091-CIT

Implementation of AES Encryption on GPUs

Ibrahim B. Elsakka, Ahmed G. Ismael and Ahmed W. Elshazly
Department of Computer Engineering, Military Technical College, Cairo, Egypt
Email: {ibelsakka, agismael, awelshazly}@gmail.com
.
Supervisors: Assoc. Prof. Dr. Mohamed M. Fouad and Eng. Ahmed A. Abdelrahman
Department of Computer Engineering, Military Technical College, Cairo, Egypt
Email: {mmafoad, ahmedsoliman}@mtc.edu.eg

The importance of cryptography on ensuring security or integrity of the electronic data transaction had become higher during the past few years.Multiple security protocols are currently using various block ciphers. One of the most widely used block ciphers is the Advanced Encryption Standard (AES) which is chosen as a standard for its higher efficiency and stronger security than its competitors. Unfortunately, the encryption and decryption processes of AES takes a considerable amount of time for large data size. The GPU is an attractive platform for accelerating block ciphers and other cryptography algorithms due to its massively parallel processing power. In this paper, an implementation of the AES-128 ECB Encryption on Kepler GPU architectures has been presented. The results show that encryption speeds with 207 Gbps on the NVIDIA GTX 780 (kepler) have been achieved.