2016

GPU Assisted High Performance RSA Encryption

Zhe Zhao
Cleveland State University

Alec McGrady
Cleveland State University

GPU Assisted High Performance RSA Encryption

Washkewicz College of Engineering

Student Researchers: Zhe Zhao and Alec McGrady

Faculty Advisors: Haodong Wang and Janche Sang

Abstract

GPU has become highly popular due to its parallel computing ability. It accelerates operations in large scale. Many applications associate with intensive computations. RSA cryptosystem is one of them that can benefit from its utility. The purpose of this research is to implement RSA encryption and decryption by utilizing GPU to enhance the performance of the process. Since RSA public key and private key operations actually consist of large integer multiplications in a finite field, this research explores the efficient algorithms and implementations of the high performance GPU large integer multiplications.

Our work has been implemented on the following three different GPU platforms: (1) Ohio Super Computing's Ruby machine; (2) NVidia Quadro K620 graphic card on HP Z230 workstation; (3) NVidia Shield 8" Tablet. In particular, we develop and implement the row-wise and column-wise multiplication schemes that sufficiently take the advantage of GPU computing parallelism. Our experiments show that the GPU-assisted large integer multiplication accelerates the process by up to 200 times. The performance enhancement of RSA operations is also observed on the platforms of Ohio Super Computing Center and HP workstation. Due to the time constraint, we only test the 1024-bit RSA operations. In our future work, we expect to have much more performance enhancement on the RSA cryptosystem operations with larger key sizes.