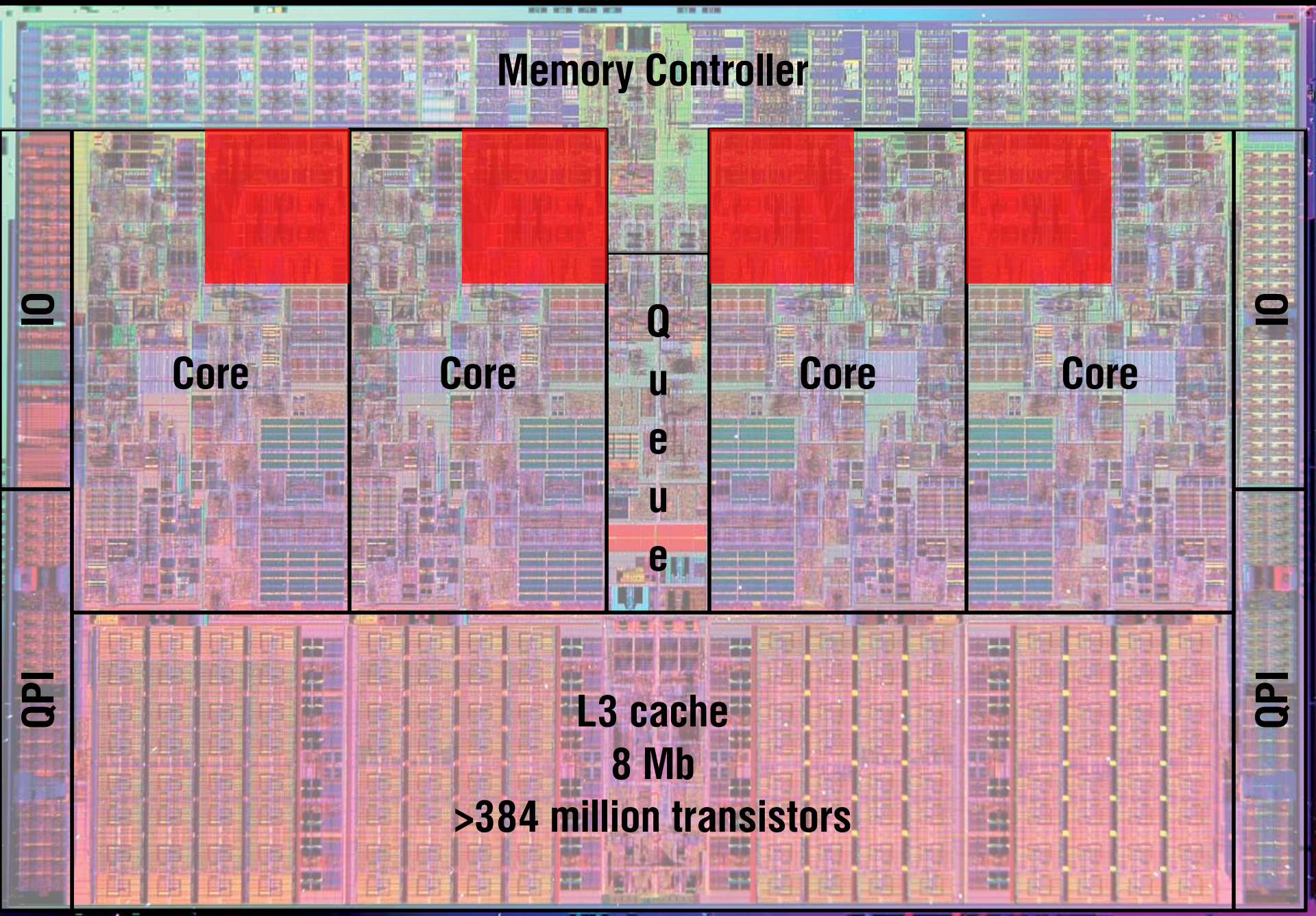
Intel® Core™ i7-965

"The highest performing desktop processor on the planet."

4 cores
3,2 GHz
731 million transistors
263 mm^2


Memory Controller
IO
Core
Core
Q
u
e
u
e
Core
Core
IO
QPI
L3 cache
8 Mb
>384 million transistors
QPI

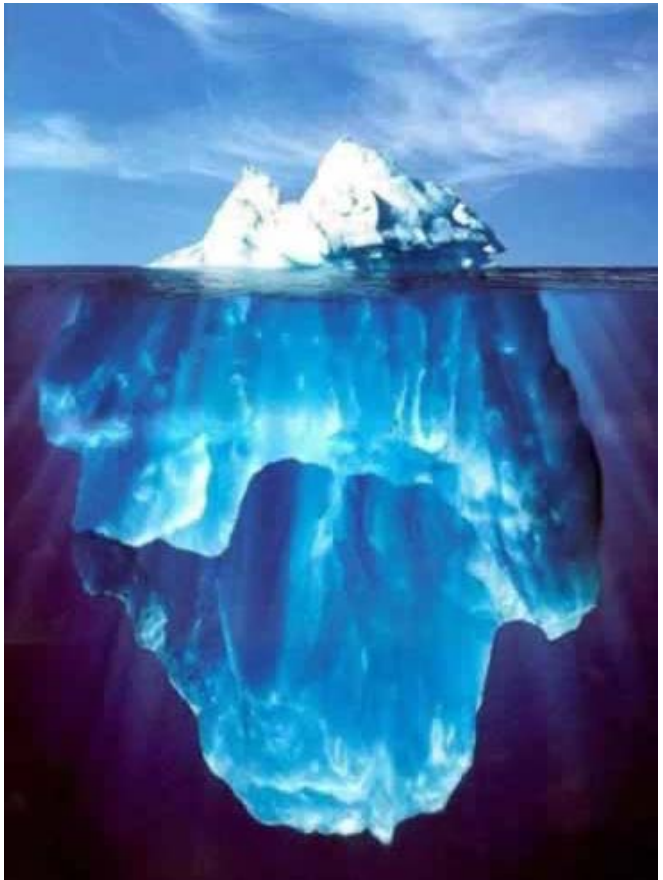

Execution Units
Out-of-Order Scheduling & Retirement
IO
Core
L1 Data
Memory Ordering & Execution
Instruction Decode & Microcode
Core
IO
QPI
L2
Paging
Branch Prediction
Inst Fetch & L1
QPI


Memory Controller
IO
Core
Core
Q
u
e
u
e
Core
Core
IO
QPI
L3 cache
8 Mb
>384 million transistors
QPI

CPU dedicates only about **10%** to the execution units!

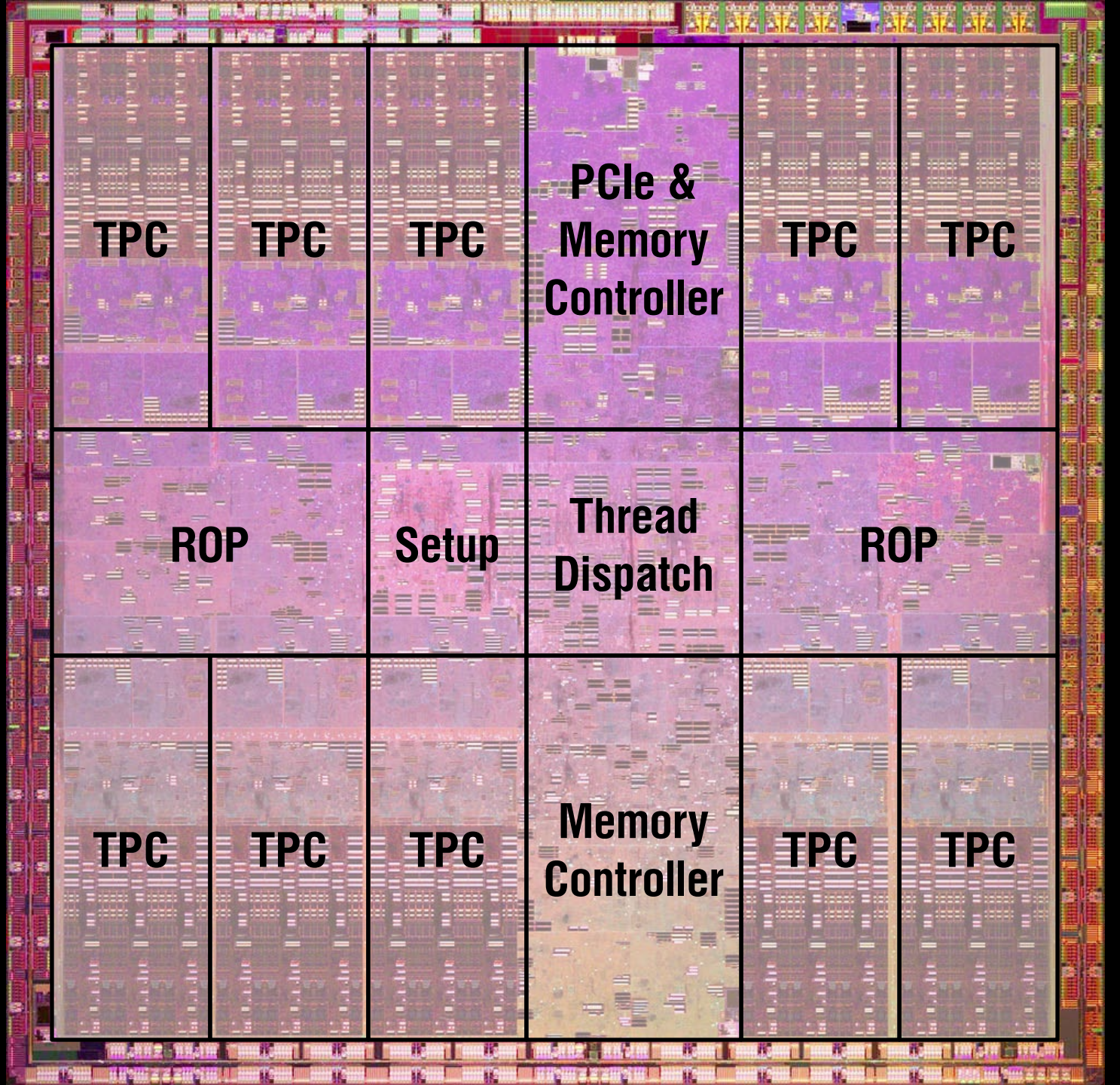
1/10

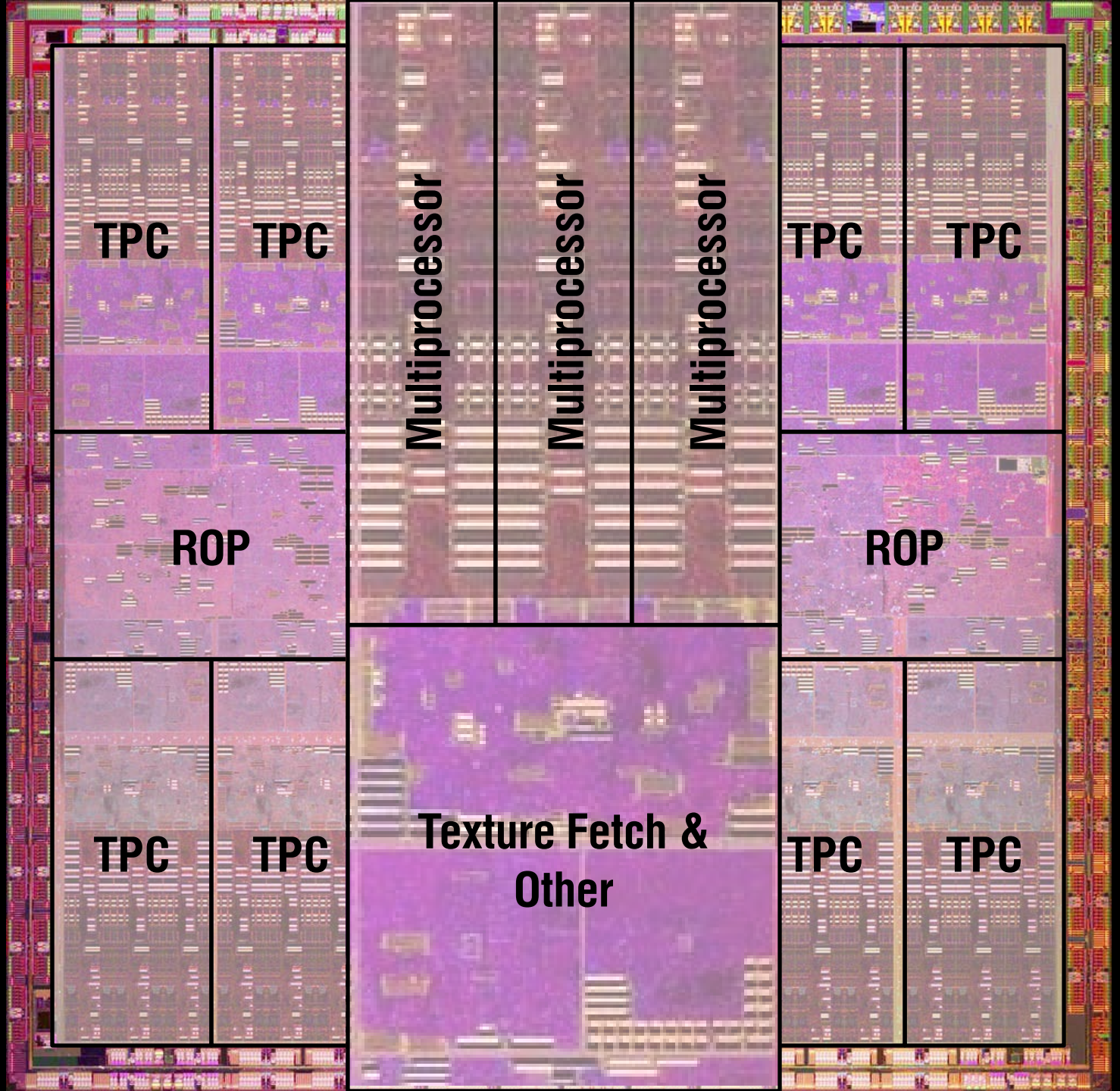
CPU dedicates only about **10%** to the execution units!

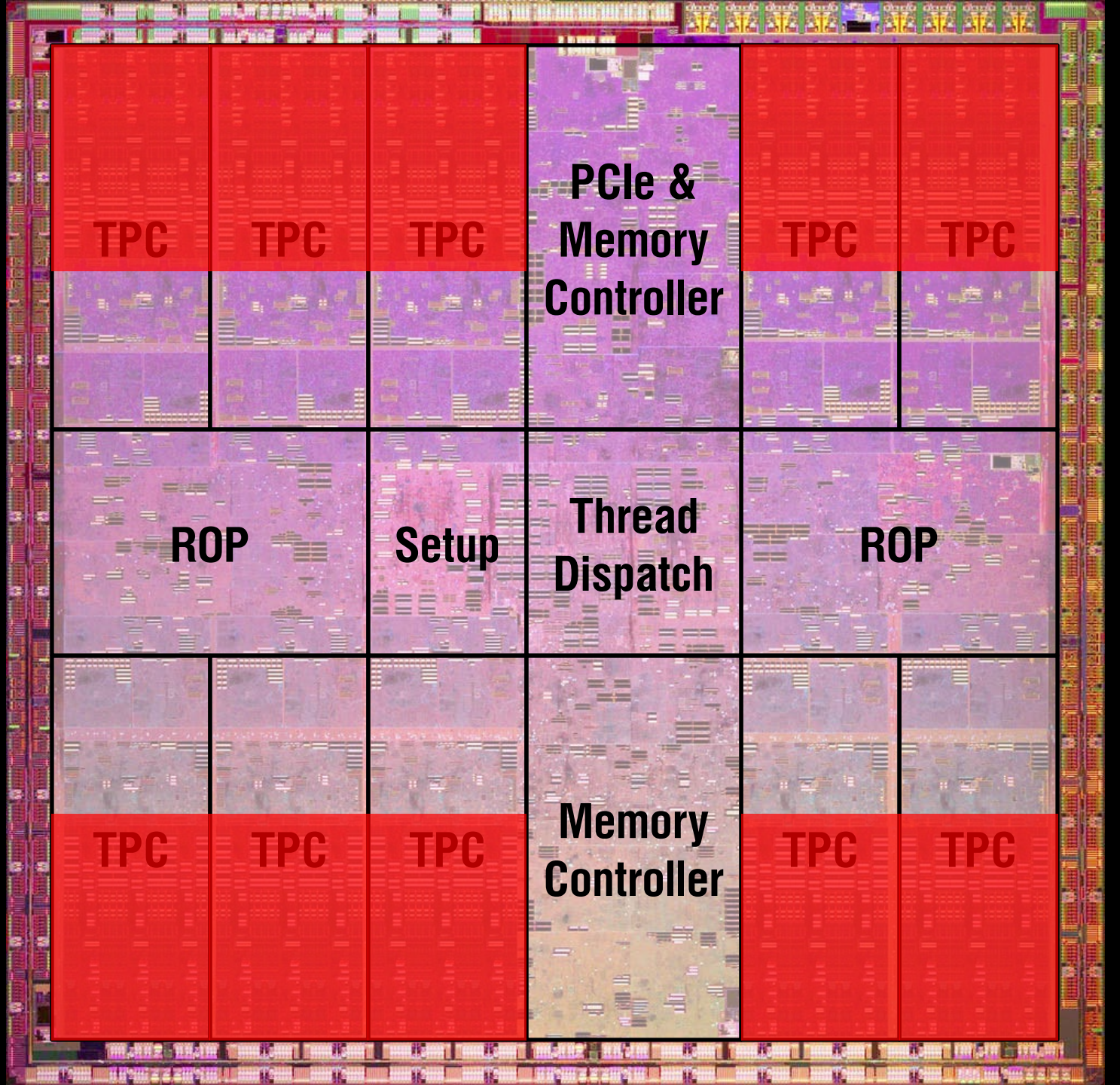


NVIDIA®
GeForce® GTX 285

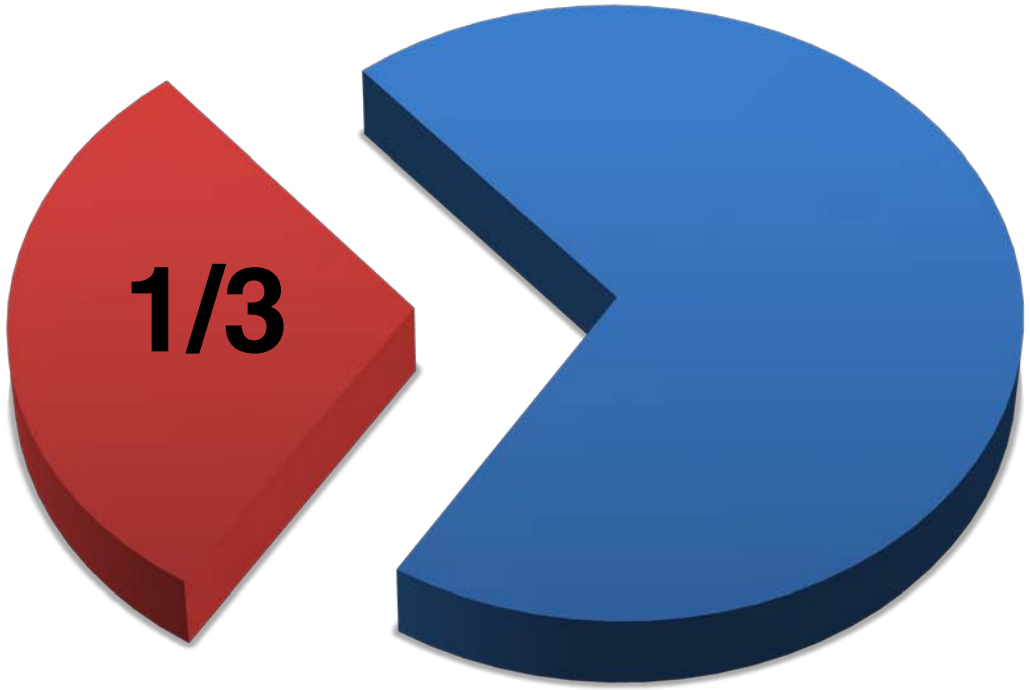
240 cores
1.476 GHz
1.4 billion transistors
470 mm^2


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


TPC
TPC
Multiprocessor
Multiprocessor
Multiprocessor
TPC
TPC
ROP
ROP
TPC
TPC
Texture Fetch &
Other
TPC
TPC

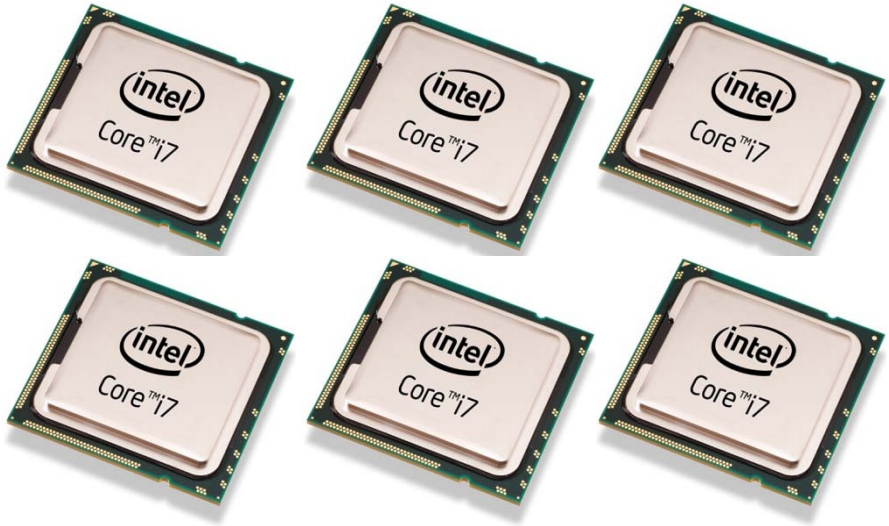

TPC
TPC
TPC
PCIe &
Memory
Controller
TPC
TPC
ROP
Setup
Thread
Dispatch
ROP
TPC
TPC
TPC
Memory
Controller
TPC
TPC

GPU dedicates about **30%** to the execution units!



GPU dedicates **6 times as many** resources to the execution units as CPU!

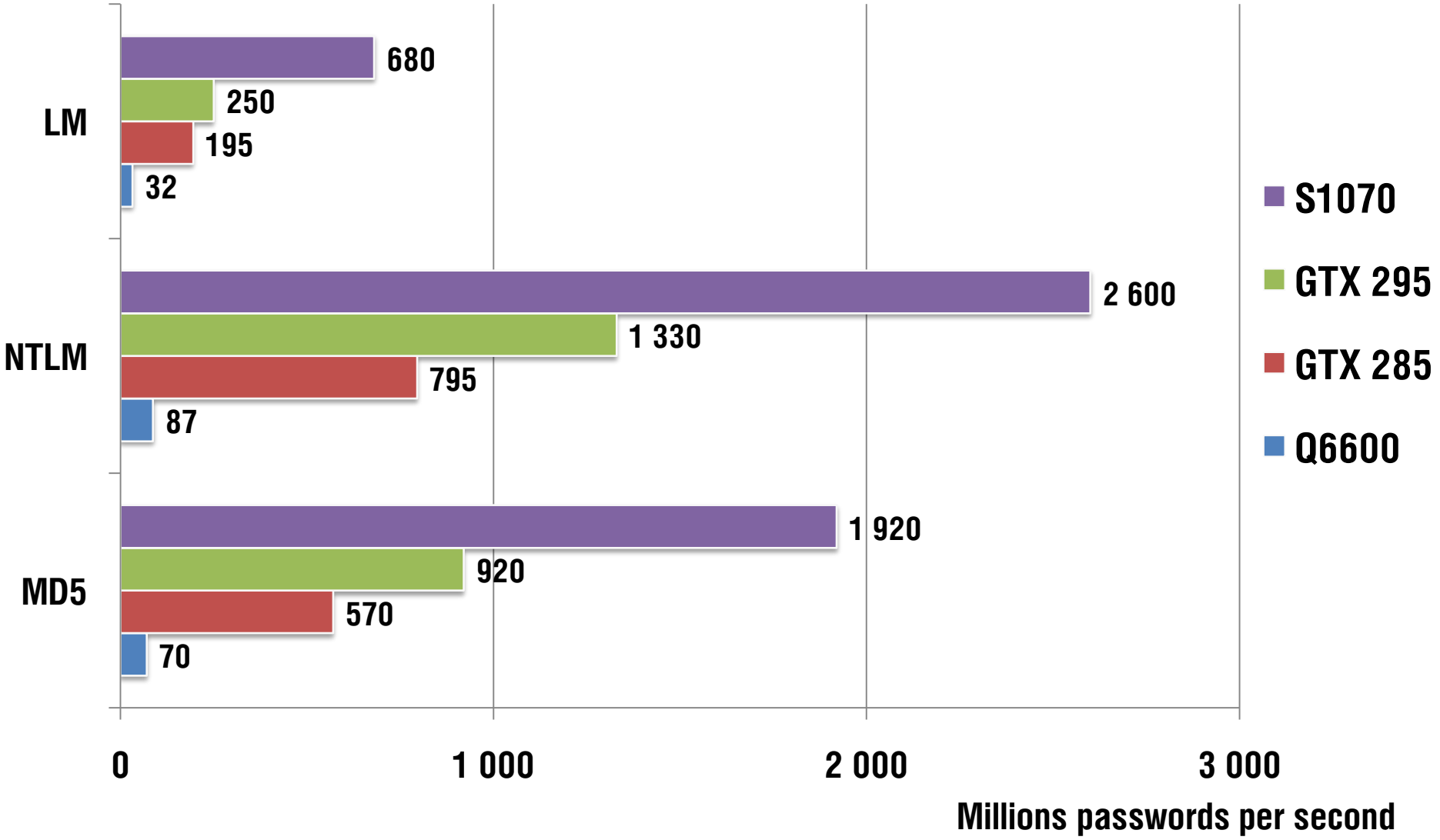
=



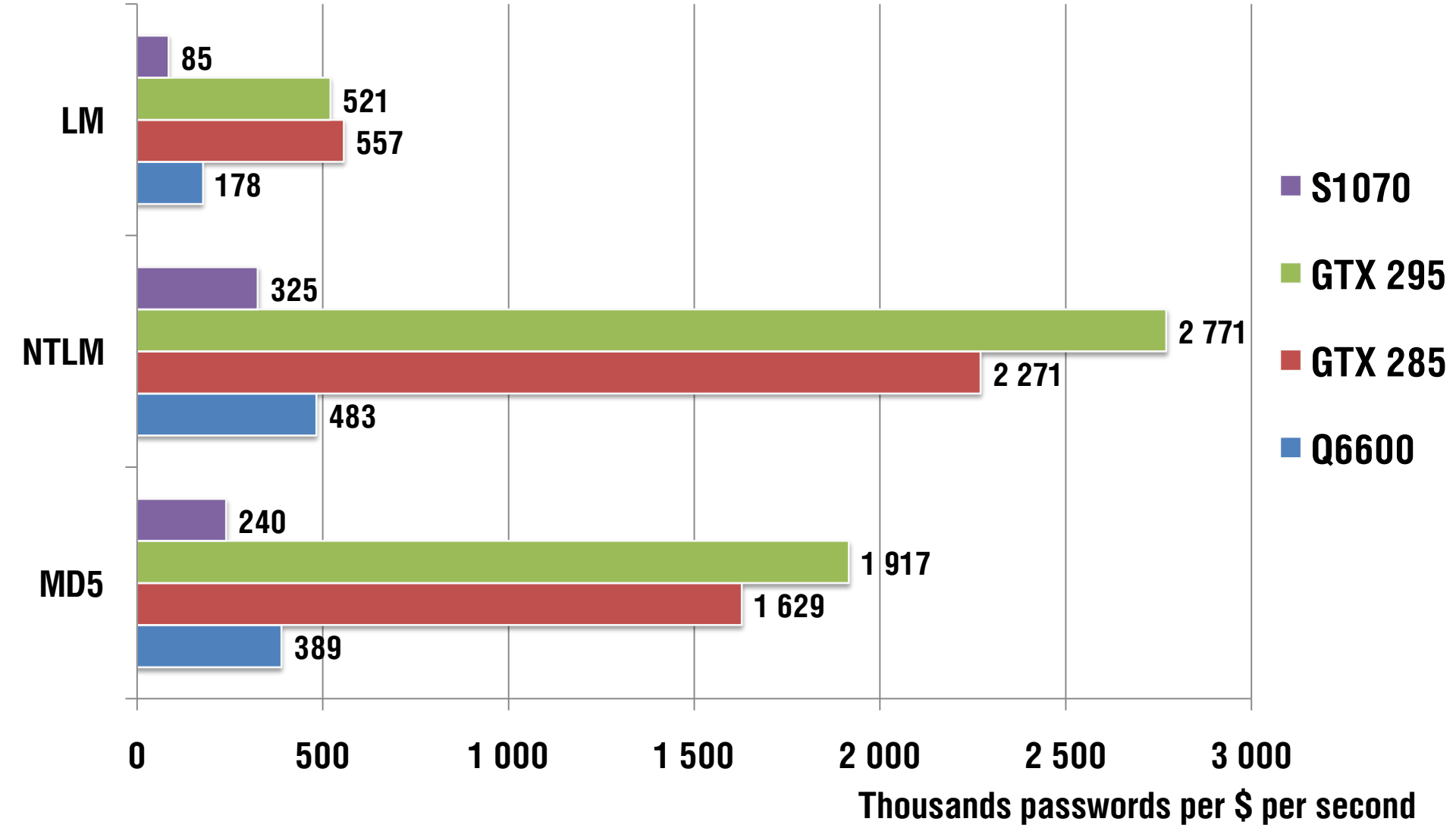
183 Watts full load

6x130=780 Watts full load

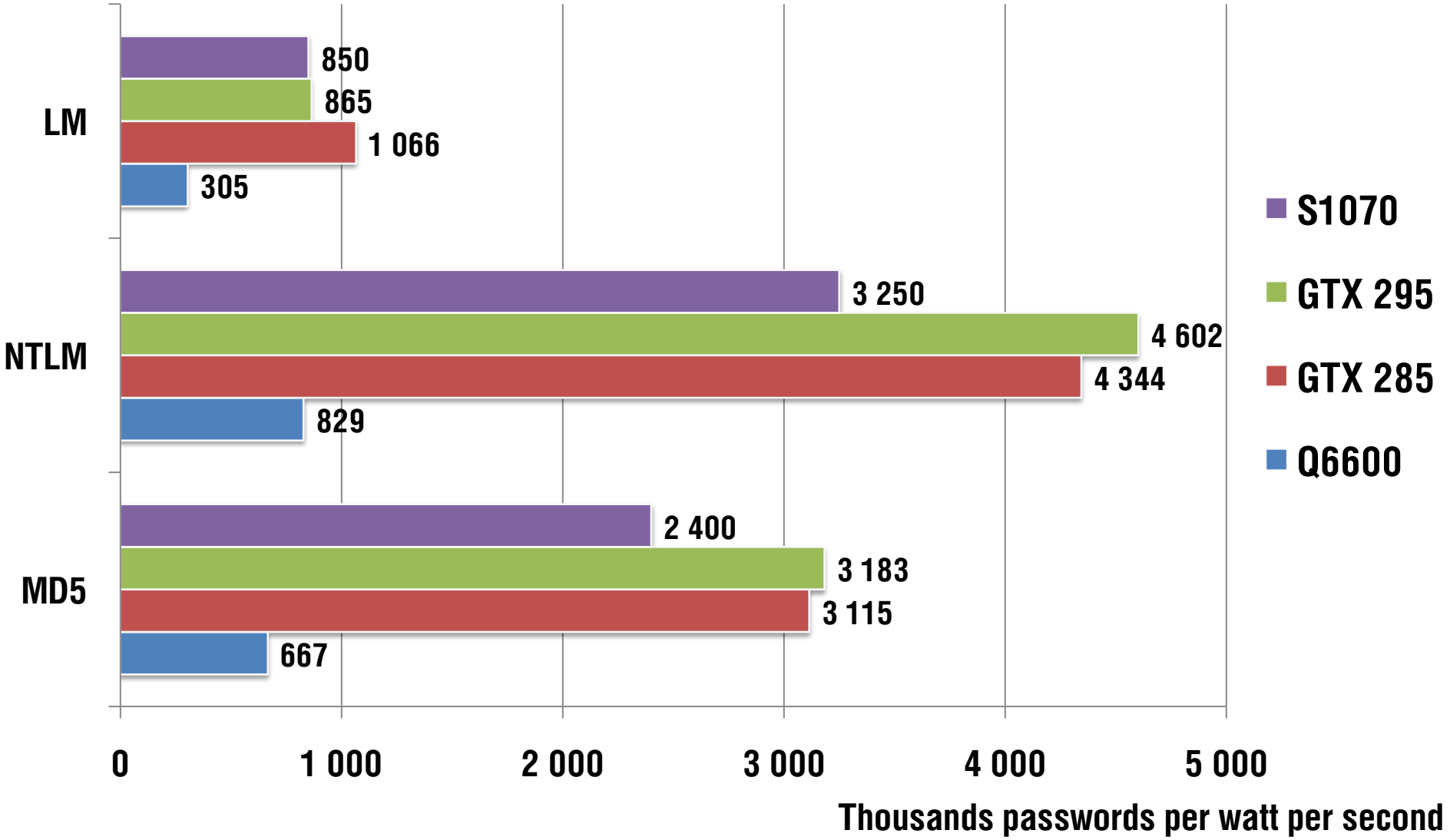
Performance



Performance per $



Performance per Watt



Bad News:

Not every algorithm is worth offloading to GPU

GPU is good at computing

but

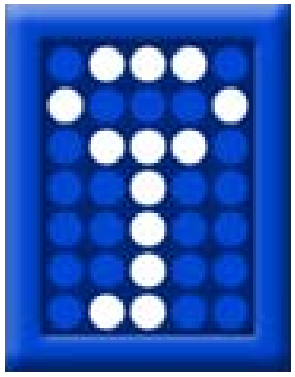
GPU is bad at accessing random memory locations

MD4 / MD5 ☑
SHA-1 / SHA-2 ☑
RIPEMD ☑
MD2 ☒
AES ☑
DES ☑
RC4 ☒

Good News:

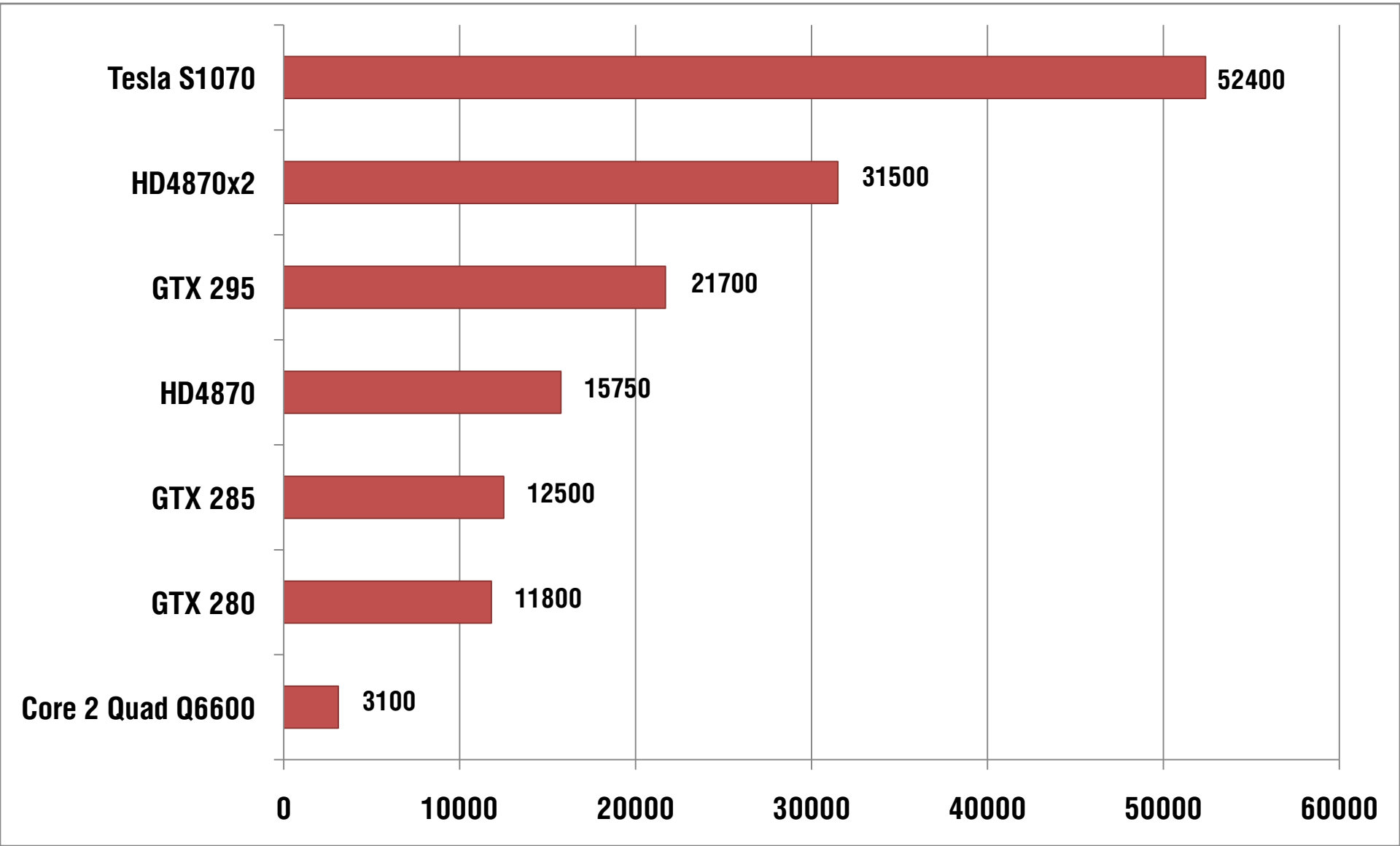
Humans love repetition


PGP




Wi Fi

WPA-PSK

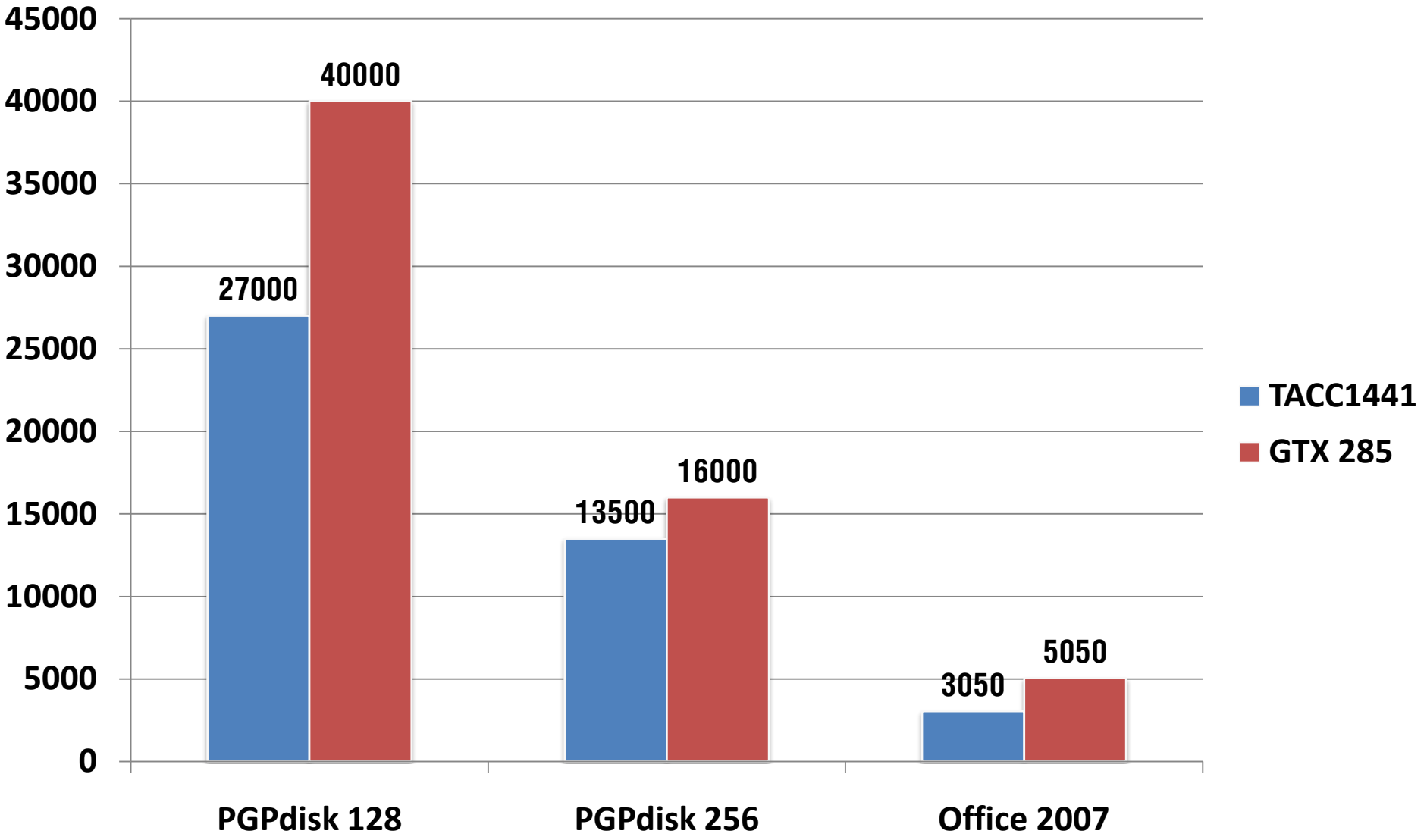

Tesla S1070
52400
HD4870x2
31500
GTX 295
21700
HD4870
15750
GTX 285
12500
GTX 280
11800
Core 2 Quad Q6600
3100
0
10000
20000
30000
40000
50000
60000

Other Accelerators?

Based on FPGA (Xilinx)
FireWire
Proprietary SDK

US $3’995

Single Unit Performance

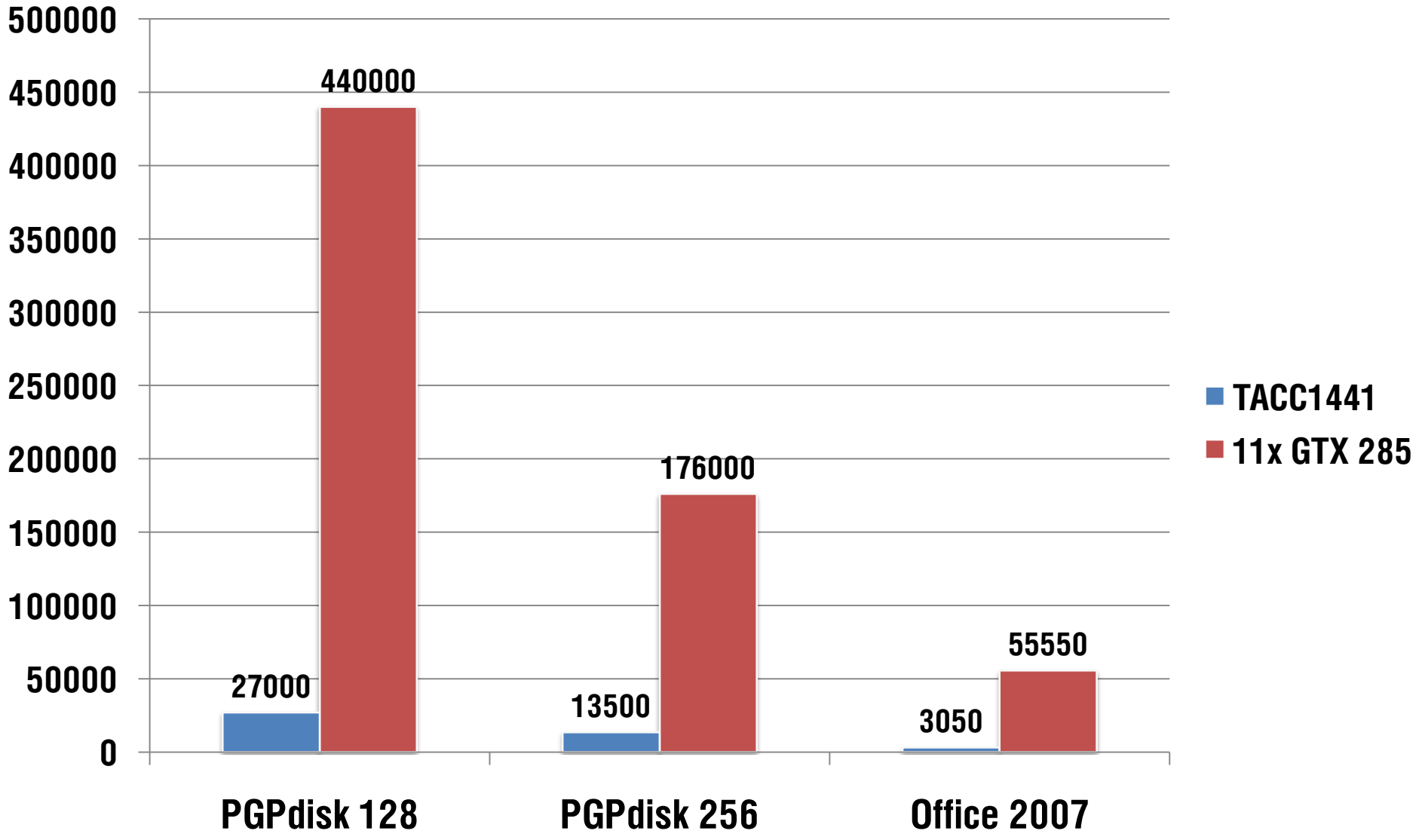


US $3’995


TABLEAU
Menu
Enter
Hardware Accelerator
Model TACC1441
Power
Host Det
Busy

US $3’995

Performance for $4K



Greener Computing

- Consider a cluster of 25 dual-CPU quad-core computers
- 400 watts full load each
- 10’000 watts total

Greener Computing

- Two Tesla S1070 provide same performance
- 800 watts full load each
- One computer for management
- 2’000 watts total


52x


TESLA
TESLA


52x

Greener Computing

- 8’000 watts saved
- 49’090 kWh a year (at 70% utilization)
- € 5’890 savings on electricity a year (at 0.12€ per kWh average rate)
- Prevents 27’500 kg CO_2 emission
- Takes 5 cars off the roads
- Saves 2’300 trees/year

Thank You!

Andrey Belenko
a.belenko@elcomsoft.com