ÇANKAYA UNIVERSITY
FACULTY OF ENGINEERING
COMPUTER ENGINEERING DEPARTMENT

Test Plan, Test Design Specifications and Test Cases

Version 1

CENG 408

Innovative System Design and Development II

A CUDA Based AES-256-CTR File Encryption

Muhammed Bera ERKAYA
201511022
Emre YÜNCÜ
201511068
Fatih TAŞDEMİR
201511058
Doğa ÜÇÜNCÜ
201411063

Advisor: Dr. *Hüseyin TEMUÇİN*

Table of Contents

1. INTRODUCTION 2
1.1 Version Control 2
1.2 Overview 2
1.3 Scope 2
1.4 Terminology 2
2. FEATURES TO BE TESTED 2
2.1 AES – CTR Mode Encryption with CPU (CTR_CPU) 2
2.1 AES – CTR Mode Encryption with GPU (CTR_GPU) 2
3. REFERENCES 3
4. TEST DESIGN SPECIFICATIONS 3
4.1 AES – CTR Mode Encryption with CPU (CTR_CPU) 3
4.1.1 Subfeatures to be tested 3
4.1 AES_CTR Mode Encryption with GPU (CTR_GPU) 4
4.1.1 Subfeatures to be tested 4

1. INTRODUCTION

1.1 Version Control

Version No	Description of Changes	Date
1.0	First Version	May 29, 2020

1.2 Overview

In our project, we conducted a time-performance test with various file sizes. By applying encryption to these files, we tested their performance on CPU and GPU. We have determined which hardware is more effective in which file size.

1.3 Scope

This document includes the test plan of the use cases, test design specifications and the test cases correspond to test plan.

1.4 Terminology

Acronym	Definition
CTR_CPU	AES – CTR Mode Encryption with CPU
CTR_GPU	AES – CTR Mode Encryption with GPU

2. FEATURES TO BE TESTED

This section lists and gives a brief description of all the major features to be tested. For each major feature there will be a Test Design Specification added at the end of this document.

2.1 AES – CTR Mode Encryption with CPU (CTR_CPU)

In the first step of the test part of our project, we performed the encryption of files of different sizes on the CPU using Counter Mode (CTR) together with the AES-256 algorithm, which is one of the encryption methods.

2.1 AES – CTR Mode Encryption with GPU (CTR_GPU)

In the second step of the test part of our project, we performed the encryption of files of different sizes on the GPU using Counter Mode (CTR) together with the AES-256 algorithm, which is one of the encryption methods.

3. REFERENCES

[1] SRS, 27 December 2019
[2] SDD, 16 February 2020

4. TEST DESIGN SPECIFICATIONS

4.1 AES – CTR Mode Encryption with CPU (CTR_CPU)

4.1.1 Subfeatures to be tested

4.1.1.1 1-KB Text File in CPU (CTR_CPU.1_KB)

The encryption time of the 1-KB file is 0,58 miliseconds in the CPU.

4.1.1.2 2-KB Text File in CPU (CTR_CPU.2_KB)

The encryption time of the 2-KB file is 0,627 miliseconds in the CPU.

4.1.1.3 4-KB Text File in CPU (CTR_CPU.4_KB)

The encryption time of the 4-KB file is 1,885 miliseconds in the CPU.

4.1.1.4 8-KB Text File in CPU (CTR_CPU.8_KB)

The encryption time of the 8-KB file is 3,421 miliseconds in the CPU.

4.1.1.5 16-KB Text File in CPU (CTR_CPU.16_KB)

The encryption time of the 16-KB file is 5,010 miliseconds in the CPU.

4.1.1.6 32-KB Text File in CPU (CTR_CPU.32_KB)

The encryption time of the 32-KB file is 6,665 miliseconds in the CPU.

4.1.1.7 64-KB Text File in CPU (CTR_CPU.64_KB)

The encryption time of the 64-KB file is 14,96 miliseconds in the CPU.

4.1.1.8 128-KB Text File in CPU (CTR_CPU.128_KB)

The encryption time of the 128-KB file is 31,784 miliseconds in the CPU.

4.1.1.9 256-KB Text File in CPU (CTR_CPU.256_KB)

The encryption time of the 256-KB file is 78,113 miliseconds in the CPU.

4.1.1.10 512-KB Text File in CPU (CTR_CPU.512_KB)

The encryption time of the 512-KB file is 112,814 miliseconds in the CPU.

4.1.1.11 1-MB Text File in CPU (CTR_CPU.1_MB)

The encryption time of the 1-MB file is 229,696 miliseconds in the CPU.

4.1.1.12 2-MB Text File in CPU (CTR_CPU.2_MB)

The encryption time of the 2-MB file is 454,108 miliseconds in the CPU.

4.1.1.13 4-MB Text File in CPU (CTR_CPU.4_MB)

The encryption time of the 4-MB file is 885,344 miliseconds in the CPU.

4.1 AES_CTR Mode Encryption with GPU (CTR_GPU)

4.1.1 Subfeatures to be tested

4.1.1.1 1-KB Text File in GPU (CTR_GPU.1_KB)

The encryption time of the 1-KB file is 57,782 miliseconds in the GPU.

4.1.1.2 2-KB Text File in GPU (CTR_GPU.2_KB)

The encryption time of the 2-KB file is 61,198 miliseconds in the GPU.

4.1.1.3 4-KB Text File in GPU (CTR_GPU.4_KB)

The encryption time of the 4-KB file is 65,386 miliseconds in the GPU.

4.1.1.4 8-KB Text File in GPU (CTR_GPU.8_KB)

The encryption time of the 8-KB file is 73,013 miliseconds in the GPU.

4.1.1.5 16-KB Text File in GPU (CTR_GPU.16_KB)

The encryption time of the 16-KB file is 73,915 miliseconds in the GPU.

4.1.1.6 32-KB Text File in GPU (CTR_GPU.32_KB)

The encryption time of the 32-KB file is 75,20 miliseconds in the GPU

4.1.1.7 64-KB Text File in GPU(CTR_GPU.64_KB)

The encryption time of the 64-KB file is 76,002 miliseconds in the GPU

4.1.1.8 128-KB Text File in GPU (CTR_GPU.128_KB)

The encryption time of the 128-KB file is 79,03 miliseconds in the GPU

4.1.1.9 256-KB Text File in GPU (CTR_GPU.256_KB)

The encryption time of the 256-KB file is 80,80 miliseconds in the GPU

4.1.1.10 512-KB Text File in GPU (CTR_GPU.512_KB)

The encryption time of the 512-KB file is 81,53 miliseconds in the GPU

4.1.1.11 1-MB KB Text File in GPU (CTR_GPU.1_MB)

The encryption time of the 1-MB file is 83,113 miliseconds in the GPU.

4.1.1.12 2-MB Text File in GPU (CTR_GPU.2_MB)

The encryption time of the 2-MB file is 86,989 miliseconds in the GPU.

4.1.1.13 4-MB Text File in GPU (CTR_GPU.4_MB)

The encryption time of the 4-MB file is 88,07 miliseconds in the GPU.