Consumo Energético En Arquitecturas Multicore. Análisis Sobre Un Algoritmo De Criptografía Simétrica

CACIC 2012

Fernando Romero, Adrian Pousa, Victoria Sanz, Armando De Giusti

Objetivo

Presentar un análisis de consumo energético de dos tipos de arquitecturas multicore:

- Cluster de multicore (MPI)
- GPU (Cuda)

Se utilizó para este análisis el algoritmo de criptografía AES.

Trabajo previo (CACIC 2011) mostrando la Eficiencia de AES-GPU.

Motivación

- Importancia del consumo energético: Mayor demanda de energía por crecimiento en el uso de dispositivos electrónicos.
- Arquitecturas y herramientas paralelas para reducir tiempo de ejecución.
- Más cores o máquinas => Menor tiempo => Mayor consumo.
- Elección de algoritmo + arquitectura que provean mejor relación FLOP/WATT.

AES (Breve descripción)

- Standard muy utilizado.
- Algoritmo de cifrado simétrico por bloques.
- Datos a cifrar/descifrar se dividen en bloques (estado).
- Operaciones a cada estado a partir de una clave inicial y diez claves generadas a partir de la primera.

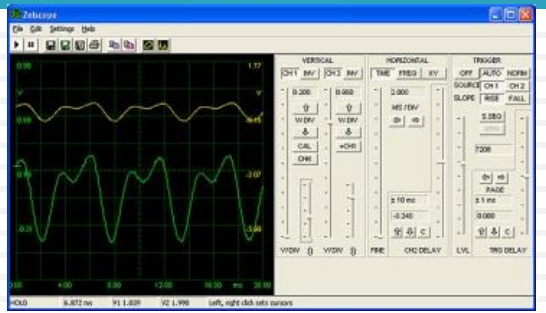
AES (Implementaciones paralelas)

- Cada hilo o proceso cifra/descifra uno o varios estados en forma paralela.
- Dos implementaciones:
  - AES-MPI: sobre cluster de multicore.
  - AES-CUDA: sobre GPU.
- AES-CUDA: Mejor rendimiento en tiempo de ejecución (CACIC 2011)
- Análisis de consumo energético del algoritmo sobre GPU y cluster de multicore.

Metodología - medición consumo

- La energía de ambas arquitecturas fue medida en Joules:
  1 Joule = 1 Watt por Segundo
- Watt es una unidad de potencia que puede calculada como:
  $W = I.V$
- Un Joule o Watt por segundo es la energía que desarrolla una corriente de un Ampere durante un segundo, siendo la corriente impulsada por una diferencia de potencial de un Volt
- Medida indirectamente. Por separado corriente (I) y voltaje(v).

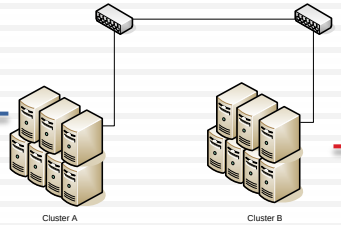
Metodología - medición consumo



Toma corriente

Voltaje (Volt)

Cluster



Maquina GPU

Osciloscopio

Corriente (Ampere)

Pinza transductora
(A la entrada de la fuente)

Muestras:

Voltaje (buffer Bv:10KB – 40ms)

Corriente (buffer Bi:10KB – 40ms)

Intervalo de muestreo:

40ms/10KB = 3,9µs

USB

PC y SW de análisis de señales

Metodología - medición consumo

Osciloscopio

Muestras:

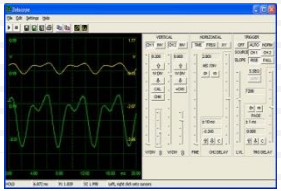
Voltaje (buffer Bv:10KB – 40ms)

Corriente (buffer Bi:10KB – 40ms)

Intervalo de muestreo:

40ms/10KB = 3,9µs

PC y SW de análisis de señales



USB

Watt a partir de Volt y Ampere:

$$B_W[i] = B_I[i] \,.\, B_V[i] \quad \forall\, j \in Z, j \in [0,10240]$$

Valor Eficaz del buffer:

$$\text{RMS} = \sqrt{\frac{1}{T_2 - T_1} \int_{T_1}^{T_2} f(t)^2 dt}$$

Consumo total de la aplicación:

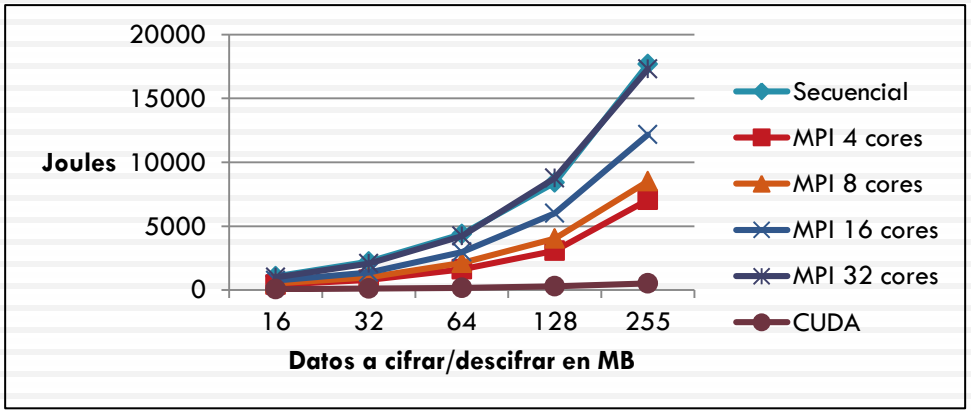
$$Joules = \sum_{k=0}^{Muestras} RMS(Bw_k)$$

Arquitecturas

- AES-secuencial ejecutado sobre:
  - Máquina con Procesador i5 2300 (4 cores físicos) – 8GB RAM.
- AES-MPI ejecutado sobre:
  - Cluster de máquinas con Procesador i5 2300 (4 cores físicos) - 8GB RAM.
  - Conectividad 1Gbit Ethernet.
- AES-CUDA ejecutado sobre:
  - Nvidia Geforce GTX 560TI: 384 SPs, 8 SMs (48 SPs por SM)

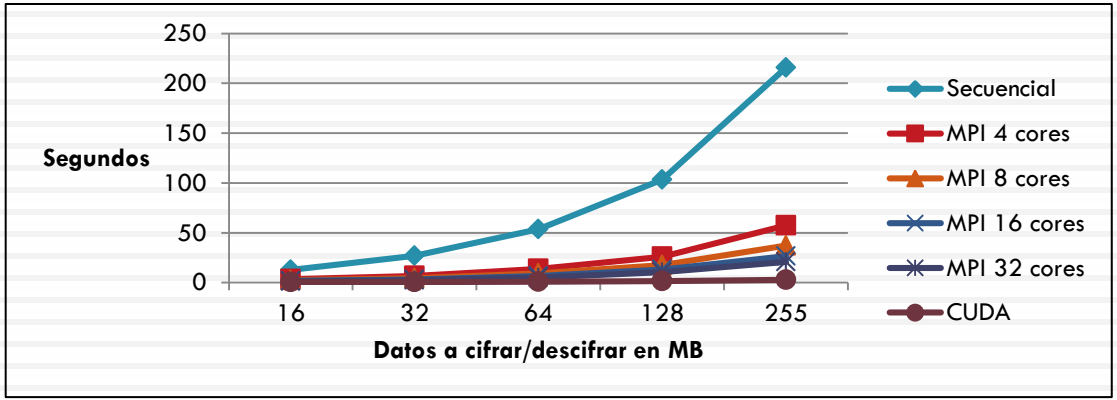
Resultados: Joules de la aplicación

MegaBytes	Secuencial	MPI 4 cores (1 Maquina)	MPI 8 cores (2 Maquinas)	MPI 16 cores (4 Maquinas)	MPI 32 cores (8 Maquinas)	CUDA
16	1073,8454	417,0014	532,4198	743,0065	1000,9787	69,6309
32	2219,3307	801,7640	992,2515	1382,4791	2067,1985	111,0463
64	4375,8023	1634,6110	2113,6083	2979,2766	4232,7257	161,8118
128	8418,3768	3066,8609	4033,8559	5994,1951	8769,7185	294,5490
255	17685,4759	7050,1483	8513,3998	12159,6573	17305,2101	509,1929



Resultados: Tiempo de muestreo (en segundos)

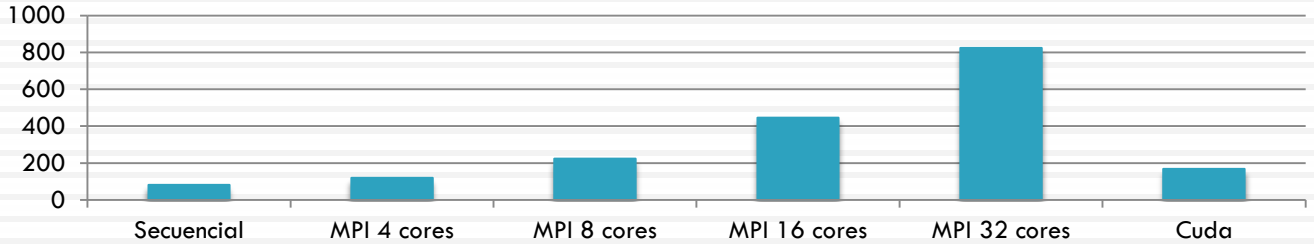
MegaBytes	Secuencial	MPI 4 cores (1 Maquina)	MPI 8 cores (2 Maquinas)	MPI 16 cores (4 Maquinas)	MPI 32 cores (8 Maquinas)	CUDA
16	12,92	3,6	2,56	1,76	1,24	0,44
32	27	6,76	4,44	3,16	2,52	0,68
64	53,52	13,84	9,32	6,64	5,16	0,96
128	103,32	25,84	17,52	13,04	10,48	1,68
255	215,84	57,32	37,08	26,52	20,64	2,92



Resultados

- Watts consumidos por segundo= Joules totales/ tiempo de muestreo

MegaBytes	Secuencial	MPI 4 cores (1 Maquina)	MPI 8 cores (2 Maquinas)	MPI 16 cores (4 Maquinas)	MPI 32 cores (8 Maquinas)	CUDA
16	83,1149	115,8337	207,9764	422,1627	807,2408	158,2520
32	82,1974	118,6041	223,4800	437,4933	820,3168	163,3033
64	81,7601	118,1077	226,7820	448,6862	820,2956	168,5539
128	81,4786	118,6865	230,2429	459,6775	836,8052	175,3267
255	81,9378	122,9963	229,5954	458,5089	838,4307	174,3811
Promedio	82,0978	118,8456	223,6153	445,3057	824,6178	167,9634



Conclusiones

- Análisis energético, caso de estudio AES, de dos arquitecturas multicore: GPU y cluster de multicore.
- AES-GPU: Mejor rendimiento en tiempo de ejecución (CACIC 2011)
- AES-GPU: Mejor rendimiento en consumo.
- Alcanzar ese rendimiento con un cluster => mayor cantidad de procesadores => mayor consumo => costo energético alto.
- AES -GPU mejor relación FLOP/WATT.