Quebra de Hashes md5 versão distribuída

Andrei Costa, Leonardo Corrêa, Vinícius Santos

22 de Agosto de 2013

Modelo:

- C
- Socket
- Pthread
- Dois Códigos: Manager e Node

- Manager:
  - Tem Hashes e IP:Porta, passados por entrada
  - Distribui Trabalhos para os Nodes
- Node:
  - Tem algoritmo do md5
  - Fica escutando numa porta
  - Recebe Trabalho e retorna a resposta ou que falhou
- Trabalho:
  - Um hash
  - Um Node, com IP e Porta
  - Quantidade de chars para testar
  - Faixa que tentará resolver

Exemplo: Manager envia "6 1 2 0b4e7a0e5fe84ad35fb5f95b9ceeac79"
Nodo busca com 6 chars começando por bc (posição 1 e 2 da string de chars)

- Manager
- Duas Pilhas, de Nodes e de Hashes
- Verificar retorno de Nodes:
  - Se resolveu adiciona na Trie de resolvidos
  - Se não:
    - Se era de 4 chars: cria 86 novas de 5 chars
    - Se era de 5 chars: cria 86*86 novas de 6 chars

Node:

- Cálculo de md5
- Parte crítica implementada em Assembly
- Não Paralela

Hardware:

- Várias execuções independentes
- Uma principal:
  - Lab 2
  - 15 Computadores Dual-Core
  - Durante todo final de semana

Performance:

- Impossível contabilizar, diversas execuções independentes
- Cálculo do pior caso num Pentium Dual-Core T4300 2.10GHz:
  - 4 char: 21 segundos
  - 5 char: 86*21 segundos $\approx$ 15 minutos
  - 6 char: 86*86*21 segundos $\approx$ 22 horas

Quebra de Hashes md5 versão distribuída

Andrei Costa, Leonardo Corrêa, Vinícius Santos

22 de Agosto de 2013