# MASTER'S THESIS

## A multiple-precision integer arithmetic library for GPUs and its applications

Zhao, Kaiyong

*Date of Award:*
2011

# A Multiple-Precision Integer Arithmetic Library for GPUs and Its Applications

**ZHAO Kaiyong**

**A thesis submitted in partial fulfillment of the requirements**

**for the degree of**

**Master of Philosophy**

**Principal Supervisor: Dr. Xiaowen CHU**

**Hong Kong Baptist University**

**January 2011**

# Abstract

Public-key encryption plays a critical role in our daily life. The core component of a public-key system is a set of multiple-precision integer operations. A server that relies on public-key encryption (such as an SSL server) needs to process a large number of multiple-precision integer operations, which require huge computing power. Recent advances in Graphics Processing Units (GPUs) open a new era of GPU computing. We are motivated by the fact that GPUs could be utilized to speed up multiple-precision integer operations. This is of practical importance to end users as well as application servers. However, it is not easy to achieve high performance on GPUs due to the complicated memory architecture and the relatively slow integer operations. In this thesis, we present our design, implementation, and experimental results on a highly optimized multiple-precision integer library, GPUMP. Our library achieved a significant speedup for a number of multiple-precision integer operations.

To show the effectiveness of GPUMP, we developed a practical and secure random linear network coding system, which can be applied in peer-to-peer networks and wireless networks in order to enhance the system throughput and robustness. Network coding systems are prone to pollution attacks because a single polluted data packet from a malicious peer will be encoded with other genuine data packets and propagated to the whole network at an exponential rate. Homomorphic hash functions have been proposed to defend the pollution attacks, but there remain two challenges: (1) Homomorphic hash function requires network coding be performed in GF($q$) where $q$ is a very large prime number, which is computationally expensive due to the extensive large number operations; (2) Homomorphic hash function itself is computationally expensive for contemporary CPUs. By using the library of GPUMP, this thesis proposes to exploit the computing power of GPUs for network coding and homomorphic hashing, which leads to an integrated practical network coding solution for distributed systems.

# Table of Contents