

Quebra de Hashs

FELIPE TEIXEIRA

GUILHERME COUSIN

MURILO SCHMALFUSS

Metodologia

- ▶ Utilização do OpenMP para a paralelização dos laços de iterações
- ▶ Para a criação das hashes utilizamos a função md5 da biblioteca md5.h da openssl libcrypto

Hardware utilizado

- ▶ H2106-G7 Node: 2U chassis, AMD quad socket SAS/Raid 0,1 on board
- ▶ 4 x Opteron 6376 16-core 2.3 GHz/16M
- ▶ 128GB Memory (32 x 4GB DDR3 DIMM 1600MHz)

Hardware utilizado

```
 1 [|||||100.0%] 17 [|||||100.0%] 33 [|||||100.0%] 49 [|||||100.0%]
 2 [|||||100.0%] 18 [|||||100.0%] 34 [|||||100.0%] 50 [|||||100.0%]
 3 [|||||100.0%] 19 [|||||100.0%] 35 [|||||100.0%] 51 [|||||100.0%]
 4 [|||||100.0%] 20 [|||||100.0%] 36 [|||||100.0%] 52 [|||||100.0%]
 5 [|||||100.0%] 21 [|||||100.0%] 37 [|||||100.0%] 53 [|||||100.0%]
 6 [|||||100.0%] 22 [|||||100.0%] 38 [|||||100.0%] 54 [|||||100.0%]
 7 [|||||100.0%] 23 [|||||100.0%] 39 [|||||100.0%] 55 [|||||100.0%]
 8 [|||||100.0%] 24 [|||||100.0%] 40 [|||||100.0%] 56 [|||||100.0%]
 9 [|||||100.0%] 25 [|||||100.0%] 41 [|||||100.0%] 57 [|||||100.0%]
10 [|||||100.0%] 26 [|||||100.0%] 42 [|||||100.0%] 58 [|||||100.0%]
11 [|||||100.0%] 27 [|||||100.0%] 43 [|||||100.0%] 59 [|||||100.0%]
12 [|||||100.0%] 28 [|||||100.0%] 44 [|||||100.0%] 60 [|||||100.0%]
13 [|||||100.0%] 29 [|||||100.0%] 45 [|||||100.0%] 61 [|||||100.0%]
14 [|||||100.0%] 30 [|||||100.0%] 46 [|||||100.0%] 62 [|||||100.0%]
15 [|||||100.0%] 31 [|||||100.0%] 47 [|||||100.0%] 63 [|||||100.0%]
16 [|||||100.0%] 32 [|||||100.0%] 48 [|||||100.0%] 64 [|||||100.0%]
Mem[||| 1708/128938MB] Tasks: 118, 5372 thr; 3656 running
Swp[ 0/0MB] Load average: 3207.05 2227.17 2163.80
Uptime: 01:55:20

PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
 1 root 20 0 84212 4004 2496 S 0.0 0.0 0:07.64 /sbin/init
723 root 20 0 17760 1164 528 S 0.0 0.0 0:00.08 upstart-udev-bridge --daemon
725 root 20 0 15336 1380 728 S 0.0 0.0 0:00.08 /sbin/udev --daemon
806 root 20 0 15264 852 320 S 0.0 0.0 0:00.00 /sbin/udev --daemon
807 root 20 0 15264 864 332 S 0.0 0.0 0:00.00 /sbin/udev --daemon
1036 messagebu 20 0 81644 1560 824 S 0.0 0.0 0:00.01 dbus-daemon --system --fork --activation=upstart
1043 syslog 20 0 237M 1492 1052 S 0.0 0.0 0:00.13 rsyslogd -c5
1045 syslog 20 0 237M 1492 1052 S 0.0 0.0 0:00.10 rsyslogd -c5
1047 syslog 20 0 237M 1492 1052 S 0.0 0.0 0:00.00 rsyslogd -c5
1048 syslog 20 0 237M 1492 1052 S 0.0 0.0 0:00.00 rsyslogd -c5
1099 root 20 0 19200 1004 728 S 0.0 0.0 0:00.00 rpcbind -w
1137 root 20 0 45852 2840 2256 S 0.0 0.0 0:00.00 /usr/sbin/sshd -D
1180 statd 20 0 27420 2064 1300 S 0.0 0.0 0:00.00 rpc.statd -L
1184 root 20 0 15188 436 196 S 0.0 0.0 0:00.00 upstart-socket-bridge --daemon
1303 root 20 0 9700 872 740 S 0.0 0.0 0:00.00 /sbin/getty -8 38400 tty4
1322 root 20 0 9700 872 740 S 0.0 0.0 0:00.00 /sbin/getty -8 38400 tty5
1330 root 20 0 9696 864 740 S 0.0 0.0 0:00.00 /sbin/getty -8 38400 tty2
1331 root 20 0 9700 864 740 S 0.0 0.0 0:00.00 /sbin/getty -8 38400 tty3
1335 root 20 0 9700 872 740 S 0.0 0.0 0:00.00 /sbin/getty -8 38400 tty6
1344 root 20 0 4328 680 552 S 0.0 0.0 0:00.00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
1345 daemon 20 0 10576 348 216 S 0.0 0.0 0:00.00 atd
1346 root 20 0 12780 780 608 S 0.0 0.0 0:00.00 cron
1368 whoopsie 20 0 177M 4300 3040 S 0.0 0.0 0:00.01 whoopsie
1370 root 20 0 15980 772 564 S 0.0 0.0 0:07.42 /usr/sbin/irqbalance
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit
```

Código

- ▶ #pragma omp parallel for shared(tam, hashes_comp) private(md, stringMD, digest, i, j, k, l, m, n, o)

```
for(i = 0; i < tam; i++){
    for(j = 0; j < tam; j++){
        for(k = 0; k < tam; k++){
            for(l = 0; l < tam; l++){
                stringMD[0] = caracteres[i];
                stringMD[1] = caracteres[j];
                stringMD[2] = caracteres[k];
                stringMD[3] = caracteres[l];
                stringMD[4] = '\0';
```

Código (geração da Md5 para palavra gerada)

- ▶ `MD5((unsigned char*)stringMD, strlen(stringMD), (unsigned char*)&digest);`
 `for(o = 0; o < 16; o++){`
 `printf(&md[o*2], "%02x", (unsigned int) digest[o]);`

Código (comparação)

```
// Comparação com as hashes
for(o = 0; o < NUM_HASH; o++){
    if(memcmp(md, hashes_comp[o], sizeof(char)*33) == 0){
        #pragma omp critical
        {
            printf("%s %s\n", md, stringMD);
        }
    }
}
```

Tempo da Aplicação

- ▶ Tempo de quebra das 240 hashes foi de aproximadamente 19 horas
- ▶ O número de possibilidades de senhas com um alfabeto de 85 caracteres com uma combinação de 6 é $85^6 = 3771495155625$

Quebra de Hashs

FELIPE TEIXEIRA

GUILHERME COUSIN

MURILO SCHMALFUSS