

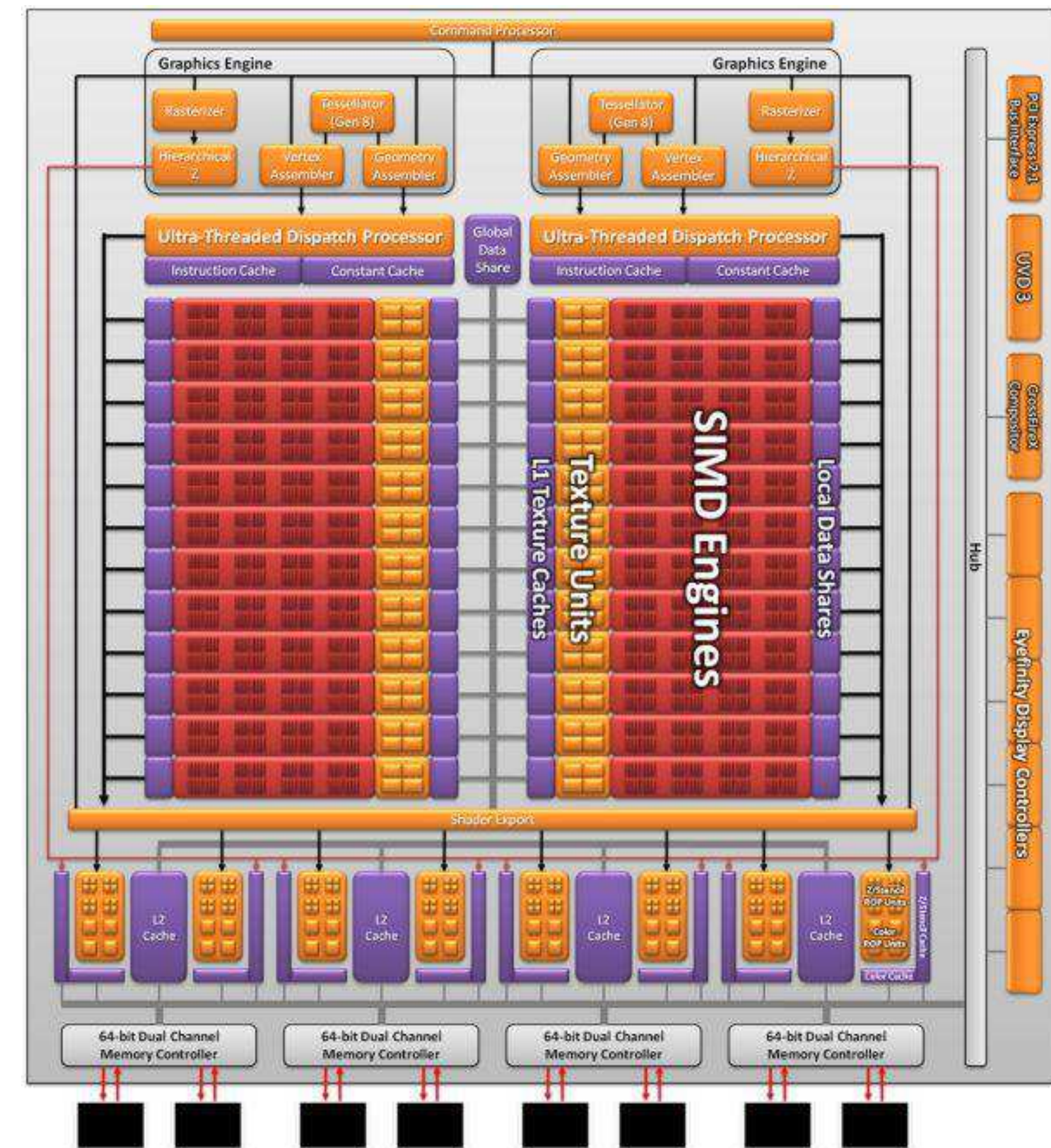
Crack Me If You Can: Using GPU Machines to Crack Passwords

Jihyun An, Charles Bristol, Mudit Buch, Madison Van Horn,
Advisor: Dr. Melissa Danforth Assistant: Alfonso Puga

Background

➤What is a GPU?

➤GPU, short for graphic processing unit, is an electric circuit used for accelerated image creation; however, due to its increased speed we can use it to crack passwords faster than the normal CPU (central processing unit).



➤ATI Radeon HD6970 diagram (anandtech.com) and picture (pcpro.co.uk)

➤How do you crack a password?

➤The first step to cracking a password using a GPU is obtaining the user database containing the different hashed passwords. Afterwards, you can use a GPU to recover the passwords using these attacks:

- Dictionary Attack:** It uses a catalog made up of a list of common passwords and/or different dictionary words.
- Masks:** It adds to the dictionary attack by generating different sequences of characters either before or after the word from the dictionary attack.
- Brute force attacks:** Generates random sequences of characters in order to crack the password.

➤How is a password encrypted?

- Hashing:** It converts the password into a pseudo-random sequence of characters. The hashes are stored in the user database.
- Salts:** It is random data added to the password before it is hashed in order to make the password harder to crack.

Problems

- People tend to use short and/or common passwords to remember them. They don't realize it makes it easier for GPU cracking.
- People also use these same passwords in various accounts

Solutions

- Your password should include symbols, upper and lower case letters, and digits. The password must be at least 15 characters long to have a strong password.
- Dice words:** They are compound dictionary words mixed in with other characters in order to make the password easier to remember but harder to crack.
- Password locker:** It is a secure database which requires you to remember one complicated password but grants you access to all your other passwords.

Objectives and Methods

➤Comparing two different GPUs with different stream processors to see the different recovery rates.

- NVIDIA – Used with Autocad and other less graphically intensive programs.
- ATI Radeon – Used for 3D gaming which makes it have a faster recover rate. The 3D gaming operations are more suited for password cracking.

➤Using different dictionaries to see which one is easier to crack passwords.

- example.dict (129,988 words)
- dic94.txt also known as large.dict on ATI (869,232 words)
- example.dict & password.lst (133,545 words)

➤Creating our own user data base with easy, medium, and hard passwords and seeing what the ATI machine is able to crack.

- We all chose a password we thought was easy, medium, and hard, and we used sha1 algorithm to generate the hashes.
- With the generated database, we used dictionary, a6, a7, and a3 attacks to crack the passwords.
- A6: add characters at the end of the dictionary word
- A7: add characters at the beginning of the dictionary word
- A3: brute force attack

➤Comparing different recovery rates of hashing algorithms.

- sha1: Stands for secure hash algorithms and is the most used algorithms. In an attack in 2005, it took less than 2^{69} operations to brute force the algorithm.
- sha256: Designed by the NSA and is over a decade old.
- sha512: Is one of the slowest out of the sha family.
- md5: It is considered cryptographically broken and unsuitable for further use.

Results and Conclusions

Table 1: NVIDIA VS. ATI with large.dict

| Algorithm | Attack | NVIDIA | ATI |
|-----------|---------------------|-----------------------|-------------------------|
| sha1 | Dictionary | 4 min 44 sec. | 15 sec. 60004/s |
| | Append 1 character | 1 hr. 32 min 4899/s | 34 sec. 1396.7k/s |
| | Append 2 characters | 2 days 4963/s | 14 min 31 sec 1691.1k/s |
| sha256 | Dictionary | 8 min 6 sec 1823/s | 21 sec 82368/s |
| | Append 1 character | 3 hr. 13 min 2349/s | 1 min 21 sec. 621.8k/s |
| | Append 2 characters | 4 days 6 hr. 2361/s | 23 min 17 sec. 639.3k/s |
| sha512 | Dictionary | 34 min 22 sec. 416/s | 40 sec 23337/s |
| | Append 1 character | 15 hr 34 min 286/s | 4 min 20 sec. 111.5k/s |
| | Append 2 characters | 20 days 15 hr 488/s | 2 hr. 23 min 111.0k/s |
| md5 | Dictionary | 2 min 56 sec 5284/s | 14 sec 134.9k/s |
| | Append 1 character | 38 min 57 sec 11445/s | 22 sec. 2210.5k/s |
| | Append 2 characters | 20 hr. 7 min 11795/s | 8 min 10 sec 2935.5k/s |

The ATI was much faster than the NVIDIA because of these two reasons:

- ATI had two GPU cards while NVIDIA had only one
- People have made GPU rigs with 25 ATI cards to increase the cracking rate.
- ATI is more suited for cracking passwords while NVIDIA is more for Autocad graphics and architectural drawing.

Table 2: NVIDIA with example.dict and password.lst

| Attack | md5 | sha1 |
|---------------------|----------------------|-----------------------|
| Dictionary | 49 sec. 2743/s | 1 min 7 sec. 1935/s |
| -a 6 ?l | 5 min 35 sec 10886/s | 12 min 27 sec 4775/s |
| -a 6 ?d | 2 min 34 sec 9161/s | 5 min 15 sec 4376/s |
| -a 6 ?u | 5 min 34 sec 10865/s | Approx. 12 min 13 sec |
| -a 7 ?d or ?l or ?u | 50 min 45 sec 1139/s | Approx. 2 hr. 6 min |
| -a 6 ?l?l or ?u?u | 2 hr. 6 min | Approx. 5 hr. 3 min |
| -a 6 ?d?d | 19 min 14 sec | Approx. 45 min 35 sec |
| -a 7 ?l?l or ?u?u | 2 hr. 6 min | 5 hr. 10 min |
| -a 7 ?d?d | | 2 hr. 1 min |

➤The md5 algorithm was a lot faster to crack than the sha1 algorithm.

➤It's faster to find characters that are after the dictionary word than it is to find ones that are before the word (with this GPU program).

➤Adding more characters is slower due to the combination of characters increasing.

➤(number of characters in character set)^{# of characters}

- 1 lower letter = 26^1 combinations
- 2 lower letters = 26^2 combinations

Table 3: Recovery Time of Our Chosen Passwords (ATI)

| Password | Time | Password | Time |
|----------|--------------|----------|-----------------------|
| madi | 1 sec. | jan2597 | 1 hr. 35 min 5 sec. |
| monster | 1 sec. | Password | 4 hr. 26 min 8 sec. |
| jennyan | 7 sec. | Jan563 | 4 hr. 29 min 29 sec |
| mudit | 12 sec | Madi97 | 10 hr. 31 min 55 sec. |
| apple123 | 1 min. 4 sec | din436M | 6 days 14hr 1m 30s |
| pizzapie | 5 min 2 sec. | | |

Examples of Strong Passwords:

M@rBr@M238 a24Brg31.hI M@R32vZX2011Aug C0RnT0RtillAr85
my4NQ#4ha90G~7 EnqI80AedpF9Pf2

➤The strength of the passwords depends on the size of the dictionary and the number of GPU cards used by the cracker.

➤There are massive dictionaries with hundreds of millions of words including "nonsense words" that may be able to crack these passwords.

Acknowledgements and References

➤Chevron and NSF for funding REVS-UP

➤GPU Program: oclHashcat-plus @ <http://hashcat.net/oclhashcat-plus/>



A portion of the 25 GPU rig. The image is from bitcointalk.org.