# Последовательная программа

При запуске в режиме тестирования скорости производится шифрование блока данных(длина одного блока DES составляет 64 бита) на 1 000 000 наборов последовательных ключей. Тестирование производилось на процессоре Intel Core i3 2310M (2.1GHz). За один проход обрабатывалось 32 ключа (один набор). В результирующее время не входит инициализация и подготовка данных. Результаты:

|  |  |  |
| --- | --- | --- |
| 1. Последовател. прог-ма | 1. Общее время тестирования | 1. Скорость подбора |
| 1. 1 | 1. 3.282635 | 1. 304633.320488 |

# Реализация с использованием MPI

При запуске в режиме тестирования скорости производится шифрование блока данных на n\*1 000 000 наборов последовательных на каждом процессоре ключей (Старшие биты различны на каждом процессоре). За один проход обрабатывалось 32 ключа (один набор). Тестирование производилось на 2х ядерном Intel Core i3 2310M. Результаты:

|  |  |  |
| --- | --- | --- |
| Количество процессоров n | Общее время тестирования | Скорость подбора |
| 1 | 3.207105 | 311807.697137 |
| 2 | 3.227007 | 619769.311511 |
| 4 | 5.989788 | 667803.261650 |
| 8 | 12.225421 | 654374.195499 |
| 16 | 25.167001 | 635753.143344 |

# Реализация с использованием Open MP

Подбирается 1 000 000 наборов по 32 ключа на каждом потоке.

Результаты:

|  |  |  |
| --- | --- | --- |
| Количество процессов | Общее время тестирования | Скорость подбора |
| 1 | 3.290189 | 303933.907748 |
| 2 | 3.281502 | 609477.001690 |
| 4 | 6.554501 | 610267.661871 |
| 8 | 13.039269 | 613531.326028 |
| 16 | 25.975727 | 615959.661110 |
| 32 | 52.398892 | 610699.936174 |

# Реализация с использованием потоков Posix

Результаты:

|  |  |  |
| --- | --- | --- |
| Количество процессов | Общее время тестирования | Скорость подбора |
| 1 | 3.272789 | 305549.792547 |
| 2 | 3.282805 | 609235.090113 |
| 4 | 6.525544 | 612975.715128 |
| 8 | 13.021544 | 614366.468370 |
| 16 | 26.142455 | 612031.272503 |
| 32 | 52.479744 | 609759.071995 |

# Последовательная программа с использованием SSE2

Использовались 128-битные целые числа(\_\_mm128i). Результаты:

|  |  |  |
| --- | --- | --- |
| 1. Последовател. прог-ма | 1. Общее время тестирования | 1. Скорость подбора |
| 1. SSE | 1. 3.474335 | 1. 1151299.457306 |

# Параллельная программа с использованием GPU

Использовалась реализация стандарта OpenCL от Nvidia.

Характеристики графического процессора:

CL\_DEVICE\_NAME: GeForce GT 520MX

CL\_DRIVER\_VERSION: 301.27

CL\_DEVICE\_MAX\_COMPUTE\_UNITS: 1

CL\_DEVICE\_MAX\_WORK\_ITEM\_DIMENSIONS: 3

CL\_DEVICE\_MAX\_WORK\_ITEM\_SIZES: 1024 / 1024 / 64

CL\_DEVICE\_MAX\_WORK\_GROUP\_SIZE: 1024

CL\_DEVICE\_MAX\_CLOCK\_FREQUENCY: 1800 MHz

|  |  |  |
| --- | --- | --- |
| Вызовы ядра (Внутри ядра подбирается 1 набор ключей(32 ключа)) | 1. Общее время тестирования | 1. Скорость подбора |
| Размер решётки: {1024\*2048}  Вызовы ядра: 1 | 1. 5.865 | 1. 357448.781 |
| Размер решётки: {2048}  Вызовы ядра: 1024 | 1. 6.082 | 1. 344812.890 |
| Размер решётки: {1024}   1. Вызовы ядра: 2048 | 1. 6.243 | 1. 335920.551 |
| Размер решётки: {8192}   1. Вызовы ядра: 1 2. Внутри ядра подбирается 256 наборов | 1. 6.218 | 1. 337271.148 |

Вывод: оптимальная стратегия – увеличение числа узлов решетки.