Multiplication of Two Bignum Prime Numbers on a Nvidia Graphic Card

Johannes Häbe
jh-191149@hs-weingarten.de

Maximilian Nestle
mn-192181@hs-weingarten.de

Ravensburg-Weingarten University of Applied Sciences

March 26, 2020

Abstract

This paper is about testing the performance of the NVIDIA CUDA Fast Fourier Transform library (cuFFT) by multiplying bignum prime numbers on the graphic card. Several different tests are presented, evaluated and compared.

1 Introduction

The fast multiplication of two large prime numbers is necessary in some procedures to hack asymmetrical encryption algorithms like the RSA encryption. These computations are normally made on the CPU. Within this paper, General Purpose Computing On GPUs (GPGPU) is used to multiply bignum prime numbers with the help of the NVIDIA CUDA Fast Fourier Transform library (cuFFT). For this purpose, the computing time of bignum multiplication on CPU and GPU is compared and evaluated in this paper.

2 Hardware and Environment

For the multiplications we used .. as GPU and ... as CPU. The Linux distribution Ubuntu is used as the operating system. To compile the code we used ....