Marcus Bakker & Roel van der Jagt

GPU-based passwords cracking

Content

- Background information
- Main question
- Test approach
- GPGPU vs CPU
- Conclusion
- Discussion
- Future

Background information

- General computations with GPUs has become available (GPGPU)
- GPU performances develop fast
- Hashes can be brute forced with enough power

Main question

- What should we (KPMG) advise our clients regarding password length and complexity now GPU-based password cracking has become reality?

Test approach 1/2

- Length: 6, 8, 10 and 12
- Characters: 0, a, a0, aA0, aA0~
- 5 passwords each
- Total: 4*5*5 = 100 passwords

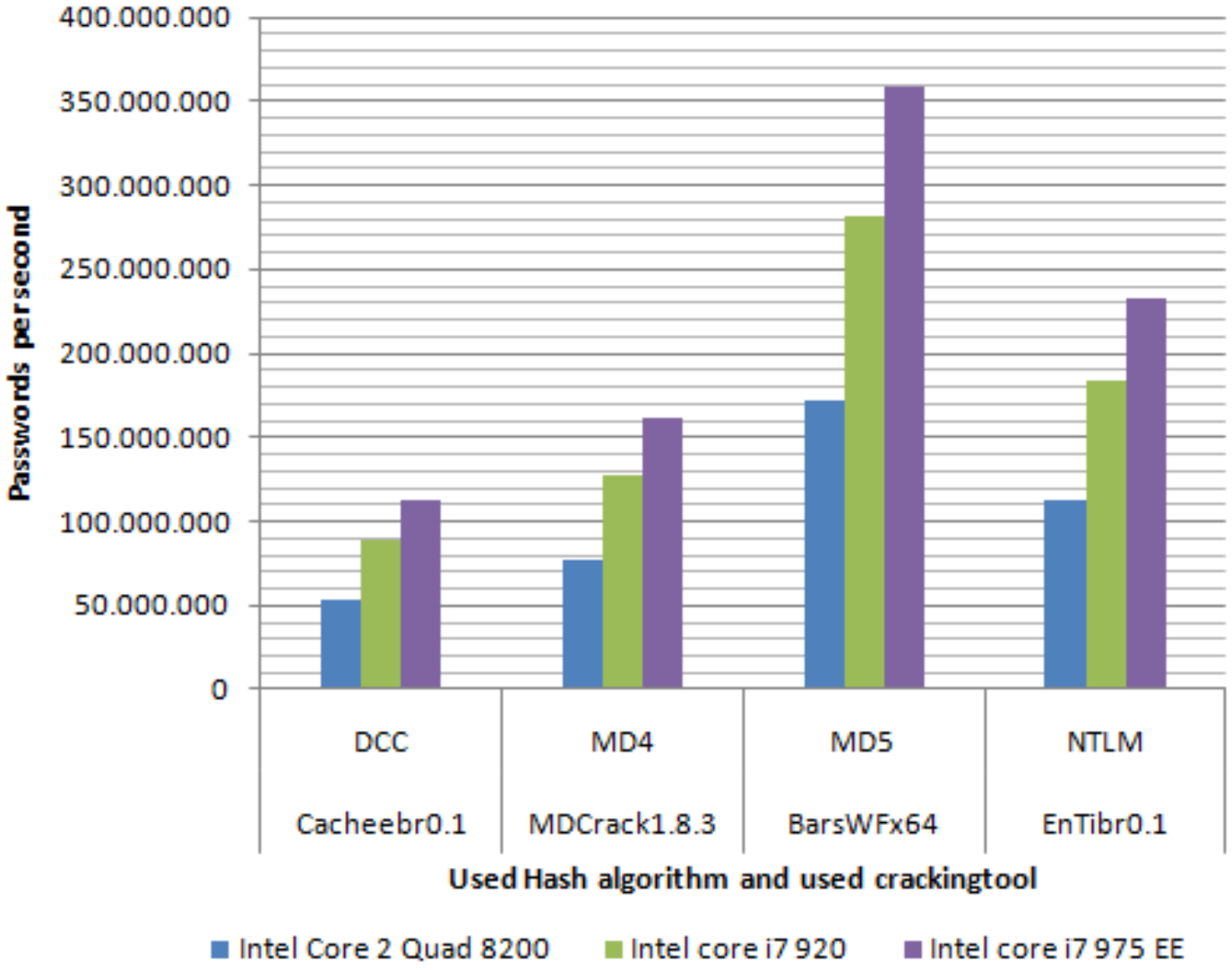
- 4 tools
- 4 hashes
  - MD5
  - NTLM
  - DCC
  - Oracle 11g

Test approach 2/2

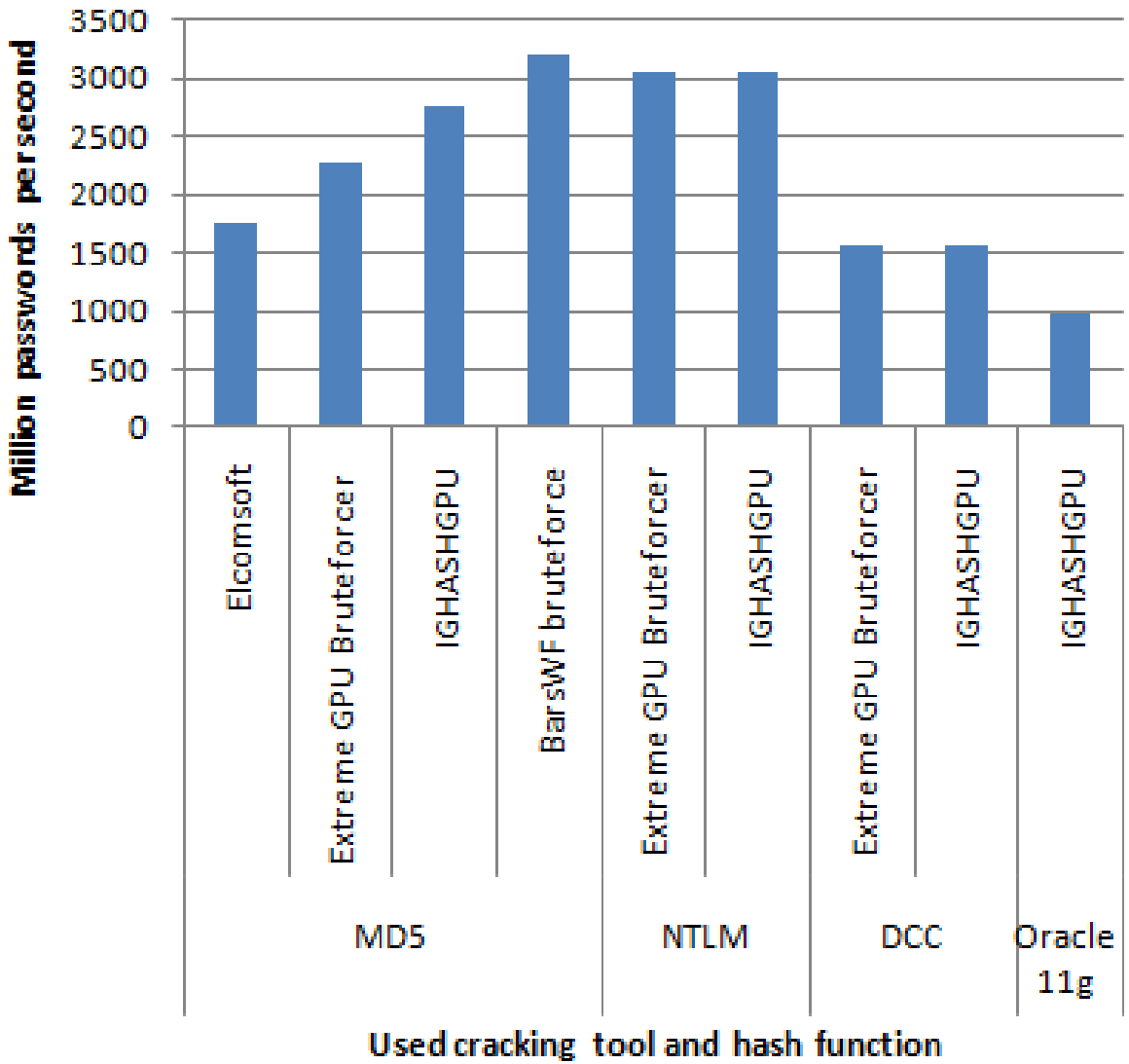
- Total: 9 tests, 400 hashes, 900 results

- Tested for single passwords
- Test hardware
  - Intel Core i7 920
  - 2x Nvidia GTX295

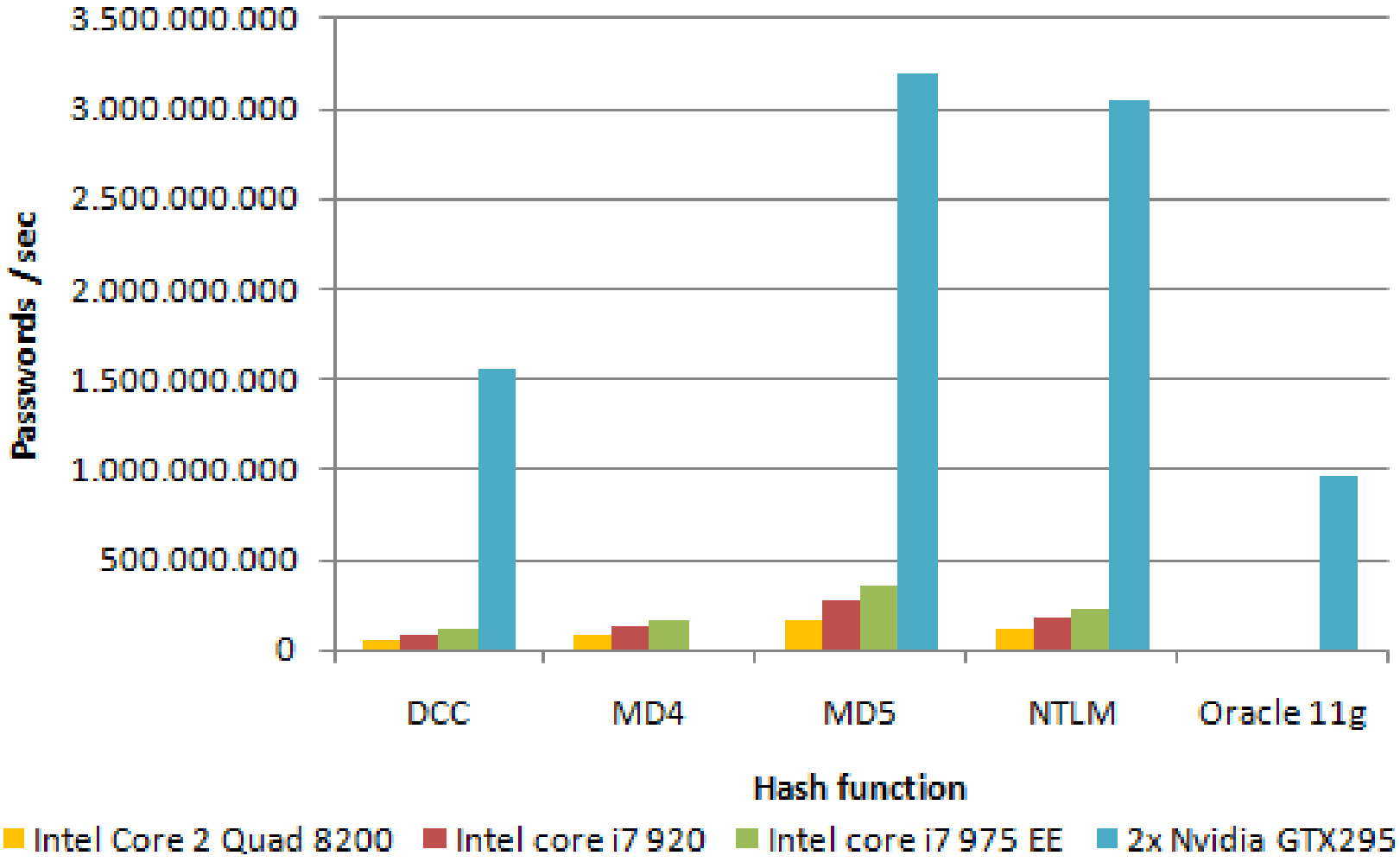
Passwords / sec on CPU



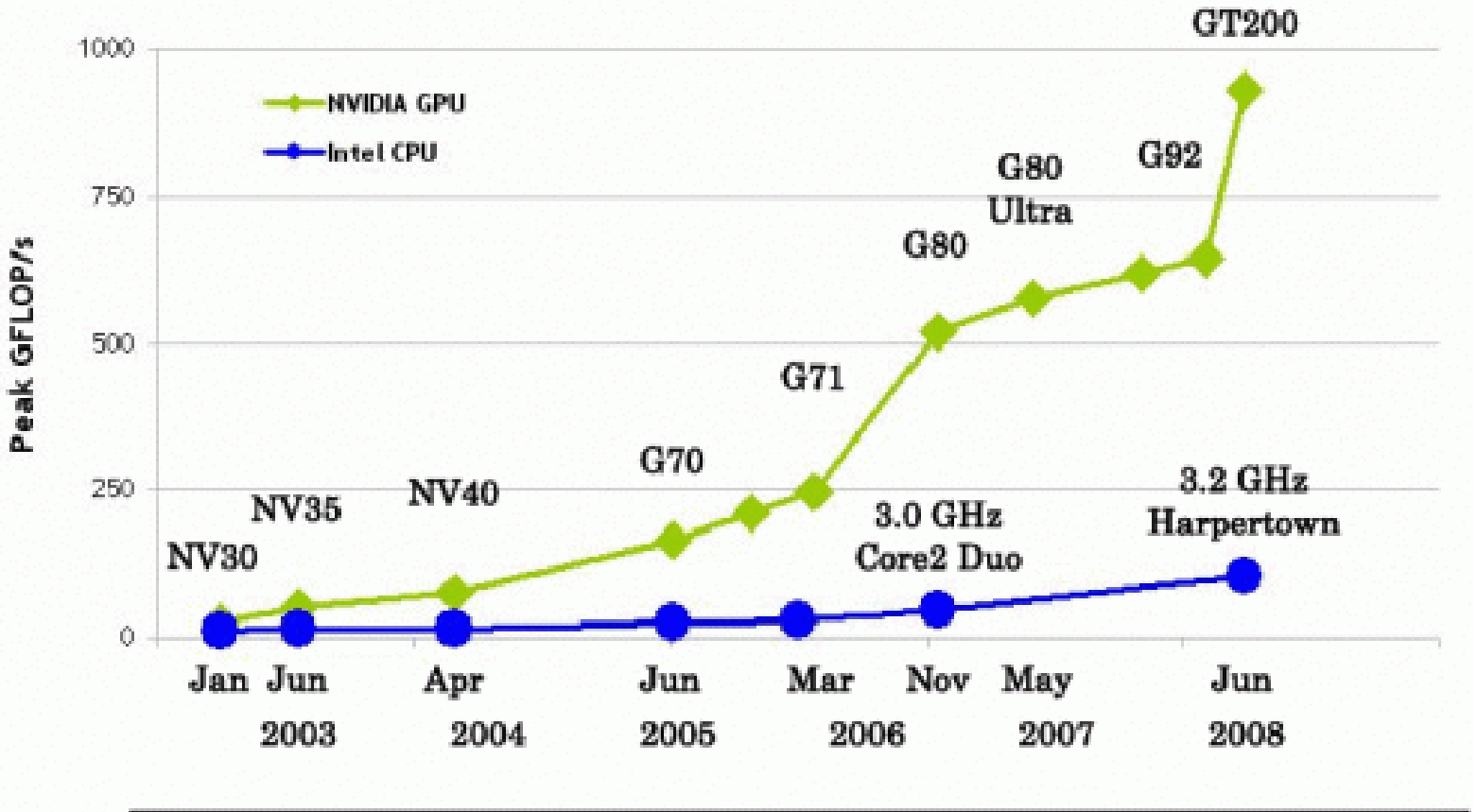
Passwords / sec on GPGPU



GPGPU vs CPU in pwd/sec



GPGPU vs CPU in GFLOPS



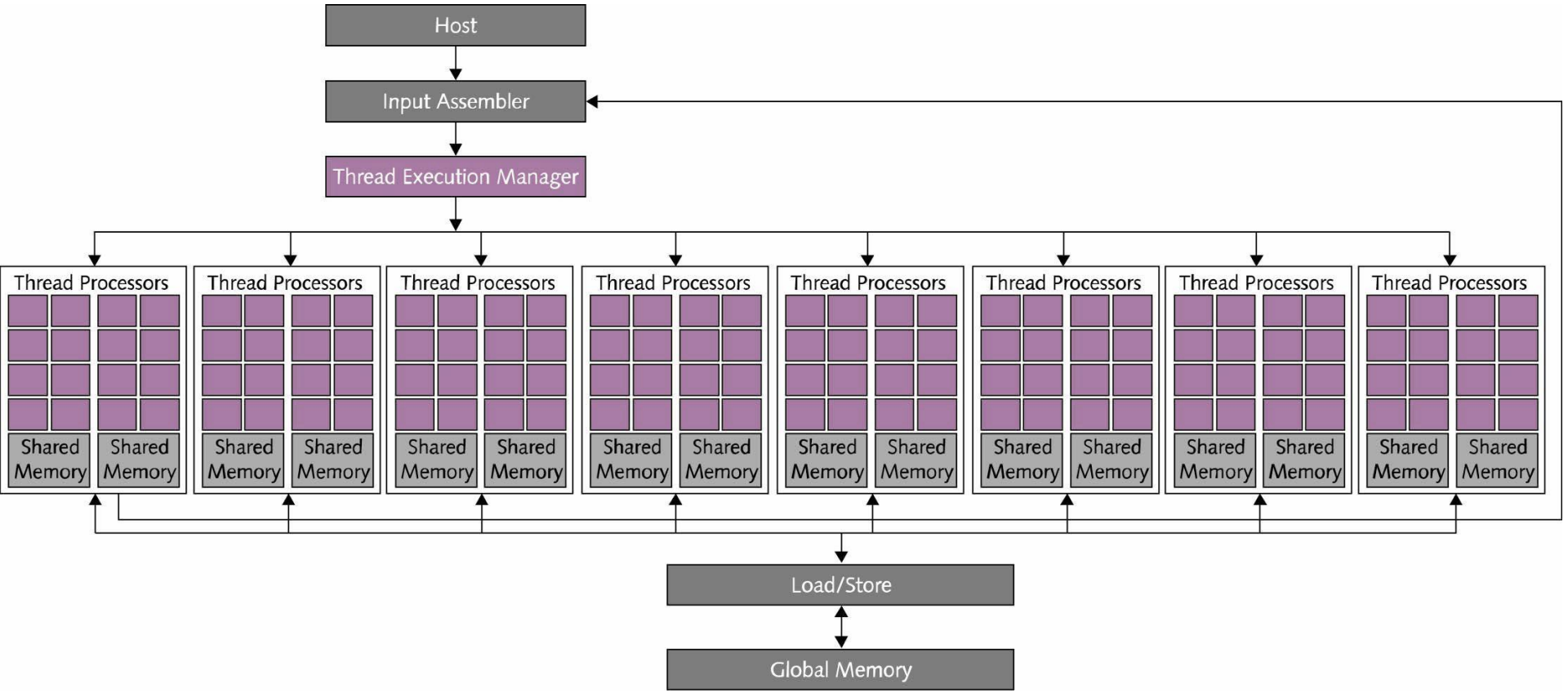
GT200 = GeForce GTX 280	G71 = GeForce 7900 GTX	NV35 = GeForce FX 5950 Ultra
G92 = GeForce 9800 GTX	G70 = GeForce 7800 GTX	NV30 = GeForce FX 5800
G80 = GeForce 8800 GTX	NV40 = GeForce 6800 Ultra	

GPGPU vs CPU

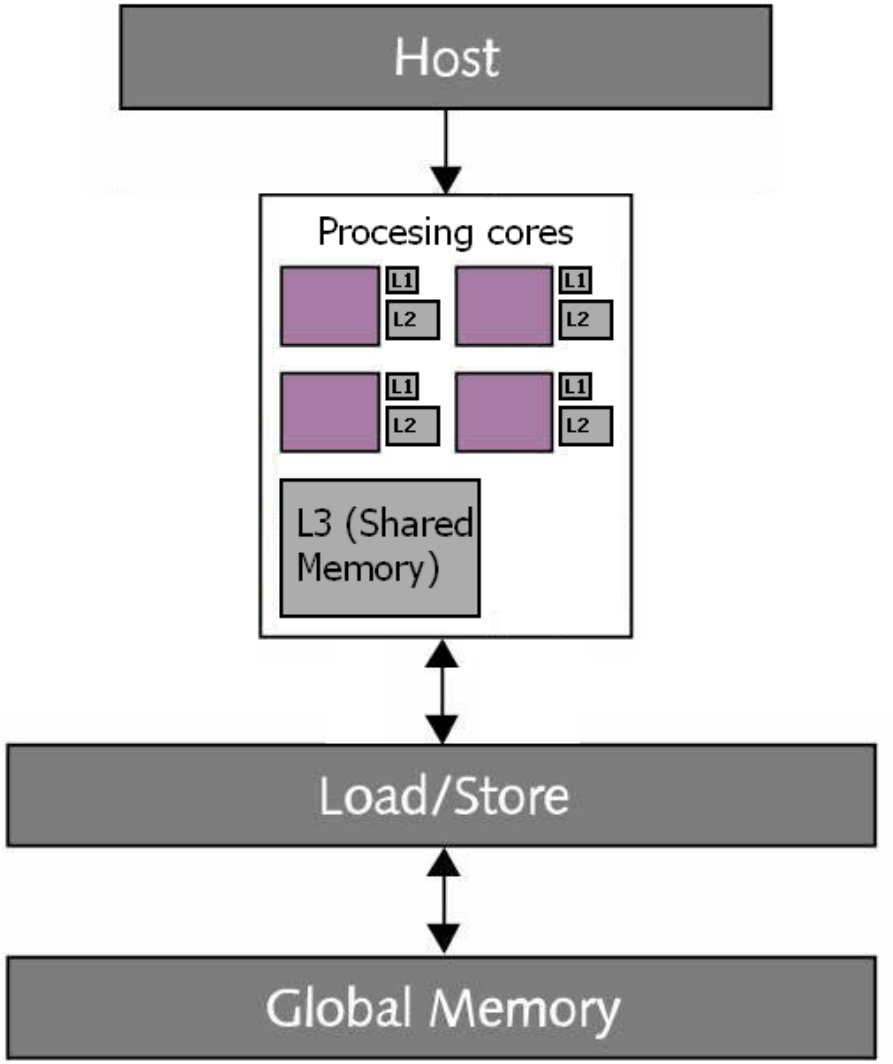
- Parallel vs Serial
- SIMD vs SISD
- Limited vs Full instruction set

- Disadvantage GPGPU
  - Limited amount of memory available per thread
  - Limited amount of shared memory
  - Off-chip memory access takes a lot of cycles
  - Limited instruction set

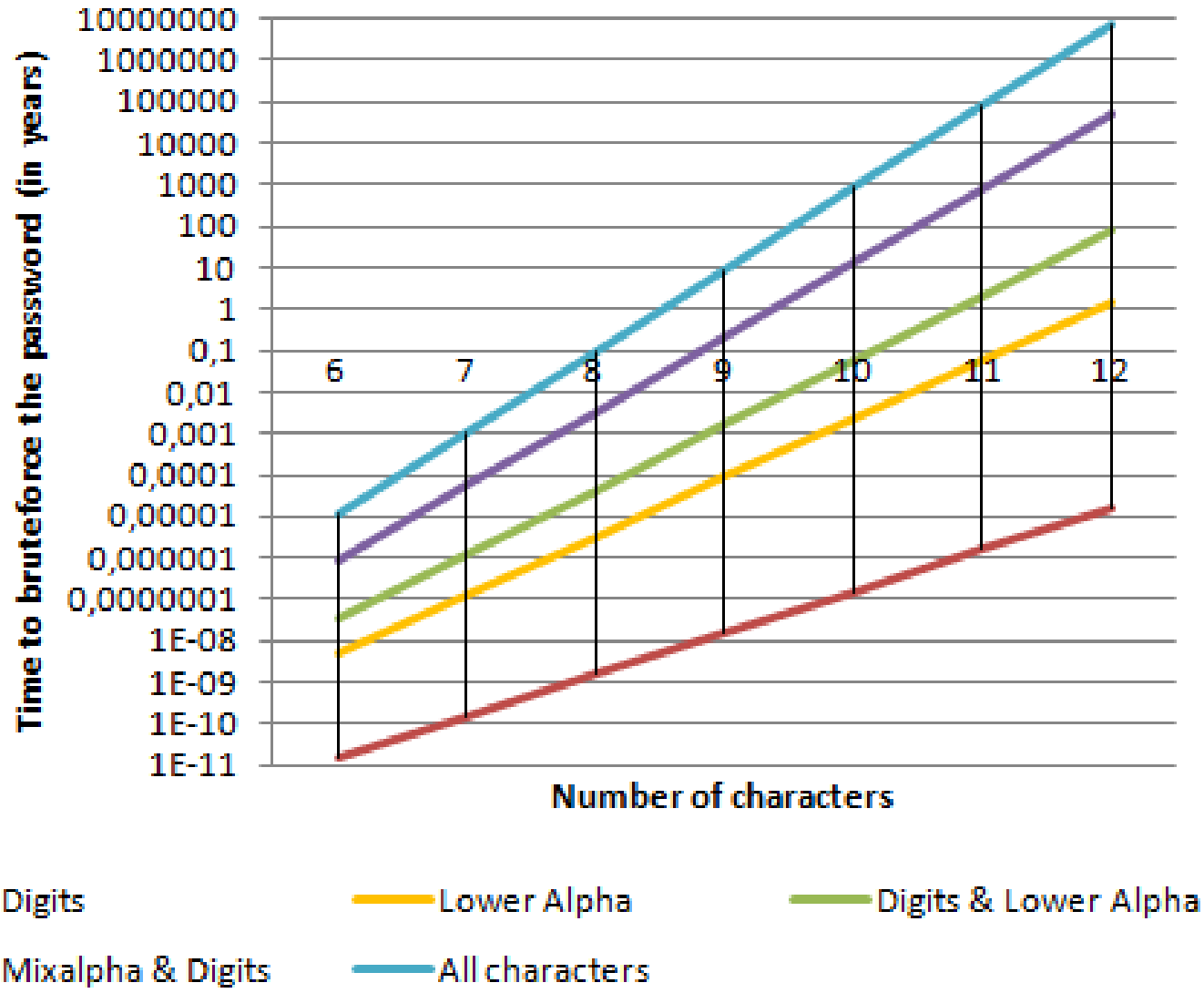
GPGPU vs CPU


Host
Input Assembler
Thread Execution Manager
Thread Processors
Shared Memory
Load/Store
Global Memory

GPGPU vs CPU


Host
Procesing cores
L1
L2
L1
L2
L1
L2
L1
L2
L3 (Shared Memory)
Load/Store
Global Memory

Cracking times



Conclusion

- Advised password length
  - aAo~ Nine or more characters
  - aAo Ten or more characters
  - ao or Ao Twelve or more characters
- No differences per hash or tool

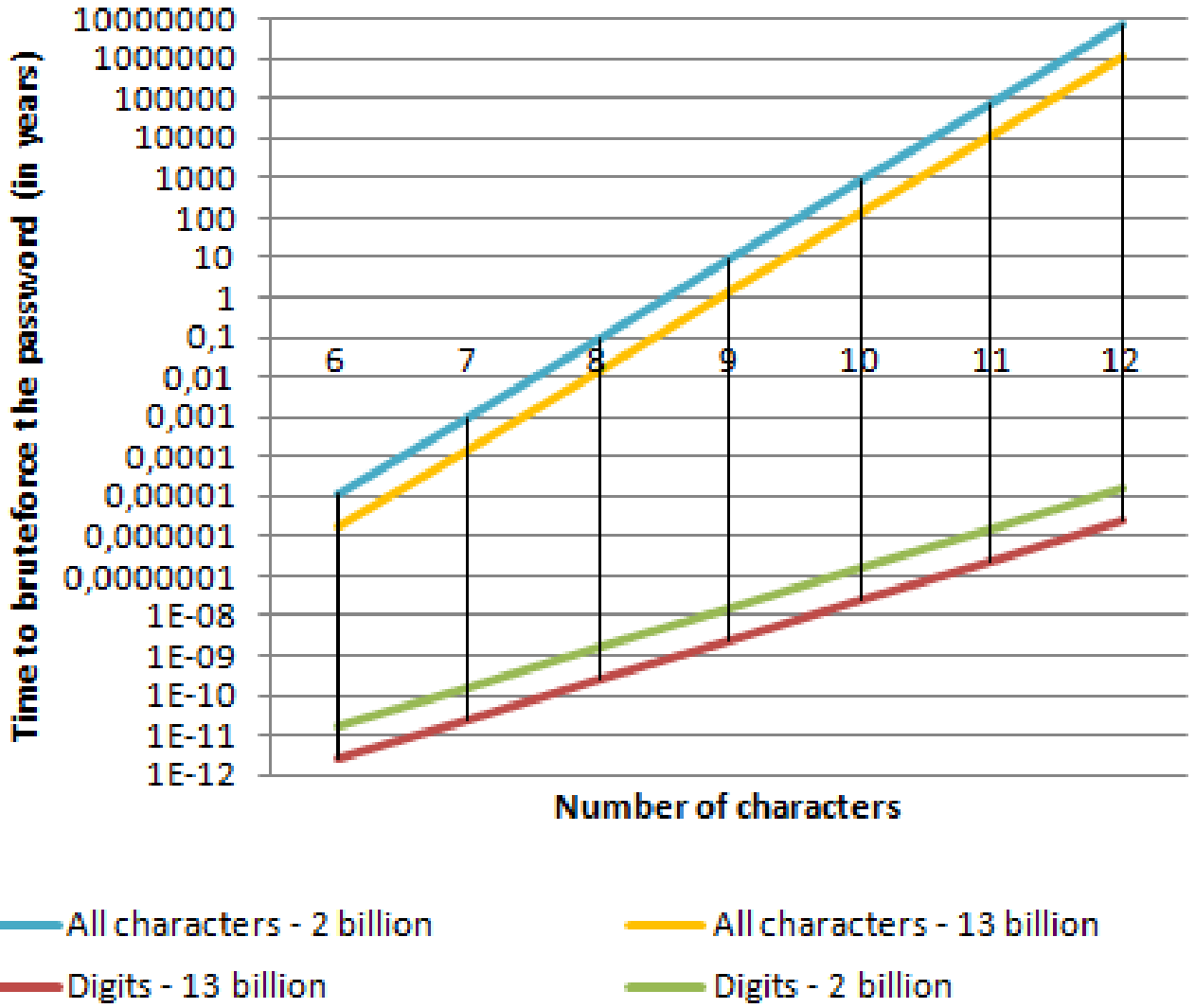
Future work

- Rainbow tables
- Dictionary attacks
- Crack the hashes left

In the future

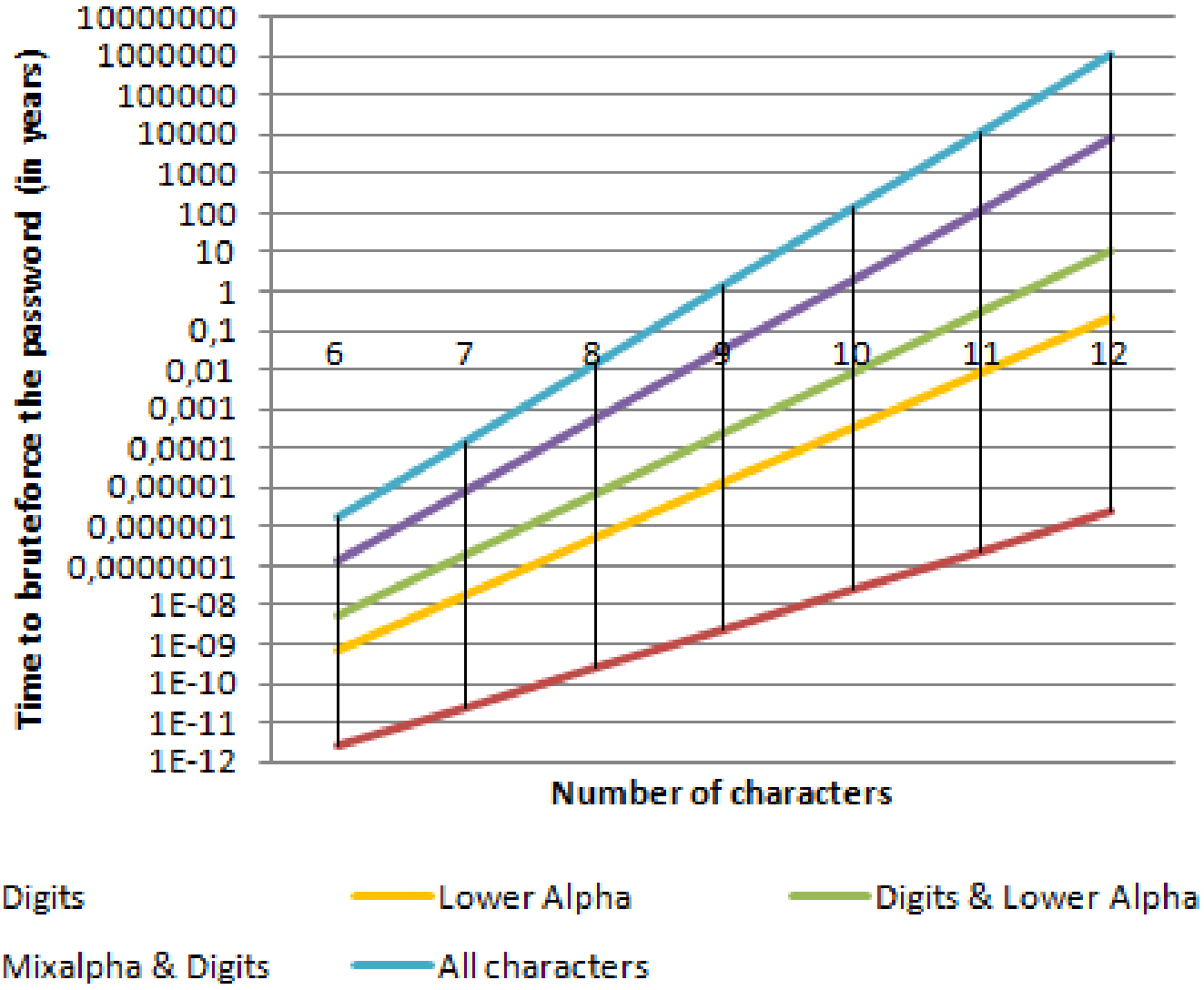
- GPUs become faster and faster
  - ATI 5970 6.1 billion passwords / second (MD5)
  - 4 times faster

Future - Passwords / sec



Questions & Feedback

Appendix 1 – Future - Passwords / sec



Appendix 2 – Entropy

- *"A measure for the amount of disorder"*
- $\log_2(n)$
- # passwords in keyspace = $2^{(\text{entropy password})}$

Character Pool	Available Characters (n)	Entropy Per Character
digits	10 (0-9)	3.32 bits
lower case letters	26 (a-z)	4.7 bits
upper case letters and digits	62 (A-Z, a-z,0-9)	5.95 bits
all standard keyboard characters	94	6.55 bits

Appendix 3 – Ratios in Pwd / Sec

	Nvidia GT295	Nvidia GT295	Nvidia GT295	Nvidia GT295	Intel Core i7 920
	Oracle11g	NTLM	DCC	MD5	
Power consumption[6] (Watt)	289	289	289	289	130
Performance (million passwords / sec	484	1550	788	1500	230
Price[7] (€)	400,-	400,-	400,-	400,-	227,-
Performance/Price ratio (passwords / sec / €)	1,21	3,88	1,97	3,75	1,01
Performance/Power consumption ratio (passwords / sec / Watt)	1,67	5,36	2,73	5,19	1,77

Appendix 4 – Ratios in GFLOPS

	Nvidia GT295	Intel Core i7 920	Intel Core i7 975
	GPU	CPU	
Power consumption[1] (Watt)	289	130	130
Performance (GFLOPS)	1788.48	44,8	55,36
Price[2] (€)	400,-	227,-	825,-
Performance/Price ratio (GLOPS / €)	4,47	0,197	0,0671
Performance/Power consumption ratio (GLOPS / Watt)	6,19	0,345	0,426