UNIVERSITÀ DEGLI STUDI DI MILANO

Dipartimento di Informatica

CORSO DI LAUREA MAGISTRALE IN INFORMATICA

PROGETTO DI GPU COMPUTING

Parallelizzazione dell'algoritmo Advanced Encryption Standard (AES) su architettura CUDA

A cura di
Andrea Ceccarelli
Tommaso Celata

Docente
Giuliano Grossi

Anno Accademico 2015/2016

Indice

Capitolo 1

Introduzione

Il progetto da noi realizzato si pone l'obiettivo di verificare i vantaggi che l'architettura CUDA può portare nella parallelizzazione di algoritmi che presentano una sostanziosa parte seriale che può essere eseguita parallelamente. Per tale motivo si è scelto l'algoritmo Advanced Encryption Standard **(AES)** che cifra stati di dimensione fissa senza concatenare i risultati tra loro dandoci la possibilità di ottenere un buon livello di parallelizzazione.

In una prima fase si è implementato l'algoritmo in linguaggio c verificandone la corretta esecuzione tramite vettori di test trovati online, poi si è modificato il codice per adattarsi e sfruttare l'architettura **CUDA**. Una prima implementazione non è stata sufficiente per ottenere dei vantaggi rispetto alla versione c, questo dovuto al fatto che venivano lanciati **troppi kernel** che creando un collo di bottiglia rendevano inutile il vantaggio portato dalla parallelizzazione. Andando avanti con le varie versioni si è diminuito sostanzialmente il numero di kernel lanciati arrivando ad ottenere buoni risultati.

Spiegheremo quindi le caratteristiche delle varie versioni implementate concentrandoci sull'argomento **parallelizzazione** e su quali vantaggi (o svantaggi) si sono ottenuti da una versione all'altra.

Capitolo 2

Advanced Encryption Standard (AES)

Sviluppato dai due crittografi belgi Joan Daemen e Vincent Rijmen l'Advanced Encryption Standard (AES), conosciuto anche come Rijndael, di cui più propriamente è una specifica implementazione, è un algoritmo di cifratura a blocchi utilizzato come standard dal governo degli Stati Uniti d'America.

Data la sua sicurezza e le sue specifiche pubbliche si presume che in un prossimo futuro venga utilizzato in tutto il mondo come è successo al suo predecessore, il Data Encryption Standard (DES) che ha perso poi efficacia per vulnerabilità intrinseche. AES è stato adottato dalla National Institute of Standards and Technology (NIST) e dalla US FIPS PUB nel novembre del 2001 dopo 5 anni di studi, standardizzazioni e selezione finale tra i vari algoritmi proposti.

2.1 Descrizione dell'algoritmo

AES opera utilizzando matrici di 4x4 byte chiamate stati (states). Quando l'algoritmo ha blocchi di 128 bit in input, la matrice State ha 4 righe e 4 colonne; se il numero di blocchi in input diventa di 32 bit più lungo, viene aggiunta una colonna allo State, e così via fino a 256 bit. In pratica, si divide il numero di bit del blocco in input per 32 e il quoziente specifica il numero di colonne.

Capitolo 3

Architettura CUDA

Capitolo 4

Parallelizzazione AES in CUDA

Capitolo 5

Risultati

Capitolo 6

Considerazioni

Bibliografia

[1] Kenneth Price , Rainer M. Storn , Jouni A. Lampinen, *Differential Evolution: A Practical Approach to Global Optimization (Natural Computing Series)*. Springer-Verlag New York, Inc., Secaucus, NJ, 2005

[2] Janez Brest, Mirjam Sepesy Maucec, *Self-adaptive Differential Evolution Algorithm using Population size Reduction and Three Strategies*. Springer Novembre 2011, Volume 15, Issue 11, pp 2157-2174

[3] Ivan Gerace, Francesca Martinelli, Patrizia Pucci, *Tecniche di Regolarizzazione in Elaborazione di Immagini*. Giornate di Algebra Lineare e Applicazioni, 2009.

[4] Swatagam Das, Ponnuthurai Nagaratnam Suganthan, *Differential Evolution: A Survey of the State-of-the-Art*. IEEE Transactions on Evolutionary Computation, vol. 15, no. 1, pp. 4-31, 2011.

[5] P.C. Hansen, J.G. Nagy, D.P. O'Leary, *Deblurring Images. Matrices, Spectra and Filtering*. SIAM Publisher, Philadelphia, 2006