AES on GPU

Dmitry Denisenko
Michael Kipper
Josh Slavkin
2009

Agenda

- What is AES?
- AES Description
- AES Modes
- AES on GPU
- Shared Constant Memory
- Data Access Patterns

2

Advanced Encryption Standard

- Encryption standard adopted by US government.
- Comprises 3 block ciphers: AES-128, AES-192 and AES-256
  - Block size: 128 bits
  - Key sizes: 128, 192 & 256 bits
- Announced on November 26, 2001
- Standard as of May 26, 2002
- The Rijndael cipher developed Joan Daemen and Vincent Rijmen

3

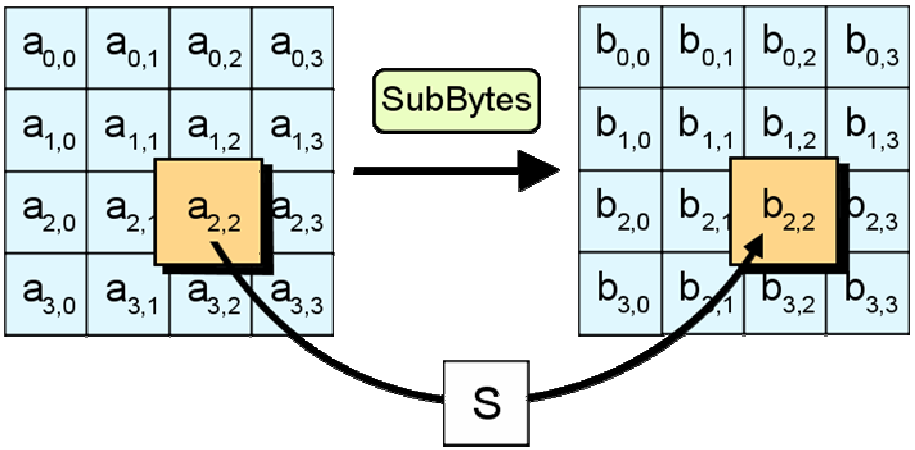
Algorithm

1. KeyExpansion
2. Initial Round
   - AddRoundKey

4

Algorithm (cont'd)

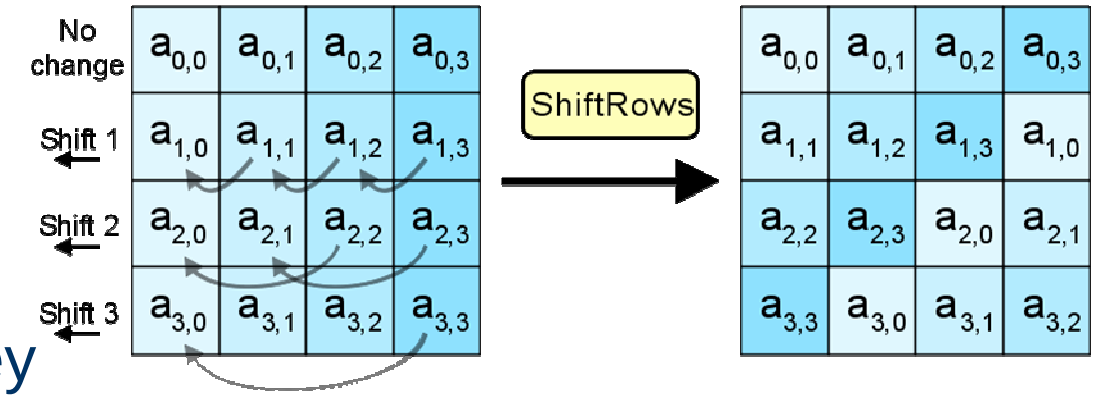
3. Rounds
   - **SubBytes**
   - ShiftRows
   - MixColumns
   - AddRoundKey



5

Algorithm (cont'd)

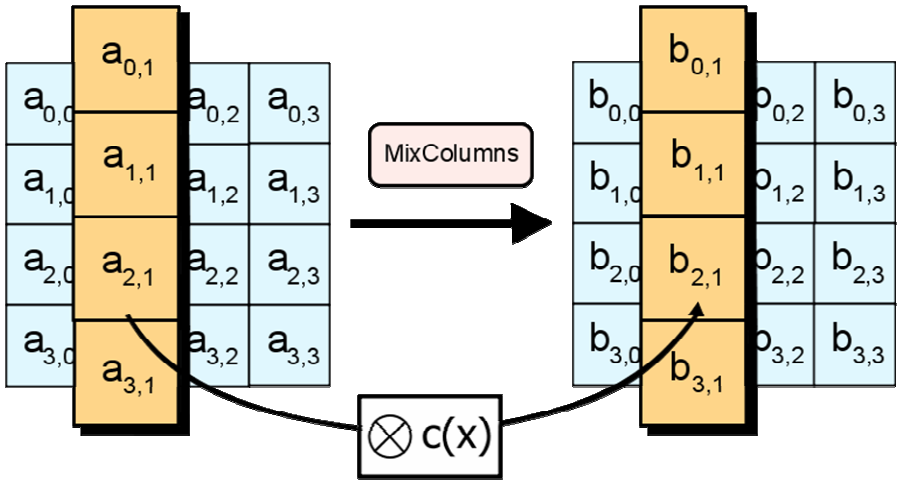
3. Rounds
   - SubBytes
   - **ShiftRows**
   - MixColumns
   - AddRoundKey



6

Algorithm (cont'd)

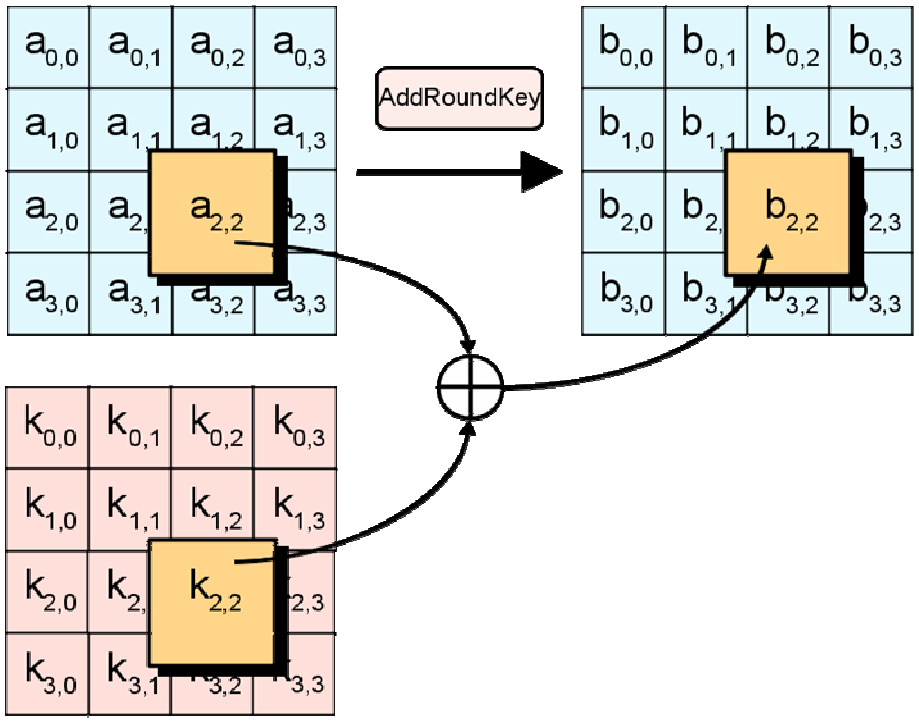
3. Rounds
   - SubBytes
   - ShiftRows
   - **MixColumns**
   - AddRoundKey



7

Algorithm (cont'd)

3. Rounds
   - SubBytes
   - ShiftRows
   - MixColumns
   - **AddRoundKey**



8

Algorithm (cont'd)

4. Final Round (no MixColumns)
   - SubBytes
   - ShiftRows
   - AddRoundKey

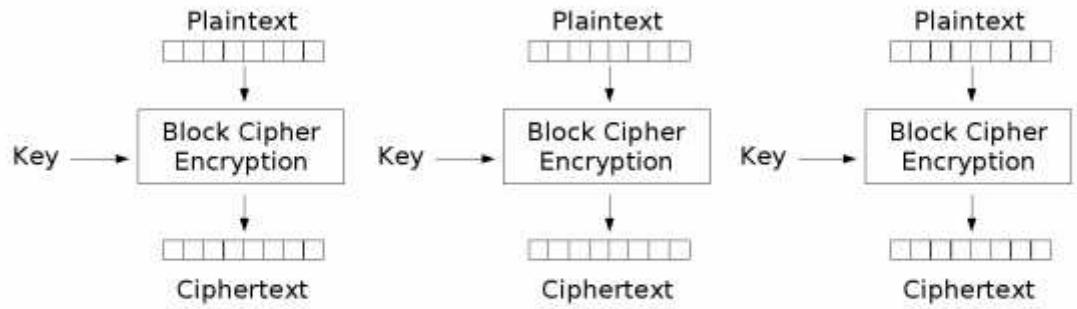
9

AES Modes

- AES is inherently block based
- Initialization vector of zero
- Several Modes Exist:
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Propogating Cipher Block Chaining (PCBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)

Modes

- Electronic Cookbook
  - Simplest mode, relatively insecure

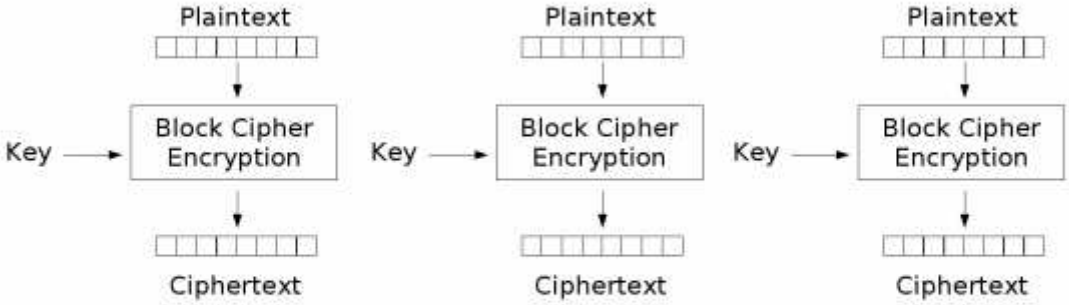


Electronic Codebook (ECB) mode encryption

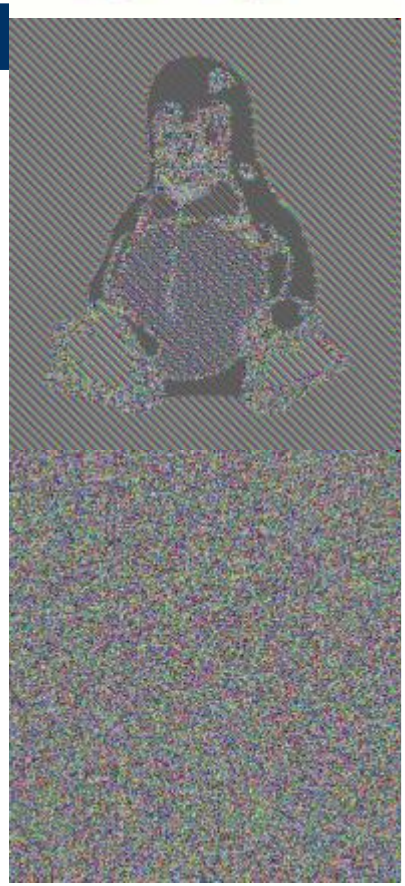
11

Modes

- Electronic Cookbook
  - Simplest mode, relatively insecure



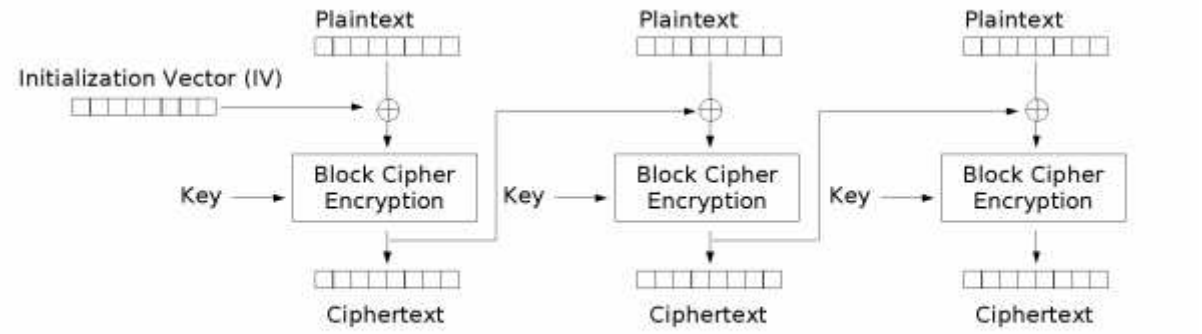
Electronic Codebook (ECB) mode encryption



12

Modes (cont'd)

- Cipher-block Chaining
  - Blocks XOR'd with previous ciphertext
  - More secure
  - Not suitable for mass parallelism

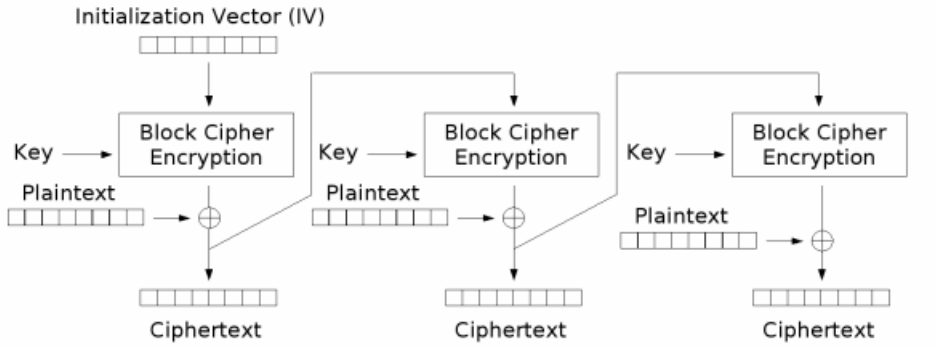


Cipher Block Chaining (CBC) mode encryption

13

Modes (cont'd)

- Propagating Cipher-block Chaining
- Cipher Feedback
- Output Feedback
  - Similar to Cipher-block Chaining
  - Uses different source for XOR/initialization vectors

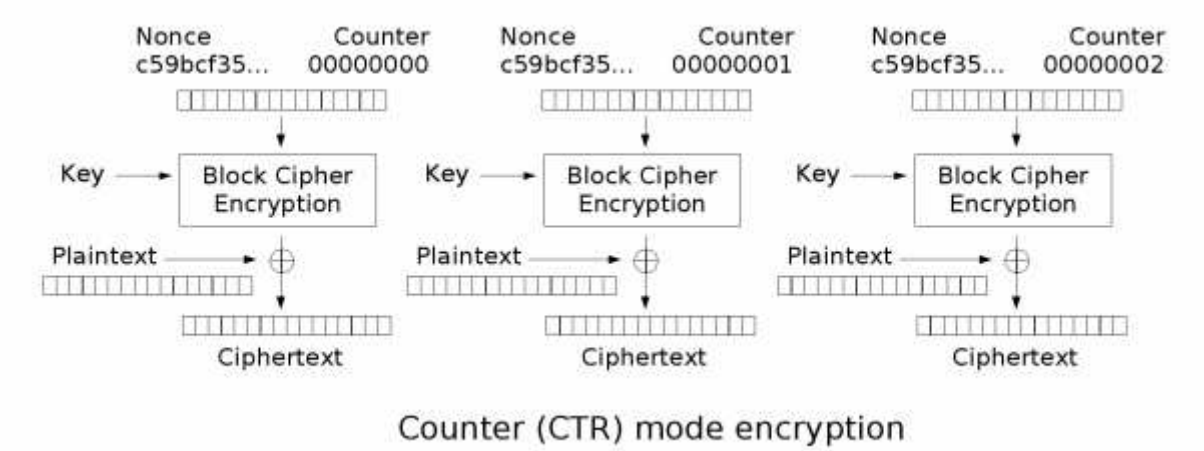


Cipher Feedback (CFB) mode encryption

14

Modes (cont'd)

- Counter
  - Modifies key with successive counter values
  - Most suitable to parallelism



Counter (CTR) mode encryption

15

AES on GPU

- Key Expansion on the CPU
  - Uses Rijndael's key schedule
  - Converts a 128-bit key to 704 bits
- Every function is implemented in both the CPU and GPU

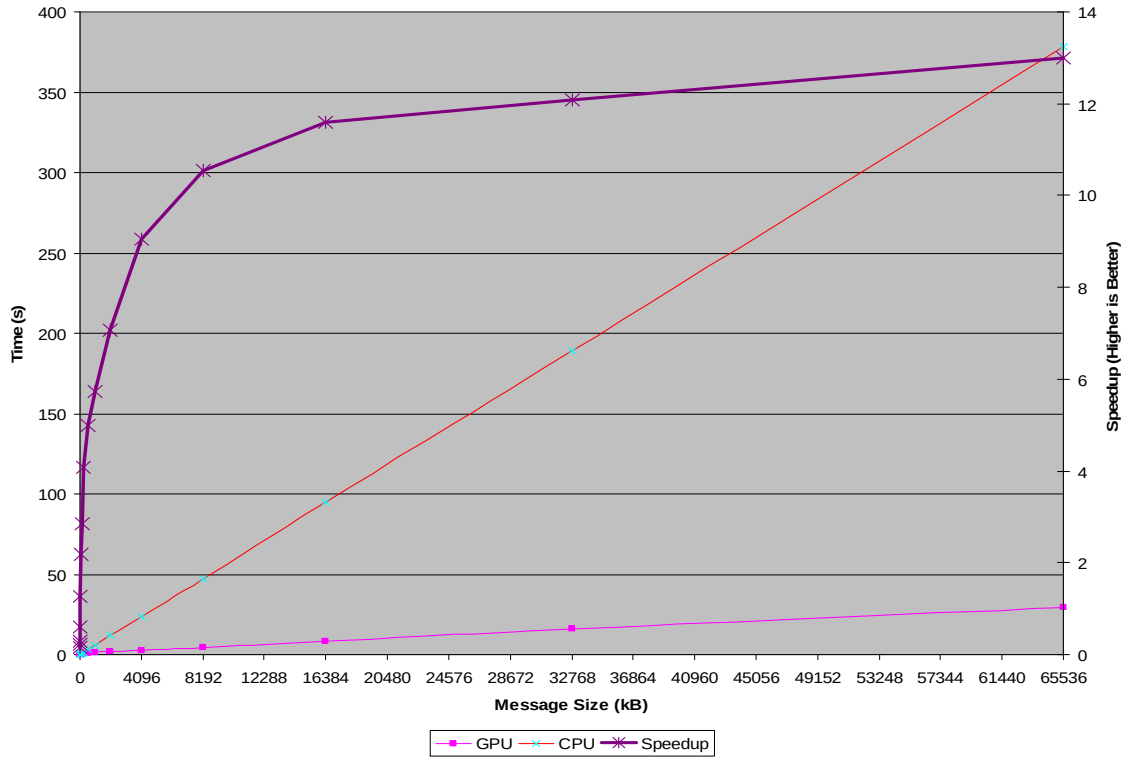
Memory Coalescing

- Each thread is simultaneously working on the same byte
- Concurrent access to data offset by some multiple of the message block size (16 bytes) is undesirable
- Solution: load message into memory for the entire block first
  - Amortize memory access latency over the entire block data space

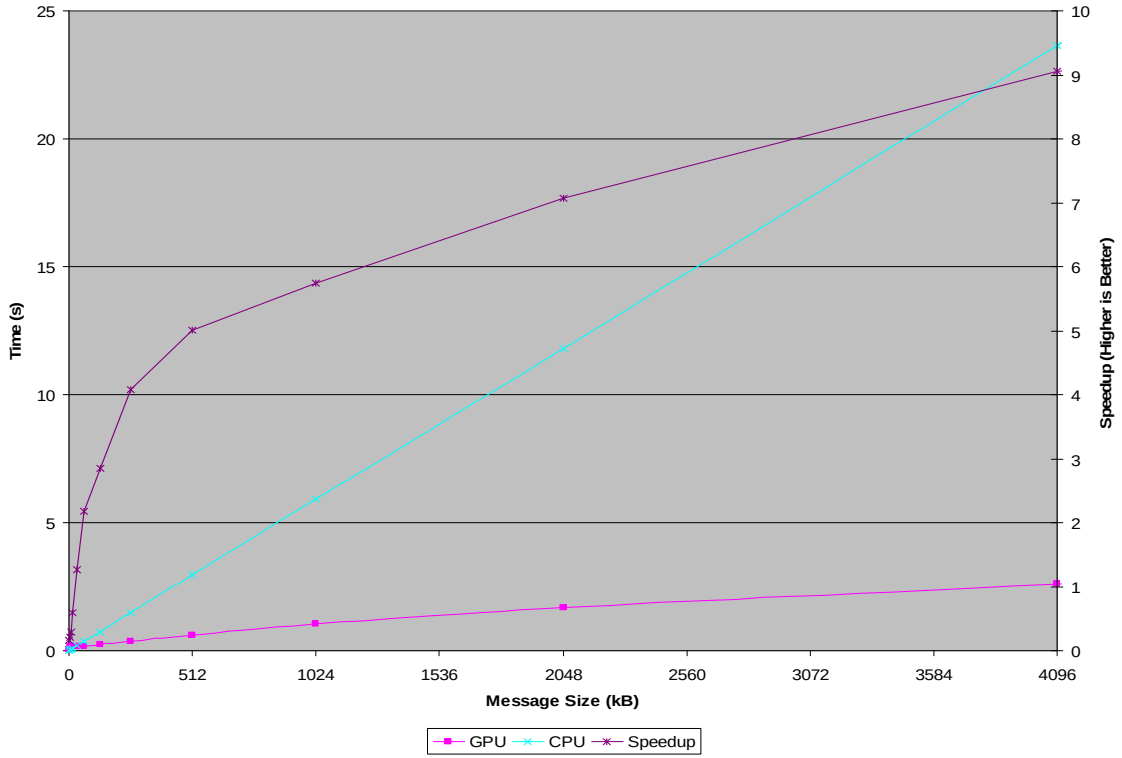
Shared Constant Memory

- AES uses lots of table lookups to save runtime computation
- There are several 16x16 tables in use:
  - SBox, InvSBox, XTimes2SBox, XTimes3SBox, XTime2, XTime9, XTimeB, XTimeD, XTimeE
  - 9x16x16 = 2,304 bytes
- GPU has 8kB of cache-backed constant memory
  - Use cudaMemcpyToSymbol()

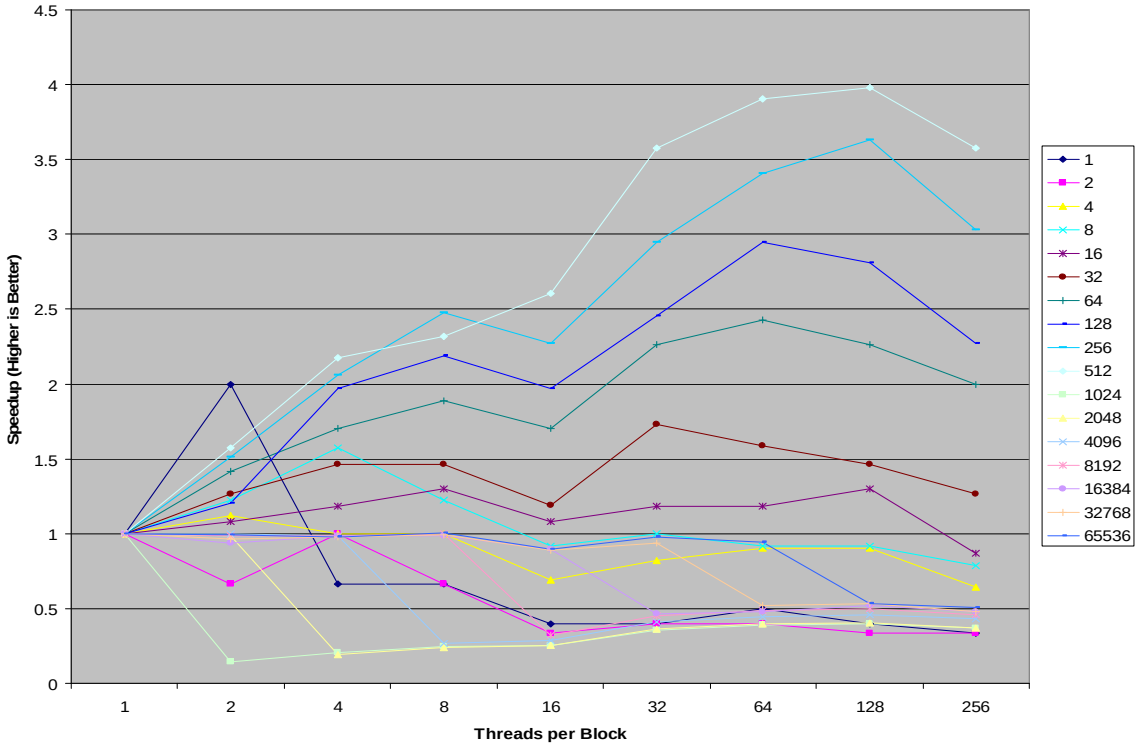
Speedup vs. File Size (256 Threads per Block)



Zoomed In


25
20
15
10
5
0
Time (s)
10
9
8
7
6
5
4
3
2
1
0
Speedup (Higher is Better)
0
512
1024
1536
2048
2560
3072
3584
4096
Message Size (kB)
GPU
CPU
Speedup

Speedup vs. Threads (File size in Kilobytes)



Discussion & Conclusion

- Optimal speedup is achieved at 128 threads per block
- 15x speedup over CPU implementation
- Shared constant memory is useful when random access patterns prevent efficient memory usage
- GPU is a viable co-processor for AES