

**ĐẠI HỌC THÁI NGUYÊN**  
**ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**ĐINH TIẾN NGỌC**

**NGHIÊN CỨU CÔNG NGHỆ XỬ LÝ GPU VÀ ỨNG DỤNG**

**THÁI NGUYÊN 2017**

## **LỜI CAM ĐOAN**

### **Tôi xin cam đoan :**

Những nghiên cứu dưới đây trong luận văn của tôi hoàn toàn trung thực không vi phạm bất kỳ quyền sở hữu trí tuệ nào. Nếu sai tôi xin chịu hoàn toàn trách nhiệm.

## **TÁC GIẢ LUẬN VĂN**

**Đinh Tiến Ngọc**

## LỜI CẢM ƠN

Lời đầu tiên tôi xin chân thành cảm ơn đến TS. Lê Quang Minh người thầy đã tận tình giúp đỡ, hướng dẫn tôi hoàn thành luận văn này.

Tôi cũng xin chân thành cảm ơn các thầy, cô giảng viên cao học người đã giúp đỡ tôi nâng cao kiến thức giúp tôi có những kiến thức bổ trợ giúp hoàn thiện cho luận văn này.

Tôi cũng xin chân thành cảm ơn người thân, bạn bè đã giúp đỡ và động viên tôi trong suốt thời gian học tập cũng như trong thời gian thực hiện đề tài.

Xin chân thành cảm ơn!

Thái Nguyên, ngày tháng 5 năm 2017

**TÁC GIẢ LUẬN VĂN**

**Đinh Tiến Ngọc**

## DANH MỤC THUẬT NGỮ

	Tiếng Anh	Tiếng Việt
	GPU	Bộ xử lý đồ họa
	gpgpu	Tính toán thông dụng trên GPU
	API	Application Program Interface : Định nghĩa một giao diện chuẩn để triệu gọi một tập các chức năng.
	coprocessor	bộ đồng xử lý
	kernel	hạt nhân
	texture	Kết cấu: cấu trúc của đối tượng, nó được xem như mô hình thu nhỏ của đối tượng.
	texturefetches	Hàm đọc kết cấu
	texturereference	Tham chiếu kết cấu
	warp	Mỗi khối được tách thành các nhóm SIMD của các luồng.
	SIMD	Single Instruction Multiple Data: đơn lệnh đa dữ liệu
	stream	Dòng
	streamingprocessor	Bộ xử lý dòng
	MIMD	Multiple Instruction Multiple Data: đa lệnh đa dữ liệu
	primariesurface	Bề mặt chính
	processor	Bộ xử lý
	Rasterization	Sự quét màn hình trên màn hình

## MỤC LỤC

LỜI CAM ĐOAN .....	i
LỜI CẢM ƠN.....	iii
DANH MỤC THUẬT NGỮ .....	iv
MỤC LỤC .....	v
DANH MỤC HÌNH VẼ .....	vii
LỜI MỞ ĐẦU .....	viii
CHƯƠNG I : KHÁI QUÁT VỀ BỘ XỬ LÝ ĐỒ HỌA GPU VÀ XỬ LÝ SONG SONG .....	1
1.1 Khái quát về xử lý song song.....	1
1.1.1 Khái quát về xử lý song song .....	1
1.1.2 Khái quát về Hệ thống máy tính song song.....	3
1.1.3 Khái quát về lập trình song song .....	7
1.1.4 Các nguyên tắc khi thiết kế giải thuật xử lý song song .....	9
1.2. Khái quát về công nghệ GPU và các ứng dụng .....	10
1.2.1. Tổng quan về GPU .....	11
1.2.2. Nguồn gốc và quá trình phát triển GPU .....	11
1.2.3. Cấu trúc của bộ xử lý đồ họa GPU .....	15
1.2.4. Lập trình trên GPU .....	19
1.2.5. Các hỗ trợ phần mềm cho xử lý tính toán trên GPU .....	22
1.2.6. Các kỹ thuật tính toán trên GPU.....	26
1.2.7.Các giải thuật ứng dụng trên GPU .....	29
CHƯƠNG II: XỬ LÝ SONG SONG TRÊN THIẾT BỊ ĐỒ HỌA GPU VỚI CUDA.	31
2.1. Khái quát về CUDA.....	31
2.2.Cơ chế lập trình và cách thức hoạt động của CUDA .....	33
2.2.1.Cơ chế lập trình.....	33
2.2.2.Cách thức hoạt động của CUDA .....	33
2.3. Tổng quan về lập trình với CUDA.....	38
2.3.1. Là ngôn ngữ lập trình mở rộng của ngôn ngữ lập trình C.....	38

2.3.2. Các phần mở rộng của CUDA.....	38
2.3.3. Biến Built-in trong CUDA.....	41
2.3.4. Biên dịch CUDA thông qua NVCC.....	42
2.3.5. Một số trường hợp cụ thể tính toán song song bằng CUDA .....	42
2.4. Các ứng dụng của CUDA trong các lĩnh vực .....	45
2.4.1. Ứng dụng của CUDA trong game .....	45
2.4.2. Ứng dụng của CUDA với video số.....	45
<b>CHƯƠNG III: SỬ DỤNG GPU ĐỂ LÀM TĂNG TỐC ĐỘ TÍNH TOÁN CHO BÀI</b>	
<b>TOÁN MÃ HÓA AES .....</b>	<b>48</b>
3.1 Giới thiệu về AES .....	48
3.2 Thuật toán mã hóa .....	48
3.2.1 Công đoạn mã hóa.....	50
3.2.2 Công đoạn giải mã .....	54
3.3 Chương trình thuật toán song song mã hóa AES sử dụng GPU.....	62
3.3.1. Giao diện chương trình demo .....	92
3.3.2. Kết quả chương trình và đánh giá hiệu suất tính toán.....	93
<b>KẾT LUẬN .....</b>	<b>88</b>
<b>TÀI LIỆU THAM KHẢO .....</b>	<b>89</b>

## DANH MỤC HÌNH VẼ

Hình 1 : Kiến trúc Von Neumann.....	1
Hình 2 : Máy tính song song có bộ nhớ chia sẻ.....	4
Hình 3 : Máy tính song song có bộ nhớ phân tán.....	5
Hình 4 : Kiến trúc máy SISD.....	5
Hình 5 : Kiến trúc máy SIMD .....	6
Hình 6 : Kiến trúc máy MISD .....	6
Hình 7 : Kiến trúc máy MIMD .....	7
Hình 8 : Mô hình lập trình truyền thông hai tác vụ của hai máy tính .....	8
Hình 9 : Mô hình lập trình song song dữ liệu.....	9
Hình10: Kiến trúc GPU của NVIDIA và AMD.....	19
Hình 11: Kiến trúc phần mềm CUDA .....	31
Hình 12: Thao tác cấp phát và thu hồi bộ nhớ .....	32
Hình 13: Vùng nhớ dùng chung mang dữ liệu gần ALU hơn .....	33
Hình 14: Sơ đồ hoạt động truyền dữ liệu giữa Host và Device.....	34
Hình 15: Khối luồng .....	36
Hình 16: Mô hình bộ nhớ trên GPU .....	37
Hình 17: Chiều của lưới và khối với chỉ số khối và luồng.....	42
Hình 18: Phương pháp đánh chỉ số luồng.....	45
Hình 19 : Mã hóa và giải mã .....	49
Hình 20: Biến đổi SubBytes() đối với mảng trạng thái .....	51
Hình 21: Mô tả Hàm ShiftRows() .....	51
Hình 22: Mô tả hàm MixColumns() .....	52
Hình 23: Mô tả hàm AddRoundKey() .....	53
Hình 24: Mô tả hàm InvShiftRow().....	55

## LỜI MỞ ĐẦU

Với sự phát triển như vũ bão của công nghệ, ngày nay công nghệ thông tin đã trở thành một phần không thể thiếu trong cuộc sống. Không những thế nó còn là một công cụ hữu hiệu trong các ngành khoa học, công nghệ cao,... đặc biệt là những ngành có nhu cầu tính toán lớn. Tuy nhiên trong khi với nhu cầu tính toán ngày càng tăng cao đó, ngành công nghệ thông tin lại gặp phải một vấn đề tối quan trọng đó là năng lực xử lý của CPU có hạn. Các nhà phát triển phần cứng đã thực hiện gia tăng mức độ xử lý cho CPU bằng cách gia tăng xung cho CPU. Tuy nhiên việc này cũng chạm ngưỡng bởi gặp phải vấn đề về tản nhiệt cho CPU do nhiệt độ CPU quá cao.

Một hướng mới đã được các nhà nghiên cứu đưa ra đó là phát triển bộ xử lý đa nhân với cơ chế xử lý song song.

Một bước phát triển trong hướng mới đó chính là bộ xử lý đồ họa – GPU (Graphics Processing Unit - bộ xử lý đồ họa). Khi mới ra đời, GPU chỉ được sử dụng với mục đích công việc phù hợp với khả năng là tăng tốc độ xử lý đồ họa, cũng như trong ngành trò chơi là chủ yếu. Nhưng với sự phát triển dần của các trò chơi và các phần mềm đồ họa, đã khiến GPU phát triển thêm và đến thế hệ GPUNV30 của NVIDIA ra đời người ta đã bắt đầu phát triển những công việc khác cho GPU như hỗ trợ tính toán dấu chấm động đơn, hỗ trợ tính toán lên cả ngàn lệnh. Và đặc biệt với tiềm năng như vậy có thể nghĩ tới việc sử dụng GPU ngoài đồ họa. Cùng với ý tưởng như vậy tôi đã liên tưởng đến việc áp dụng việc xử lý song song trên GPU thông qua ngôn ngữ lập trình CUDA. Xuất phát từ ý tưởng trên tôi đã chọn đề tài: NGHIÊN CỨU CÔNG NGHỆ XỬ LÝ GPU VÀ ỨNG DỤNG.

Luận văn gồm 3 chương chính:

**Chương 1: Khái quát về bộ xử lý đồ họa GPU và xử lý song song**, Chương này giới thiệu tổng quan về xử lý song song và bộ xử lý đồ họa GPU

**Chương 2: Xử lý song song trên thiết bị đồ họa GPU với CUDA**. Chương này nghiên cứu về ngôn ngữ lập trình CUDA và cách xử lý song song bằng CUDA trên GPU.

**Chương 3: Sử dụng GPU để làm tăng tốc độ tính toán cho bài toán mã hóa**



*AES*. Chương này tiến hành cài đặt thử chương trình song song, xử lý song song mã hóa AES trên GPU bằng ngôn ngữ CUDA và đưa ra kết quả cùng kết luận về hiệu suất của GPU.

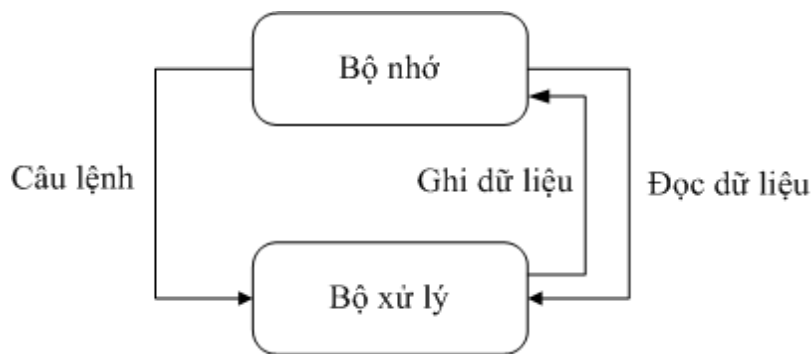
## CHƯƠNG I : KHÁI QUÁT VỀ BỘ XỬ LÝ ĐỒ HỌA GPU VÀ XỬ LÝ SONG SONG

### 1.1 Khái quát về xử lý song song

#### 1.1.1 Khái quát về xử lý song song

##### Nguồn gốc ra đời của xử lý song song

Một trong những nền tảng máy tính cơ bản đó là thiết kế máy tính của John Von Neumann. Đó là thiết kế mà ở đó một lệnh được thực hiện trên một bộ xử lý.



*Hình 1: Kiến trúc Von Neumann*

Khi cần tính toán với lượng câu lệnh và phép tính lớn thì thiết kế trên trở nên lỗi thời. Người ta đã đưa ra các phương pháp nhằm giải quyết vấn đề trên. Trong đó có việc tăng số lượng nhân xử lý hoặc kết nối nhiều máy tính thông qua mạng để tăng tốc độ xử lý.

Khi tăng tốc xử lý các phép tính trên máy tính song song, việc sử dụng các thuật toán tuần tự đã không còn thích hợp và không tận dụng hết khả năng tiềm tàng của máy tính song song. Dẫn đến việc ra đời các giải thuật song song.

##### Lý do phải xử lý song song

Như đã nói ở trên máy tính song song với bộ xử lý nhiều nhân đã thay thế dần máy tính đơn nhân, một bộ xử lý. Và với những thuật toán, câu lệnh, phép xử lý tuần tự đã không còn phù hợp với máy tính song song. Do vậy xử lý song song đã ra đời thay thế cho xử lý tuần tự nhằm đem lại hiệu năng tính toán cao hơn.

Bằng chứng đã thấy trong thực tế với nhiều bài toán xử lý với lượng dữ liệu lớn