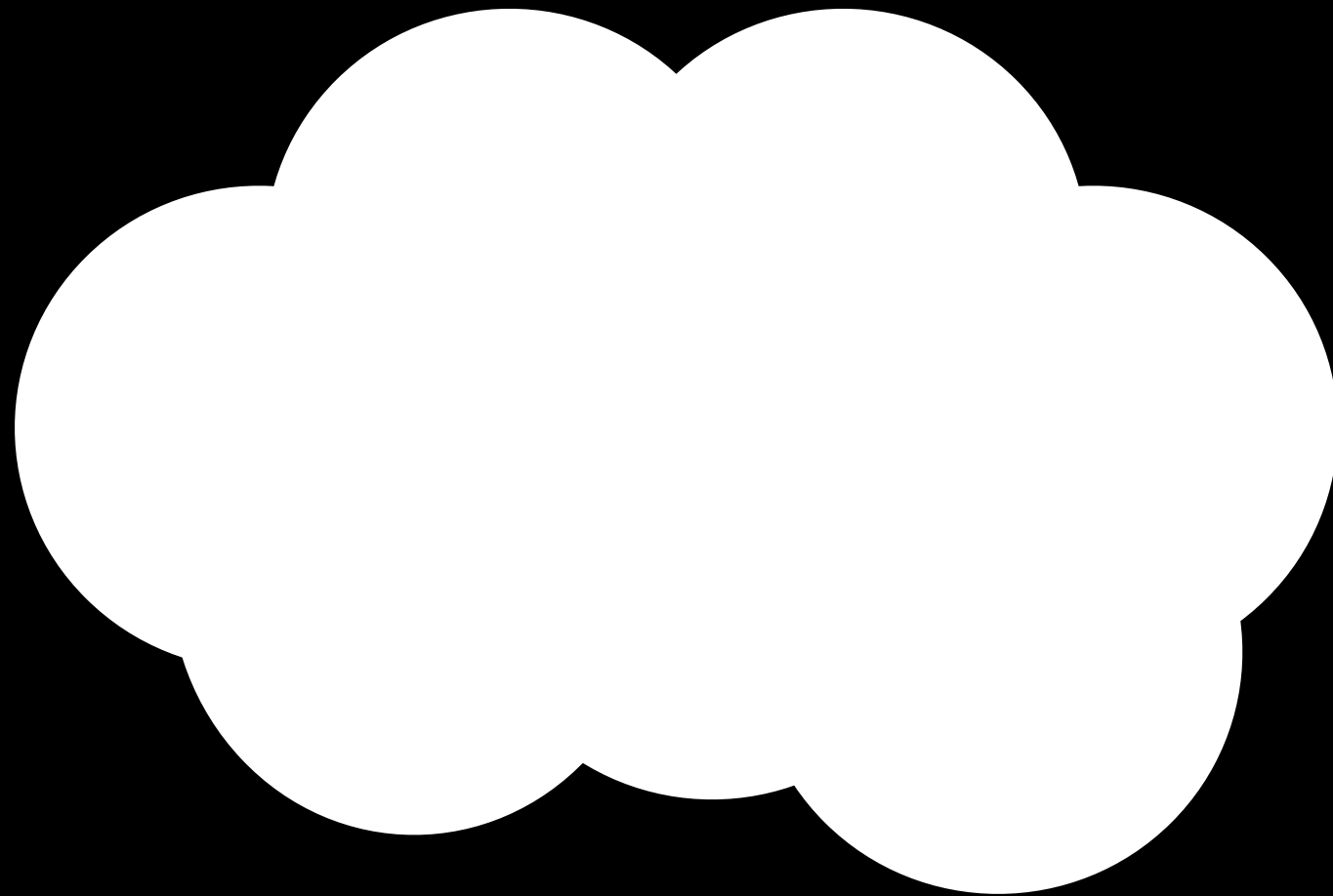


Cryptohaze Cloud Cracking



Bitweasil
cryptohaze.com

Who Am I?



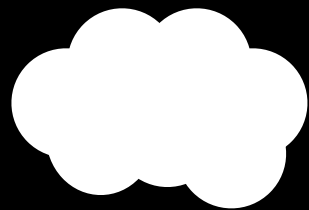
John the Ripper



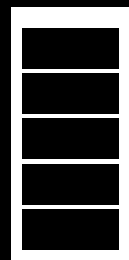
Icons



Target Hashes



The Cloud



The Cluster

State of “Cloud Cracking”



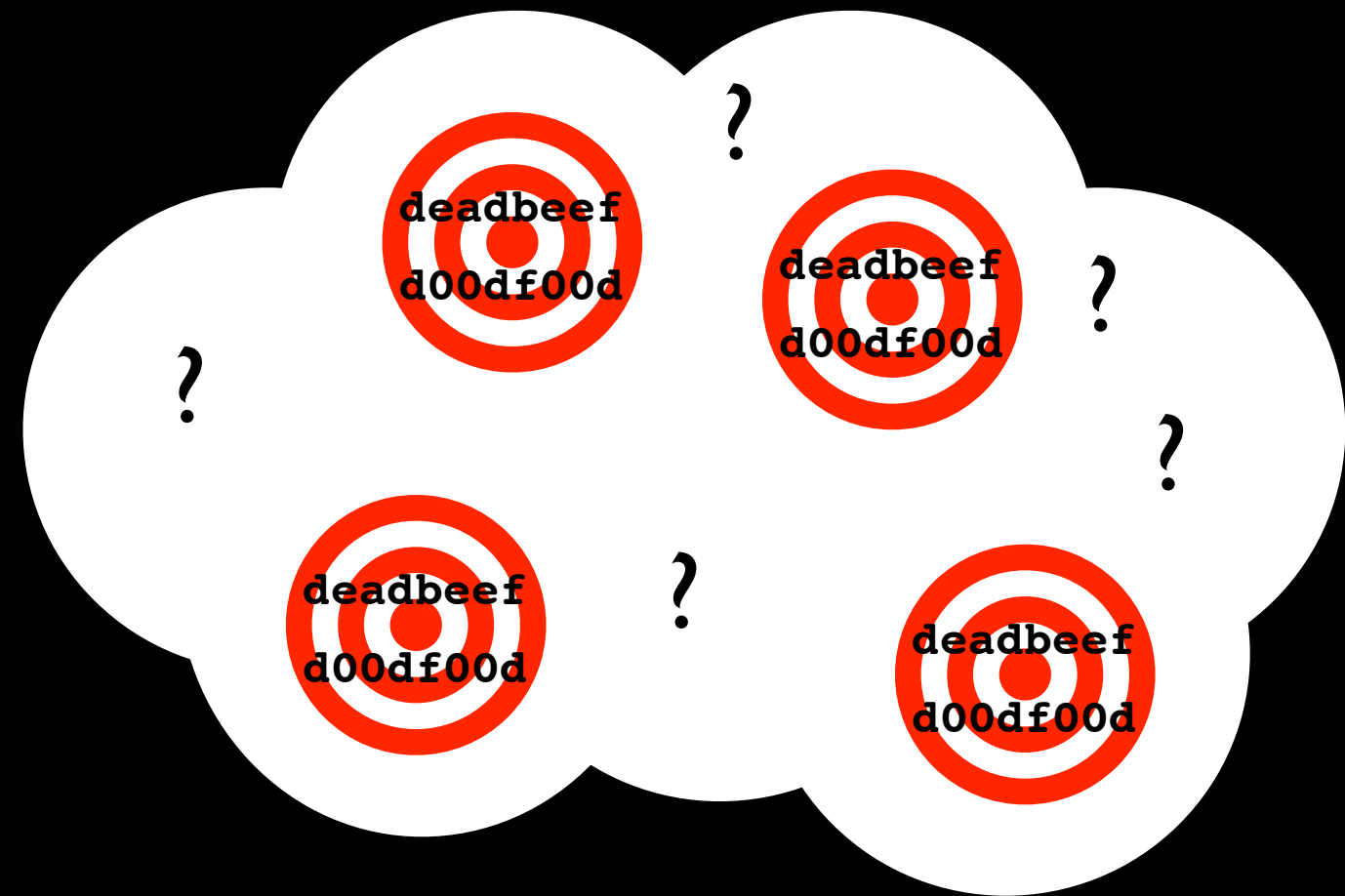
Amazon's EC2 GPU Cluster instances
(\$2.10/hr for two ancient nVidia GPUs)

Thomas Roth's Cloud Cracking Suite (MIA)

Moxie's WPACracker Cloud Service

Roll your own?

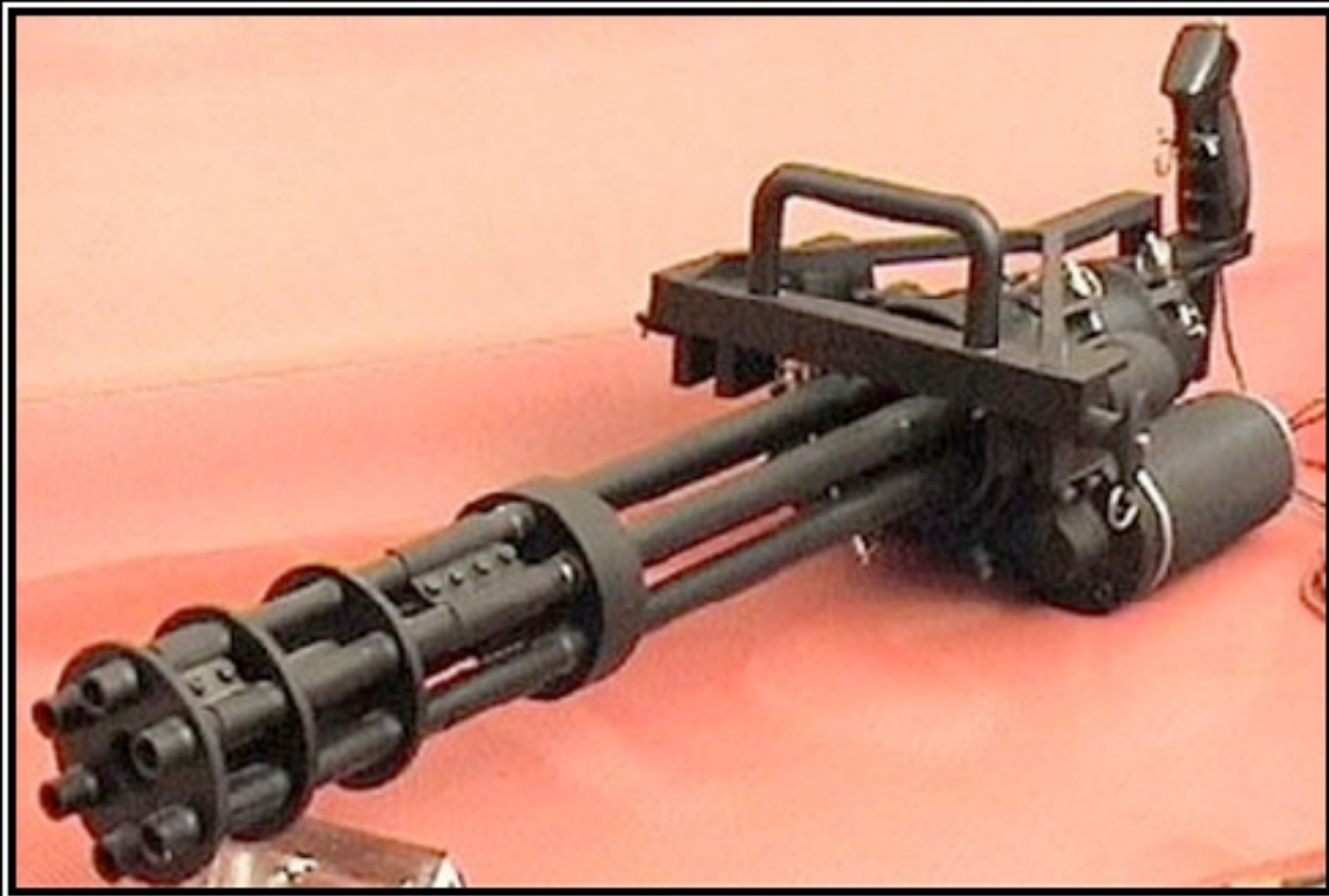
Non-disclosure of Hashes



Linkedin?
eHarmony?
Last.FM?

Crytohaze Multiforcer

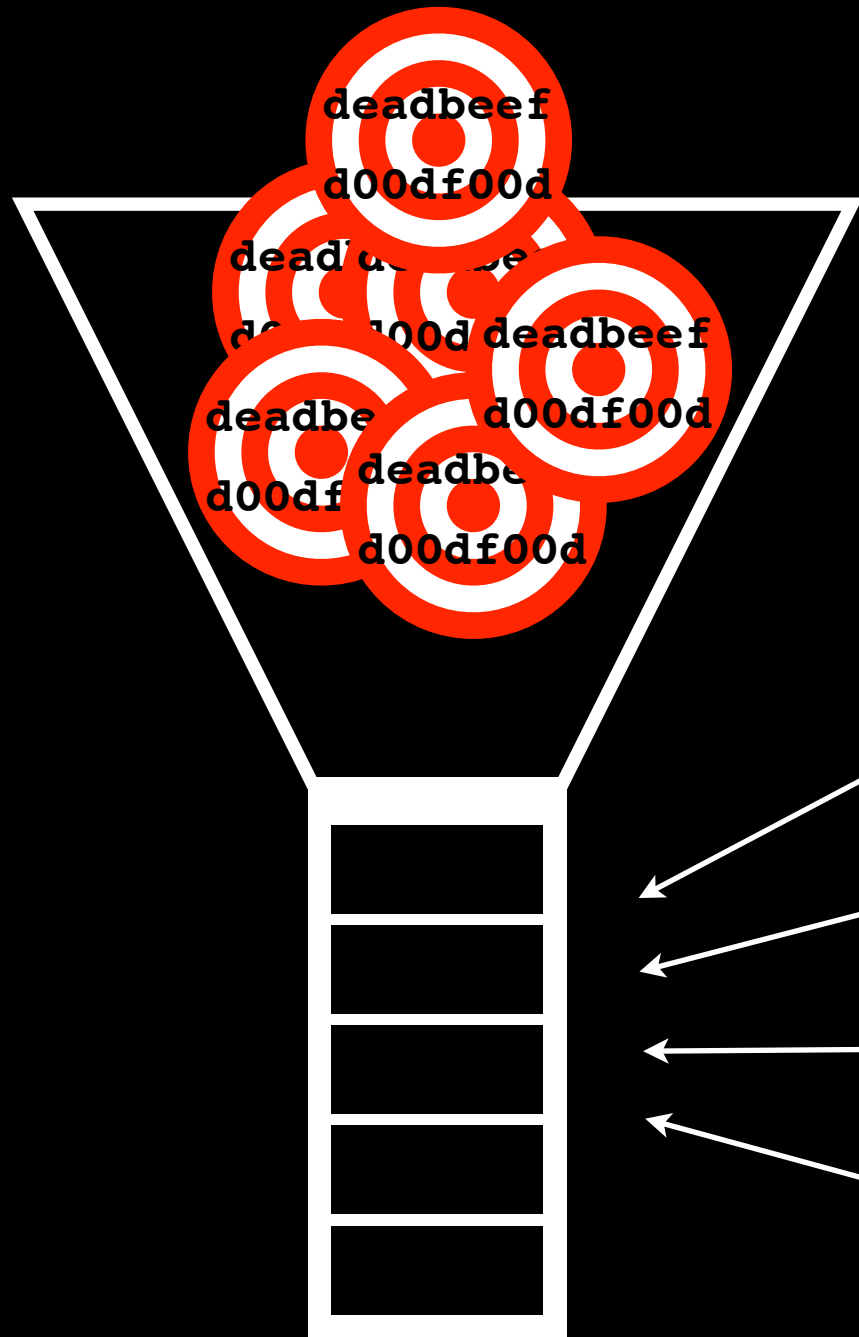
- GPLv2
- Linux, Windows, OS X
- CUDA, OpenCL, CPU
- C++ Framework
- Integrated Network Support



BRUTE FORCE

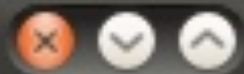
If it doesn't work, you're just not using enough.

Compute Nodes
Dedicated or Desktop
GPU or CPU
Local or Internet



--enableserver
--serveronly

--remoteip=[hostname]



File Edit View Terminal Help

'p' to pause

Cryptohaze MFN 1.31
12410

'q' to quit

Hash type : NTLM
Current PW len: 7
Total hashes : 10
Cracked hashes: 1
Total time : 00:01:43
WUs: 175/1017 (17.2%)

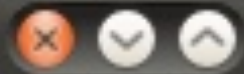
Passwords Found
8k`dES*

0: NET: 19.24B/s
1: NET: 38.39B/s
2: NET: 18.31B/s
3: NET: 15.98B/s
4: NET: 14.50B/s
5: NET: 40.77B/s
6: NET: 7.15B/s

6: [REDACTED]
5: [REDACTED]
4: [REDACTED]
3: [REDACTED]
2: [REDACTED]
1: [REDACTED]
0: [REDACTED]

Starting pw len 7

TOTAL 154.35B/s



File Edit View Terminal Help

'p' to pause

Cryptohaze MFN 1.31
12410

'q' to quit

Hash type	:	SHA1
Current PW len:	:	8
Total hashes	:	1000
Cracked hashes:	:	0
Total time	:	00:00:56
WUs:	:	0/48271 (0.0%)

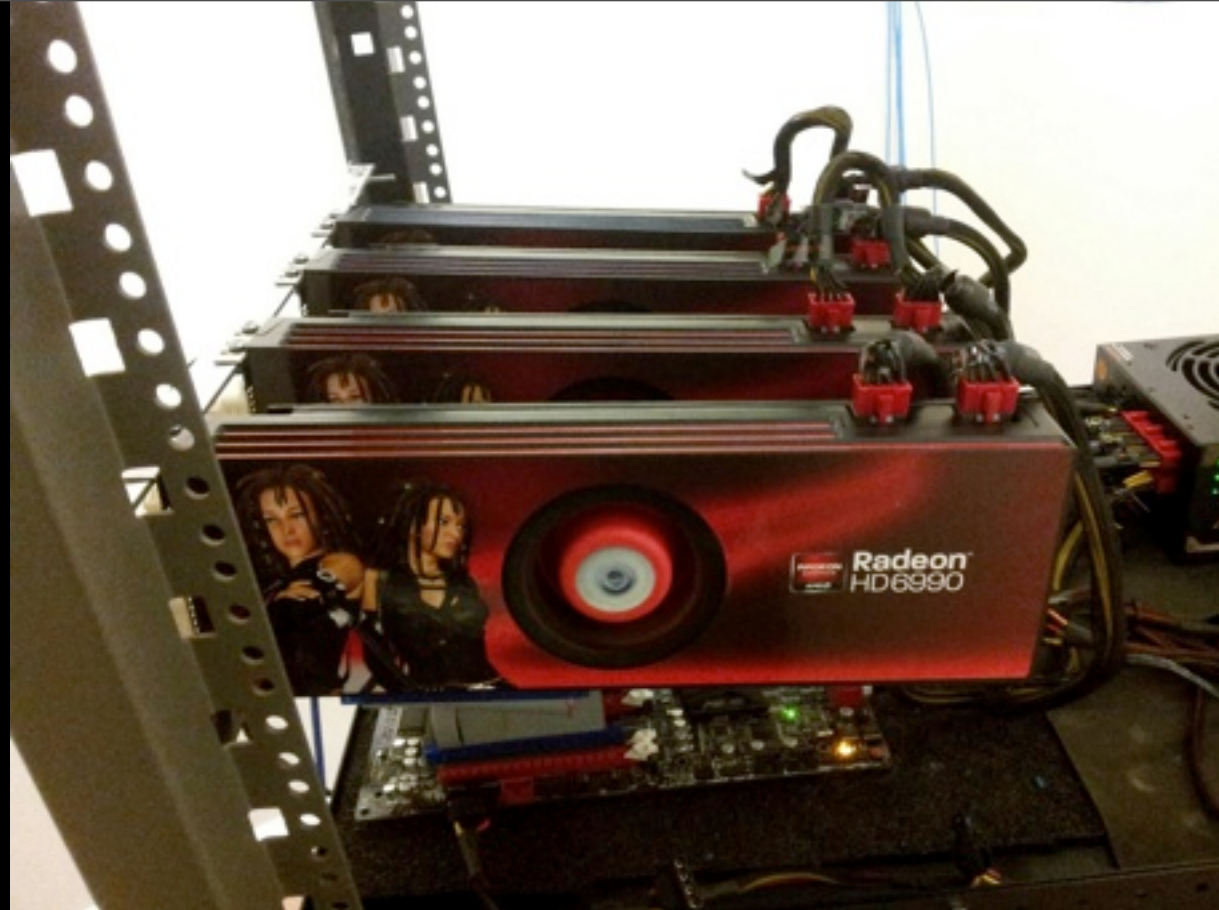
Passwords Found

0:	NET:	8.38B/s
1:	NET:	2.52B/s
2:	NET:	3.47B/s
3:	NET:	1.87B/s
4:	NET:	2.66B/s
5:	NET:	8.04B/s
6:	NET:	3.23B/s

6:	[REDACTED]
5:	[REDACTED]
4:	[REDACTED]
3:	[REDACTED]
2:	[REDACTED]
1:	[REDACTED]
0:	[REDACTED]

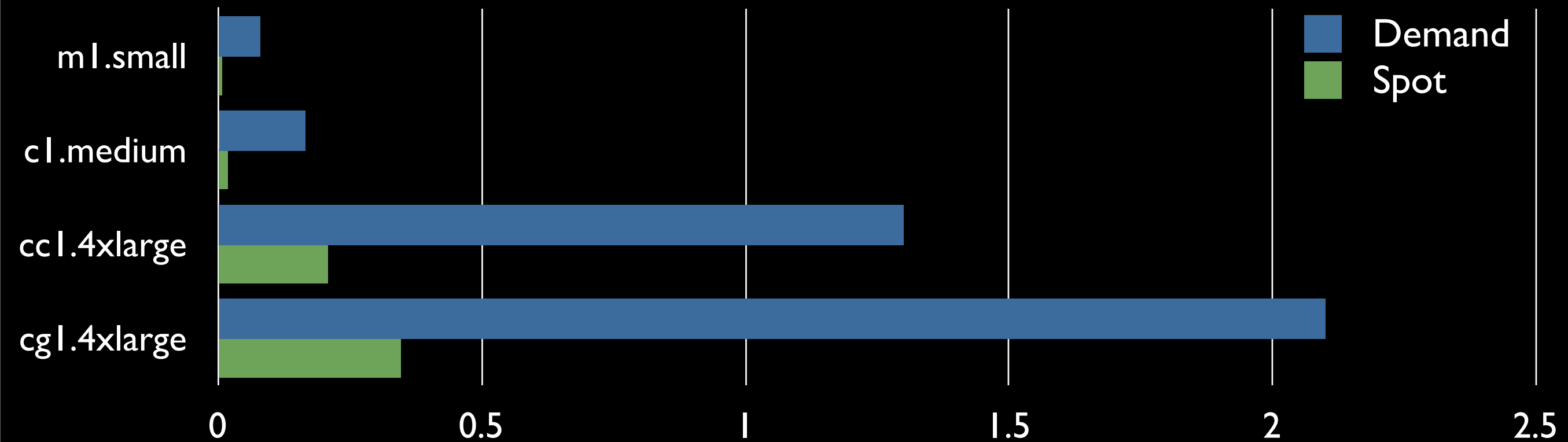
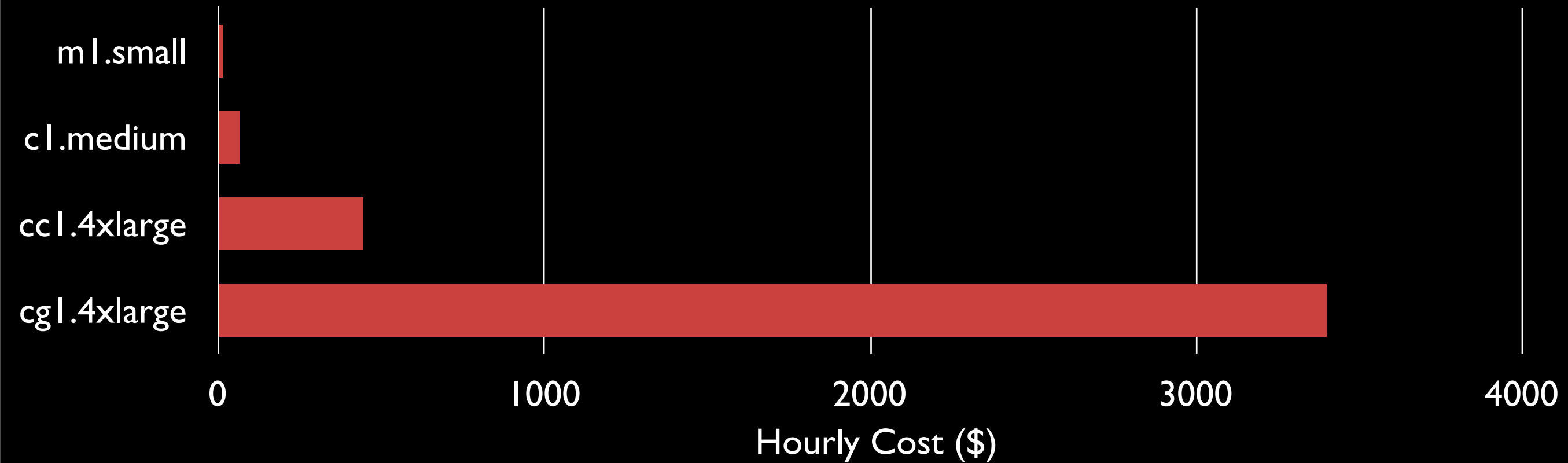
Starting pw len 8

TOTAL: 30.18B/s



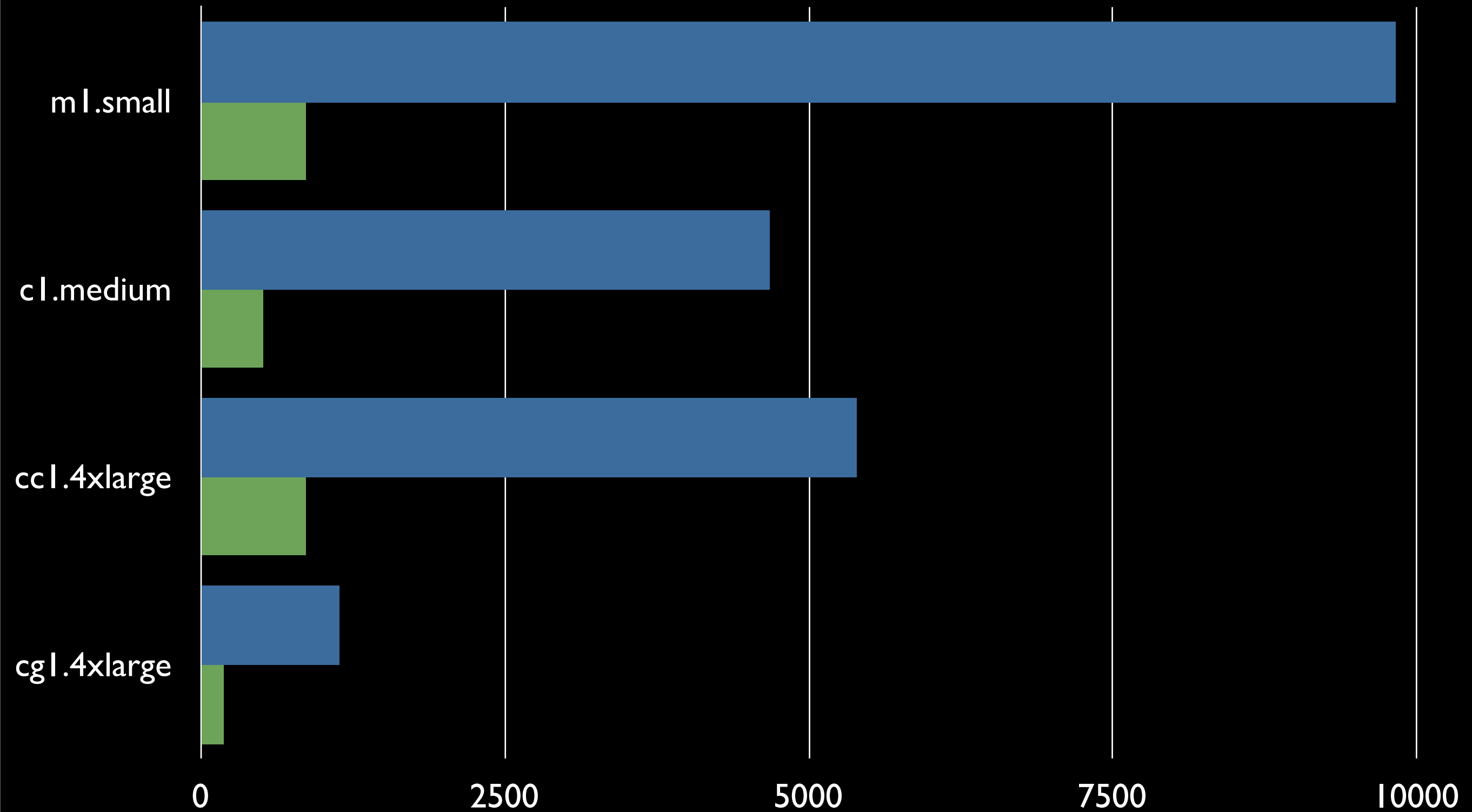
Amazon EC2 Benchmarking

Cracking Rate (M/sec)



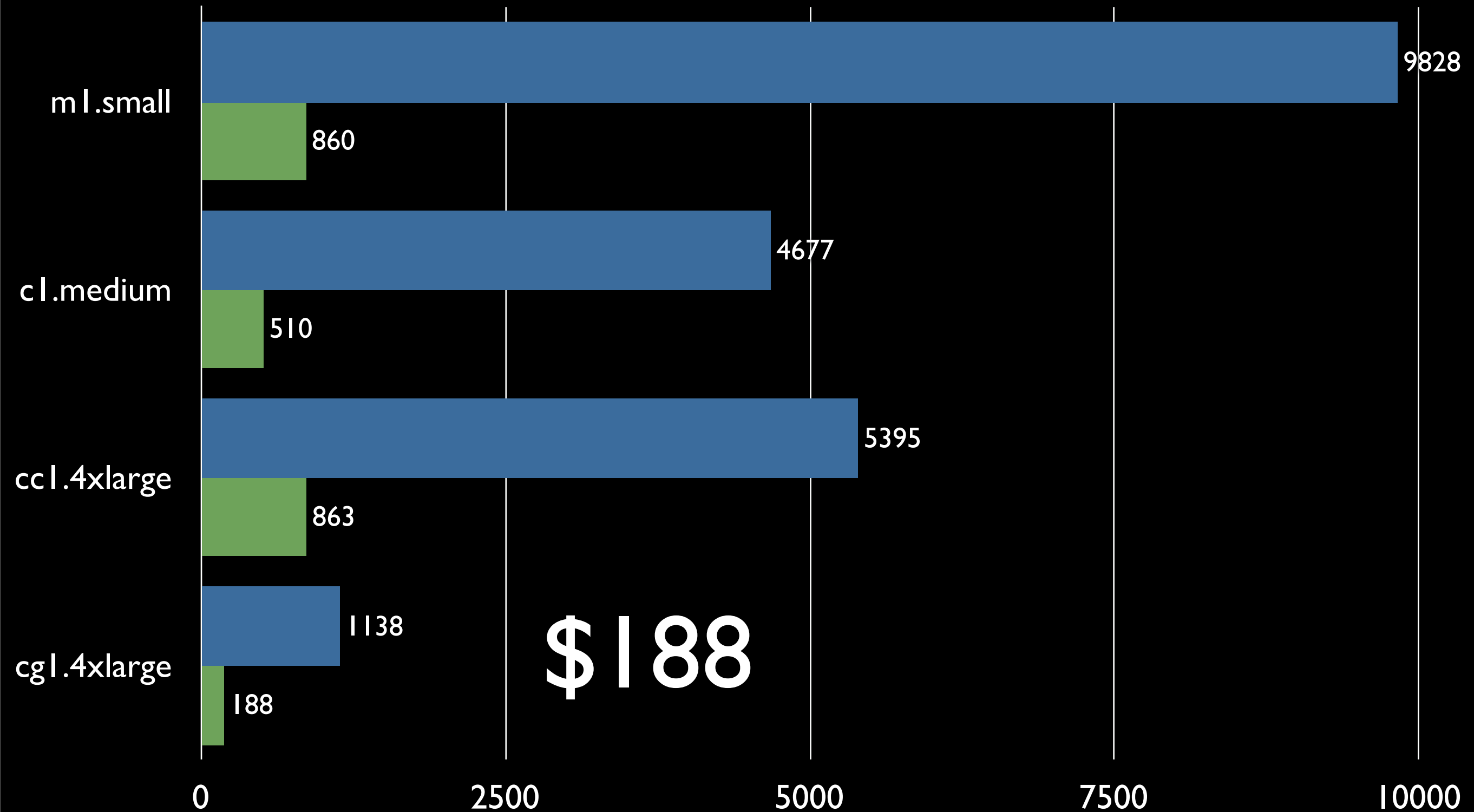
Amazon EC2 Benchmarking

Cost to Crack NTLM len8 (\$)



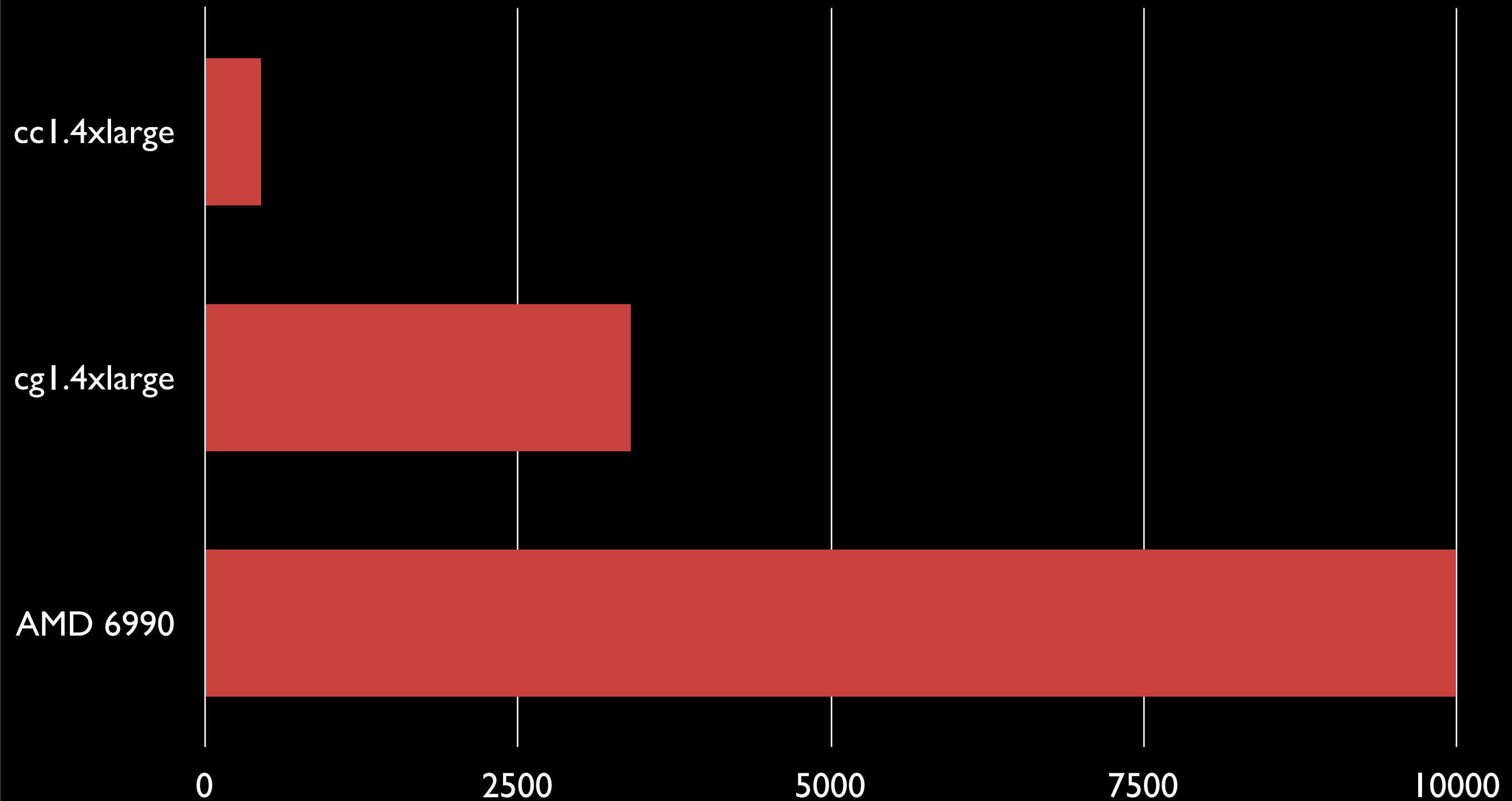
Amazon EC2 Benchmarking

Cost to Crack NTLM len8 (\$)

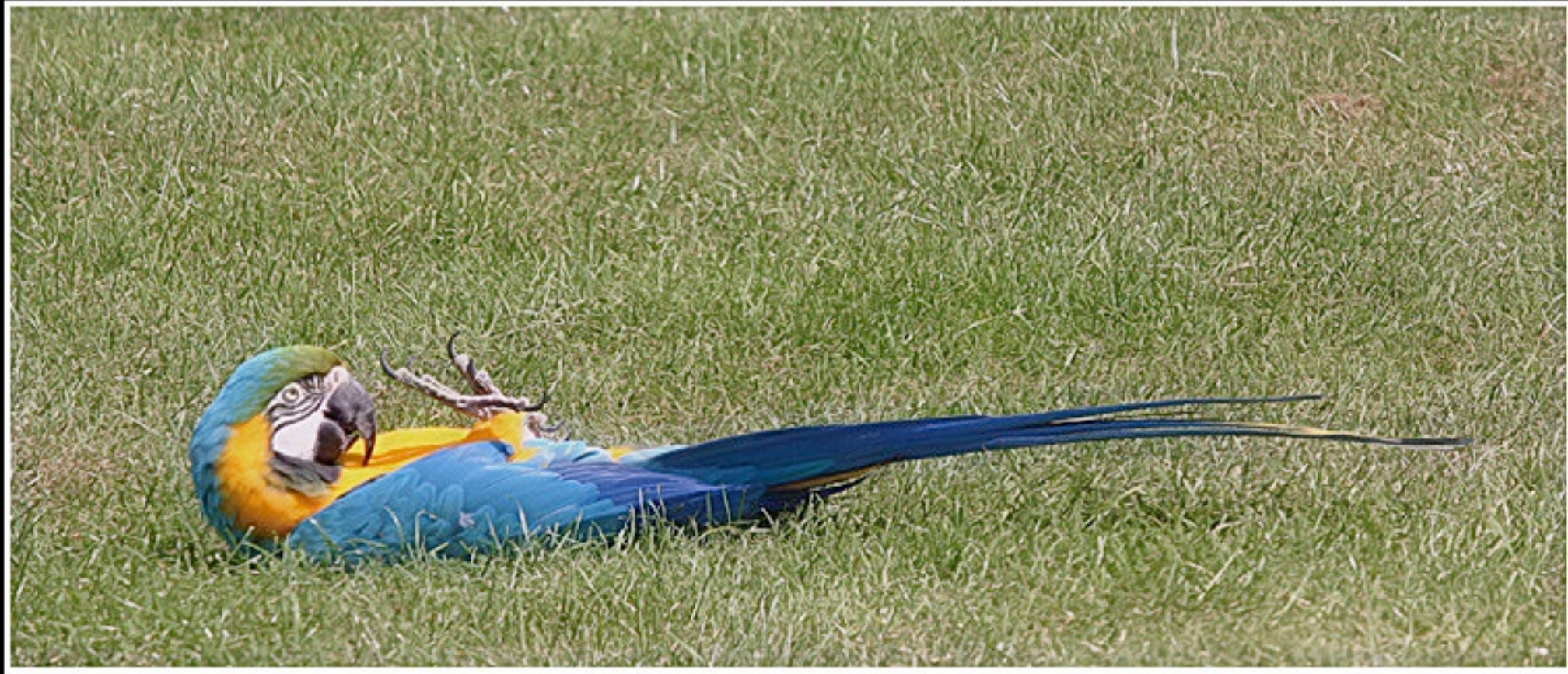


But...

Cracking Rate (M/sec)



Rainbow Tables

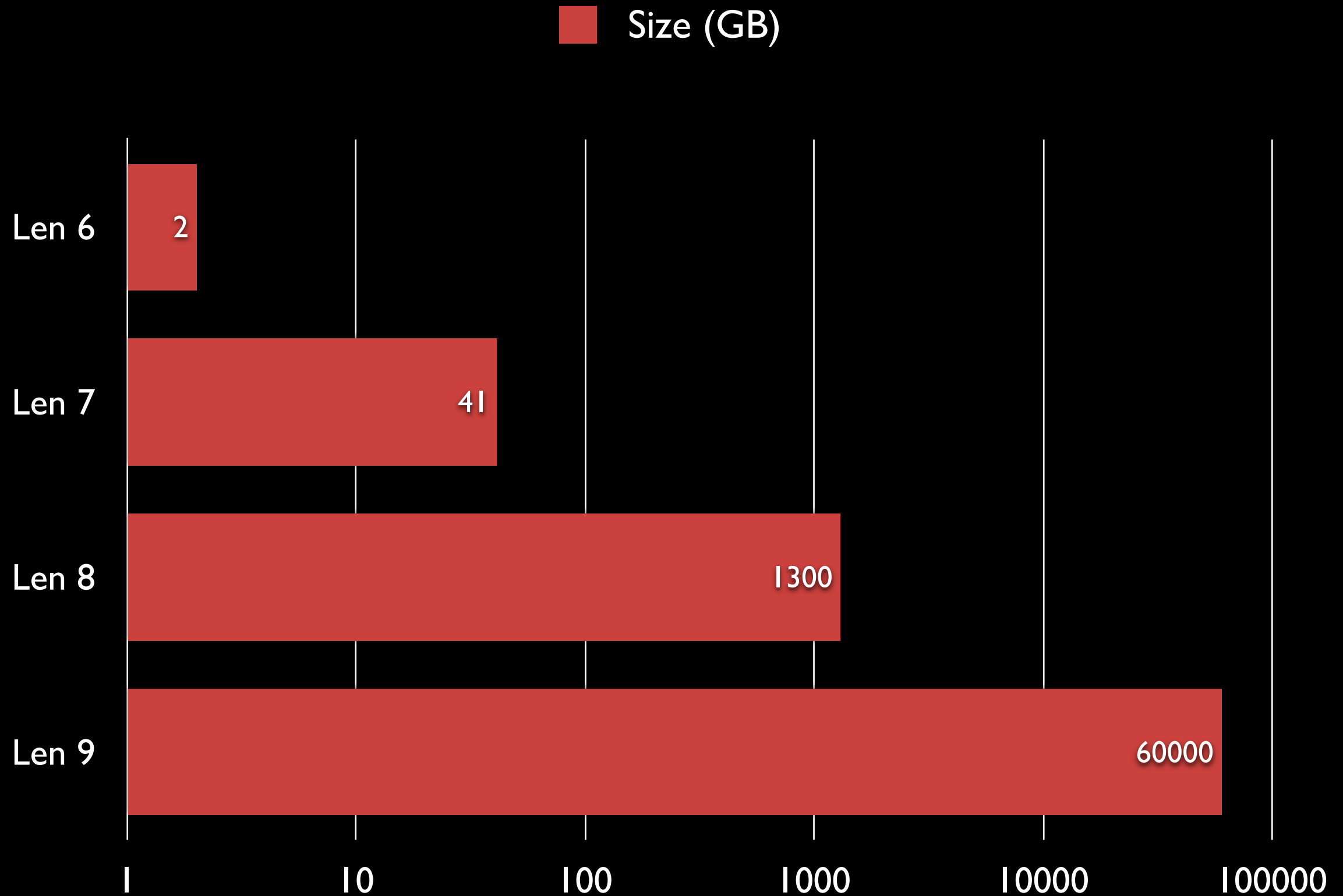


Alan Turvey 2005

Monty Pythons Dead Parrot Sketch

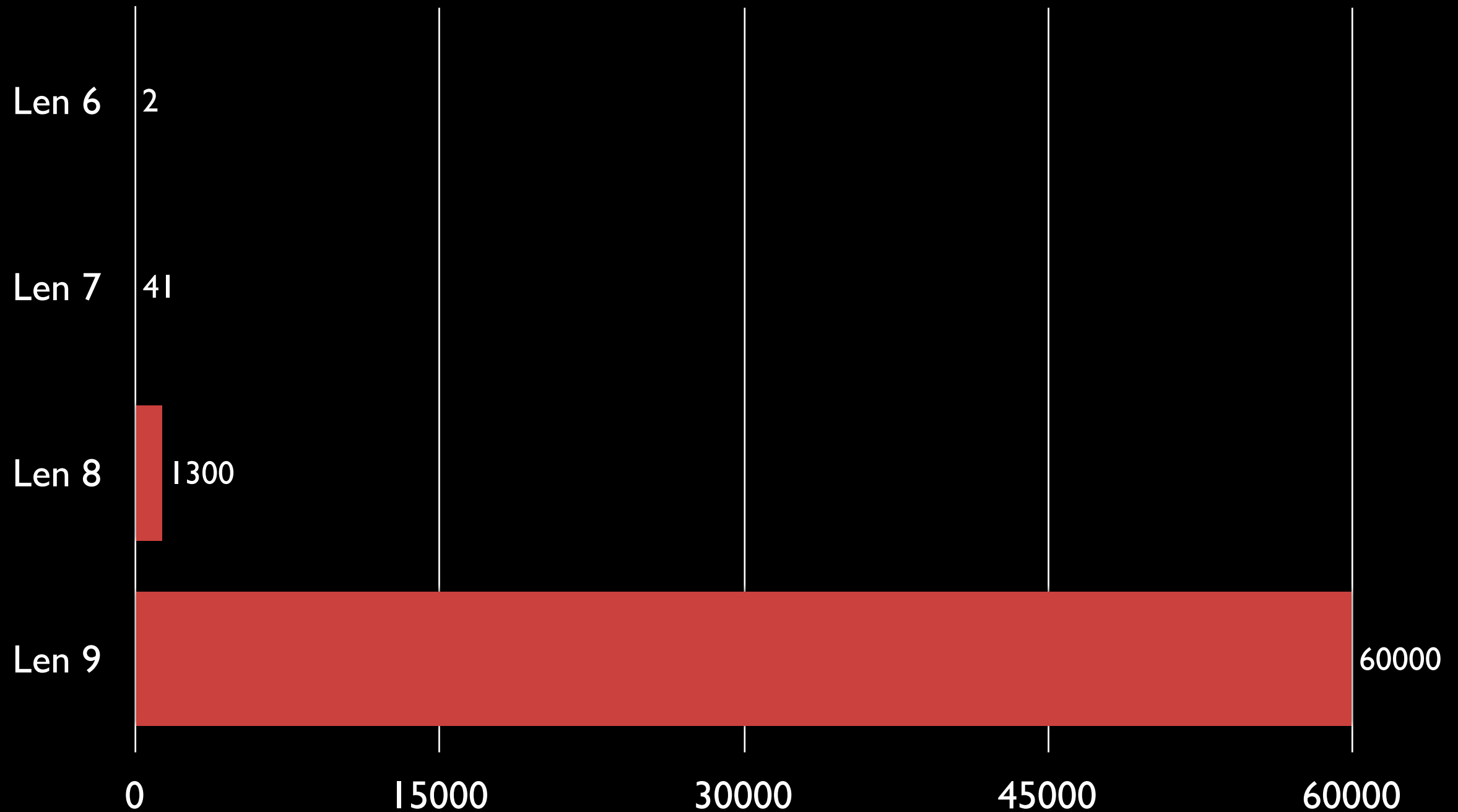
Unsalted hashes only?
Or static salts...
“Administrator”

Rainbow Table Size



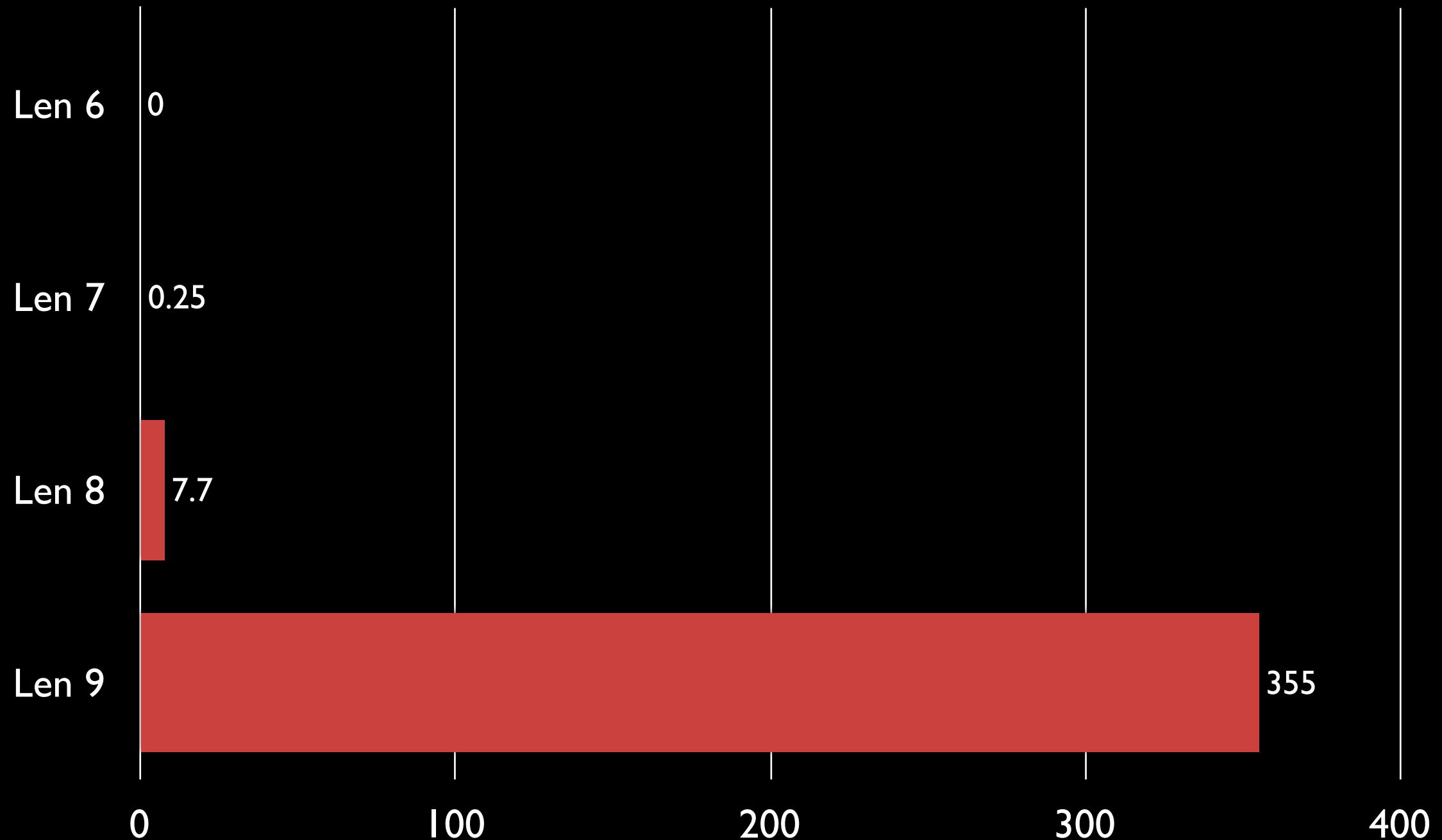
Rainbow Table Size

■ Size (GB)



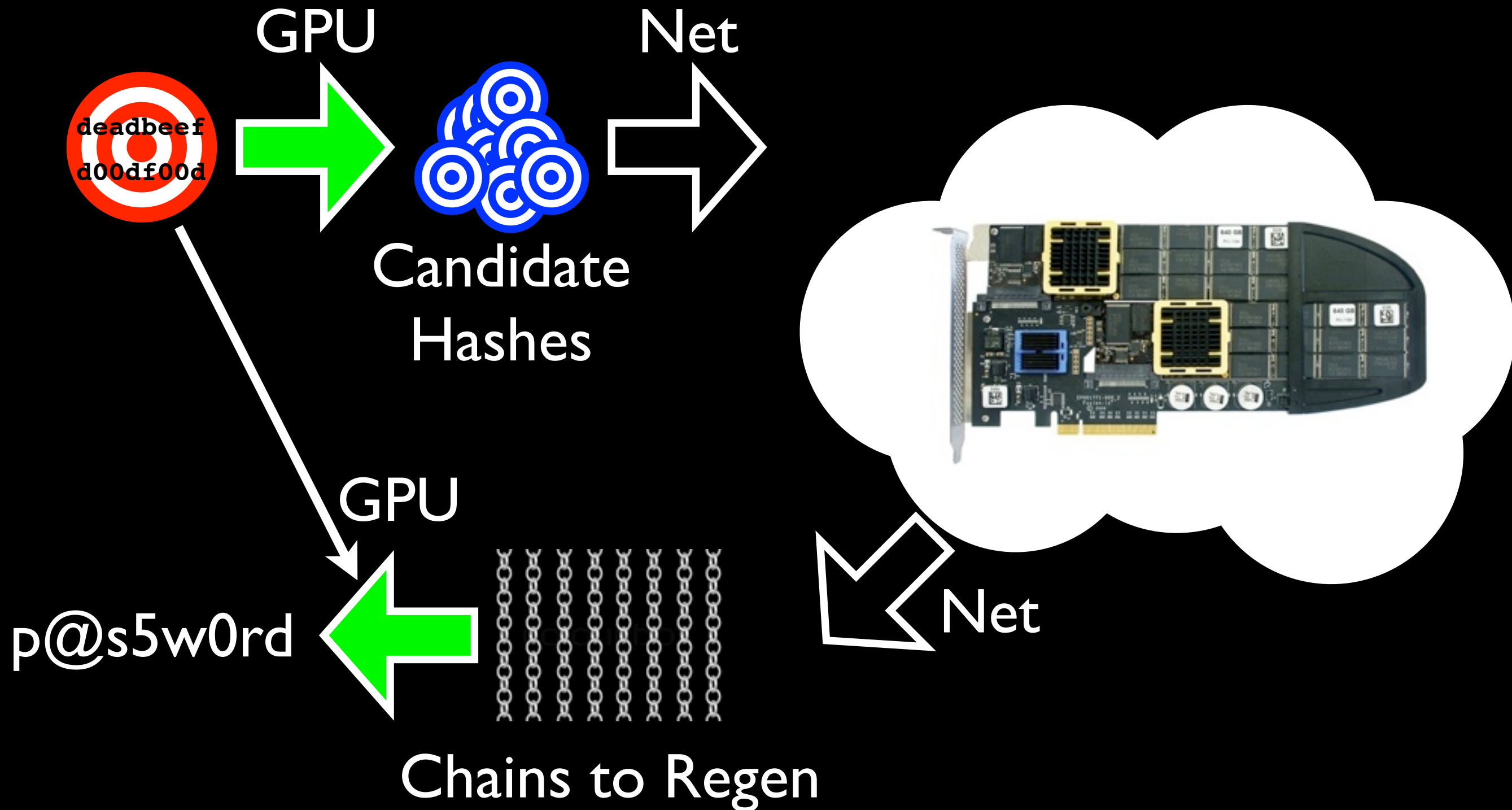
Rainbow Table Download Time

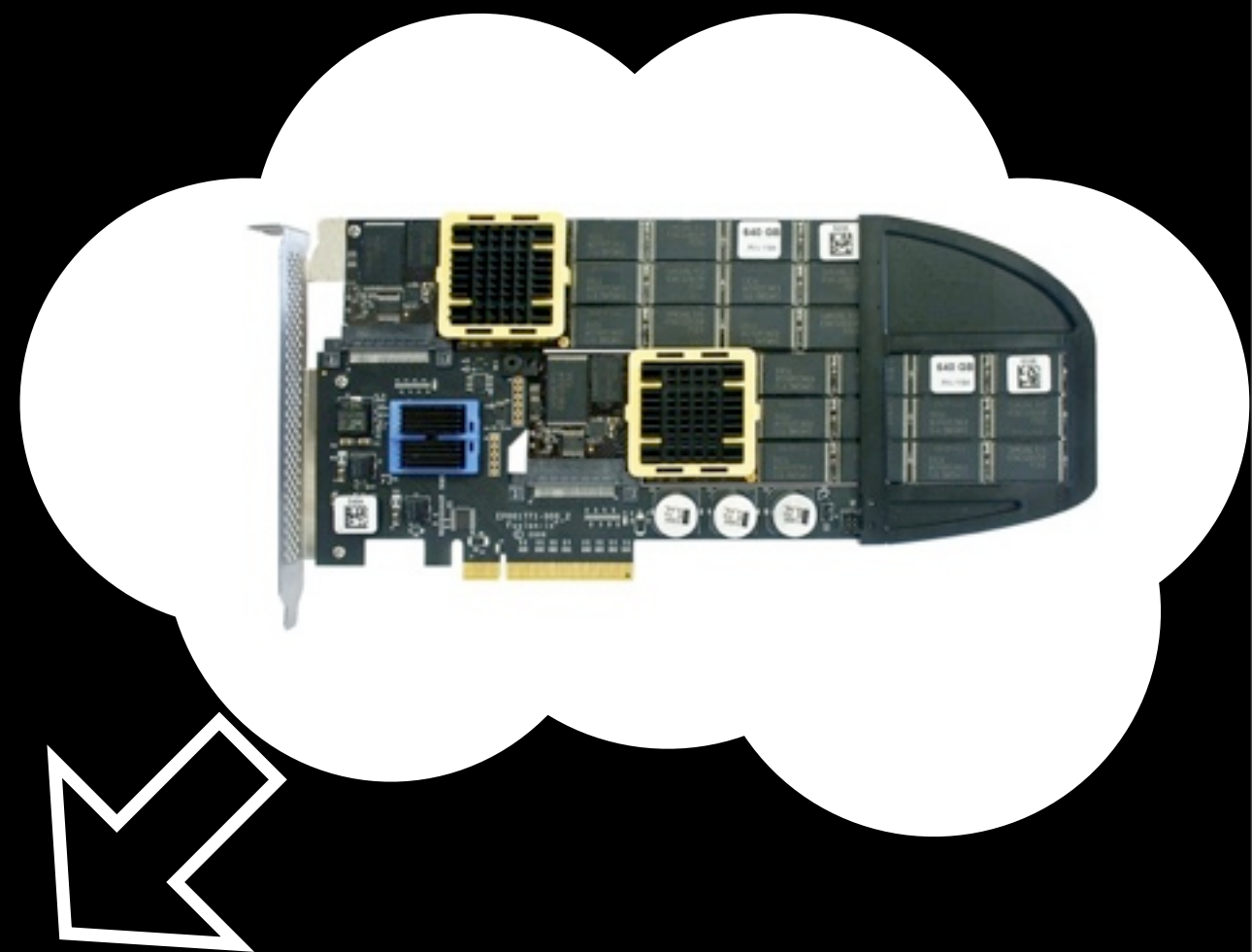
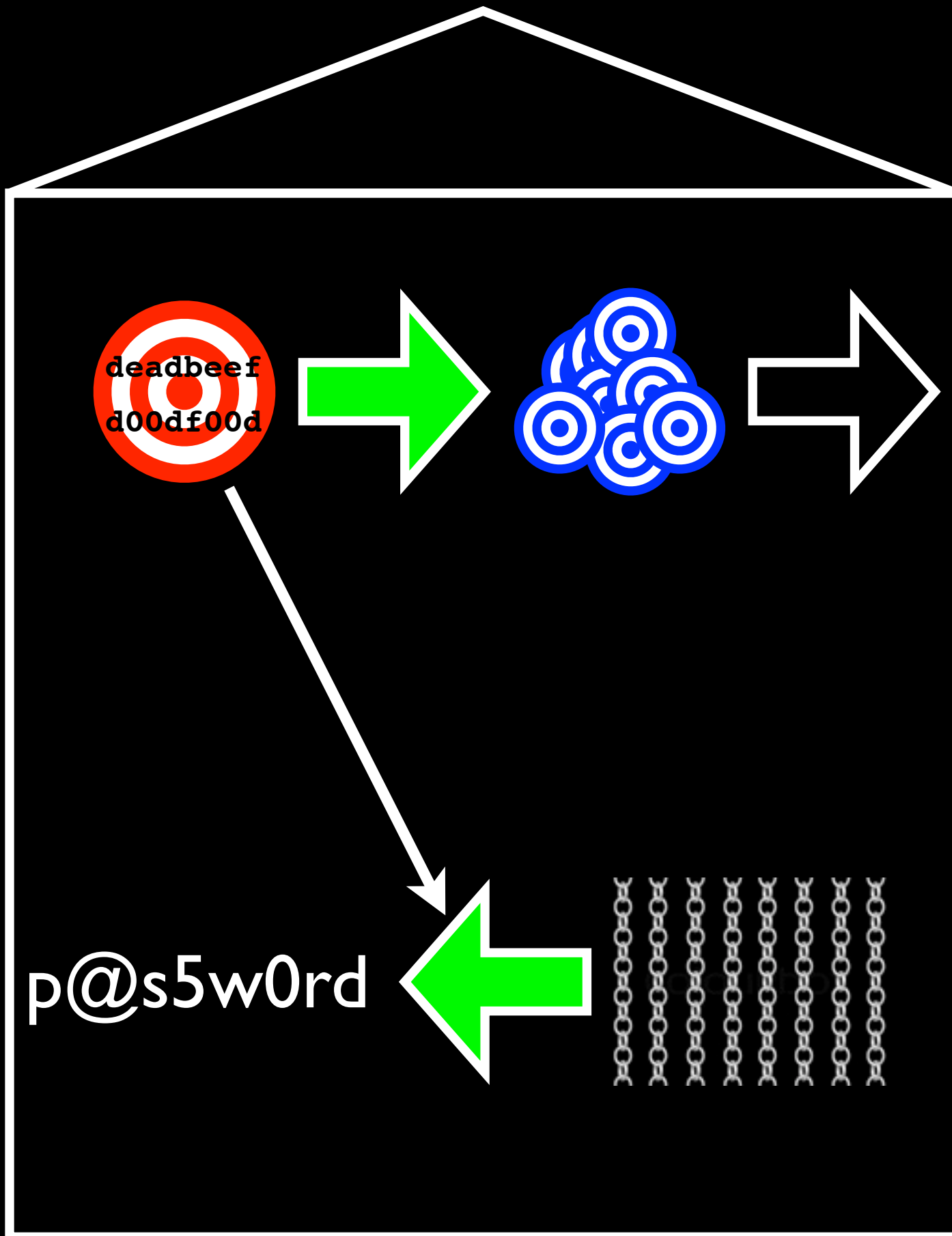
■ Time (Days, 20Mbit)



WebTables

“Tables in the Cloud”





WebTables

<https://webtables.cryptohaze.com>

- Instant access - no table downloads!
- Faster table searching
- Supports very large tables

Defenses

- Salt your passwords
- Salts **MUST** be fully random!
- Iterate your hashes

Final Thoughts

- Be Excellent!
- Open Source enhances resumes
- It takes time to be good
- Salt your passwords
- <http://plaintextoffenders.com/>

Ways to find out more

- cryptohaze.com
- webtables.cryptohaze.com
- bitweasil@cryptohaze.com
- [#cryptohaze on irc.freenode.net](https://irc.freenode.net/#cryptohaze)

