Instituto de Matemática e Estatística

EP1 - MAC0219

Implementação de Algoritmos de Criptografia e Codificação Paralelos Usando CUDA

Professor: Alfredo Goldman

Alunos: Bruno Sesso

Gustavo Estrela de Matos

São Paulo, 2 de Junho de 2017

Conteúdo

1 Introdução

Este trabalho tem como objetivo a paralelização e análise de desempenho de algoritmos de criptografia e codificação para serem rodados em GPUs. O código desenvolvido utilizará a biblioteca *Compute Unified Device Architecture* (CUDA), e portanto será compatível apenas com GPUs NVIDIA.

Pensando na arquitetura *multiple instruction single data* (MISD), escolhemos três algoritmos em que os dados não possuem grandes dependência entre si, e portanto podem ser separados mais facilmente para serem processados em paralelo. Os três algoritmos escolhidos foram:

- **Base64**: um algoritmo de codificação;
- **Rot13**: também um algoritmo de codificação;
- **Vigenere**: um algoritmo de cifração.

Para analisar a paralelização dos algoritmos a nossa principal métrica foi o tempo de execução ao processar arquivos de texto. Os três algoritmos escolhidos não tem grandes dependências ao conteúdo lido, portanto escolhemos arbitrariamente uma versão em texto puro da bíblia para medir tempos de execução. Para garantir significância estatística utilizamos o programa *perf*, que nos permite apresentar resultados médios de rodadas do algoritmo.

O computador usado nos testes...

2 Algoritmos Escolhidos

2.1 Base64

2.2 Rot13

2.3 Vigenere

3 Código Paralelo

3.1 Base64

3.2 Rot13

3.3 Vigenere

4 Discussão dos Resultados

5 Conclusão