卒業論文

題目

GPGPUによるAES-CTRモードの高速化

指導教員

大野 和彦

2018年

三重大学 工学部 情報工学科
計算機アーキテクチャ研究室

木村 亮太(410817)

内容梗概

近年, 個人情報をはじめとした様々なデジタルデータを暗号化してやりとりがされている. しかしデータ量が膨大になるにつれて暗号化には膨大な時間がかかるようになり, 高速化の需要が高まっている.

一方で, 画像処理用のユニットである GPU の性能が上がったことにより CPU よりも高い性能を出すようになり,GPU に汎用計算を行わせる GPGPU が注目されるようになった.

そこで本研究では GPGPU を用いた高速な AES 暗号化の実装を行った. CPU で実装したプログラムと GPGPU で実装したプログラムの二つにおいて暗号化の計算時間を計測した. その結果 GPGPU で実装したものが 11 倍高速であった.

Abstract

In recent years,the digital data such as personal information is encrypted and exchanged.However,as the amount of data becomes enormous,it takes time to encrypt.So,Demand for faste encryption is increasing. GPU improved than CPU.So, GPGPU which makes general purpose calculation perform to GPU has come to be noticed. In this study,I implemented high-speed AES code using GPGPU.

目 次

図 目 次

表 目 次

1　はじめに

1.1　研究目的

近年, インターネットやネットワークの普及に伴い個人情報をはじめ多くのデジタルデータが多くやりとりされている. しかし悪意ある第三者の手によりデータの改ざんや盗みが多発するようにもなり暗号化技術はいまやコンピュータセキュリティに欠かせない技術である. 他者にわからない, より安全な暗号を作るためには暗号化計算量を増やす必要があるが計算量を増やすと暗号化に非常に時間がかかる. よって暗号化技術において暗号強度だけではなく暗号化の高速化も求められるようになった. そこで本研究では GPGPU を用いた高速な AES 暗号化を実装した.

1.2　本文構成

本文の構成は以下のようになっている. 第 2 章で CUDA,AES 暗号について述べ, 第 3 章で実装方法の説明, 第 4 章で性能の評価を行い, 最後に第 5 章でまとめを行う.

2　背景

2.1　CUDA

GPU(Graphics processing unit) は本来画像処理用の演算装置である. 画像処理技術や GPU そのものの性能が上がったことにより GPU が汎用の CPU(Central Processing Unit) よりも処理速度が向上することとなった. そこで GPU を画像処理だけでなく汎用計算にも用いる GPGPU(General-Purpose computing on GPU) が注目されるようになった. 本研究では GPGPU を使用するための環境として NVIDIA 社の提供する CUDA(Compute Unified Device Architecture) を採用する

2.1.1　スレッド

CUDA では同時に多数のスレッドを実行することで並列化し、高速化している. スレッドをまとめたものをブロックといい, さらにブロックをまとめたものをグリッドと言う.

2.1.2　メモリ

fig.2.2 に示したとおりに CUDA では様々な種類のメモリが存在する. グローバルメモリは CPU から書き込みを行うことができ、大容量ではあるが速度は遅い. シェアードメモリは高速であるが容量が小さく、ブロック

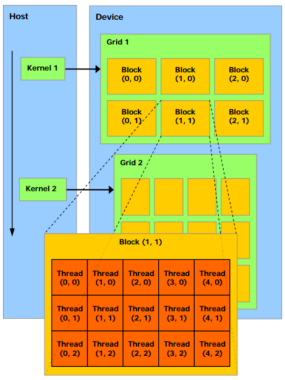

図 2.1: CUDA のアーキテクチャ [1]

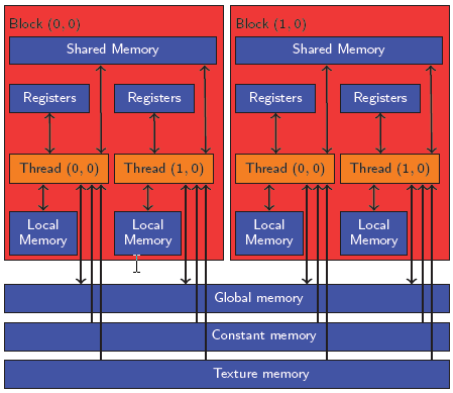

図 2.2: CUDA のメモリモデル [1]

外では使用できない特徴を持つ. ローカルメモリはスレッド内部でしかアクセスできないスレッドの作業領域であり、速度は遅い. コンスタントメモリとテキスチャメモリは速度は高速だが読み込み専用である.

このようにメモリの種類によって用途や容量, 速度が異なるためメモリの特徴に応じたプログラミングが非常に重要である.

2.2 AES 暗号

AES[2] は平文に対して 16byte ごとのブロックに区切り, それぞれ暗号化処理が行われる. 入力されたブロックに対して同じような処理を一定回数繰り返し適用するラウンド処理が行われる 2.3.AES は鍵長を 128bit,192bit,256bit の 3 種類から選択できる. 鍵長に応じてラウンド処理の回数が変わる. 本研究では鍵長を 128bit に設定した.128bit の鍵長で繰り返されるラウンド処理の回数は 10 回である.

ラウンド処理の内容はSubBytes,ShiftRows,MixColumns,AddRoundKey の 4 つの処理からなっている.SubBytes は Sbox と呼ばれるテーブルを参照した置換処理,ShiftRows は行に対してのシフト処理,MixColumns は列に対しての剰余演算処理,AddRoundKey は鍵との XOR 演算である. ラウンド処理終了後 SubBytes,ShiftRows,AddroundKey を行い暗号結果に

する.

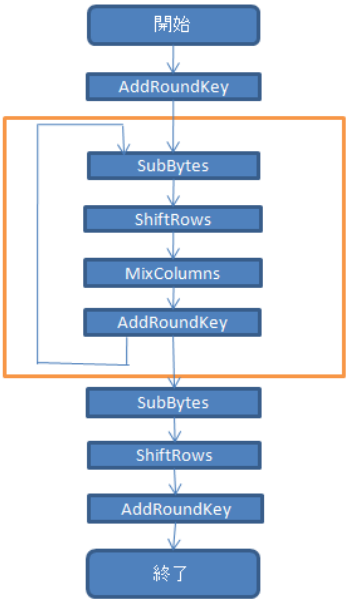

図 2.3: AES 暗号化手順

2.3 AES の問題点

先行研究 [3] では AES-ECB モード (fig.2.4) で実装している.ECB モードでは平文ブロックの暗号化処理において一つ前の暗号文ブロックなどは使わず平文ブロック単体で処理が完結するため並列化は用意である. しかし平文ブロックと暗号ブロックが 1 対 1 対応するため同じ平文からは同じ暗号文が出力される. この結果暗号文一致攻撃や暗号文改ざん攻撃といった攻撃に脆弱である.

そこで本研究では並列処理も行いつつ暗号化強度を強くする方法で実装・評価を行った.

2.4 AES-CTR

並列処理と暗号化強度の両立させる方法として AES-CTR モード (fig.2.5) が存在する.nonce(number used once) と呼ばれるカウンタを平文のかわりに暗号化する. 暗号化するたびにカウンタを 1 ずつ増加させる. そして暗号化したカウンタと平文の排他的論理和を出力することで暗号化する. これにより平文ブロックが複数存在していたとしてもカウンタ変数により平文ブロックと暗号ブロックは 1 対多の関係になることから暗号一致攻撃や暗号改ざん攻撃に対しても強くなっているといえる.

図 2.4: AES

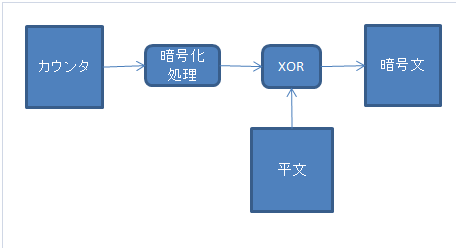

図 2.5: AES-CTR

3　実装方法

3.1　スレッド

各スレッドには 16byte の nonce の初期値を保持させた. その後スレッドに応じて nonce に定数を加算させそれぞれ暗号化を行わせることで並列化した. また各スレッドが nonce に対して独立して逐次処理を行うため, スレッド間のデータ処理がなくなりスレッド間同期が不要となった.

3.2 メモリ配置

演算をするごとにグローバルメモリにアクセスするとレイテンシが発生し処理速度が遅くなる. そこで先行研究では高速メモリであるシェアードメモリに平文を配置することで処理速度の向上を行っていた. しかしシェアードメモリの容量は少なく, また AES-CTR モードでは AES-ECB モードに比べ平文ブロックの計算量が少なく代わりに nonce カウンタブロックの計算量が多い. そのためシェアードメモリには平文ではなく nonce カウンタを配置した.

シェアードメモリの容量を確保するため平文,Sbox, 副鍵は別のメモリに配置することとした.Sbox, 副鍵で使用する数値はスレッド間で一定であり共通である. よって読み込み専用であるが高速なコンスタントメモリに配置することで処理の高速化を図った.

最後に平文は処理回数が少なく, スレッド間でデータのやりとりが存在しないためローカルメモリに配置した.

4　性能評価

4.1　実験結果

評価環境は Intel Xeon CPU E5-1620, メモリ 16GB,GeForce GTX 980 を搭載した計算機を使用した. ファイルサイズを変更しつつファイルを暗号化した実験結果を Table 4.1 および図 4.6 に示す．結果から GPU を用いたプログラムの方が実行時間が小さく,CPU と比べて最大 11 倍であった.

表 4.1: 実行時間 (秒) の比較

ファイルサイズ (KB)	1,000	4,000	15,000
CPU 版 aes	0.9	2.8	7.9
GPU 版 aes	0.2	0.4	0.7

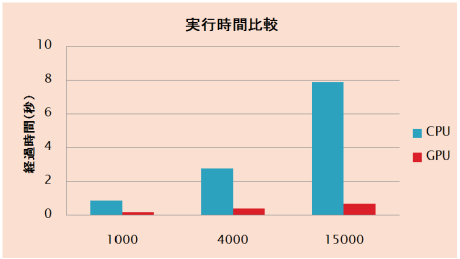

図 4.6: 各実装に対する実行時間の比較

5　おわりに

本研究では,GPU での AES 暗号の高速化および暗号強度の強化のために AES-CTR モードを実装し評価を行った．今後の課題として本研究で

行わなかったスケジューリングの最適化や実践した AES-CTR モードのだけでなくほかのモードにおいても GPGPU による高速化が期待できるか検討を行う必要がある.

謝辞

本研究を行うにあたり，ご指導，ご助言いただきました下さいました大野和彦講師に深く感謝いたします．また，様々な局面にてお世話になりましたコンピュータソフトウェア研究室の皆様にも心より感謝いたします.

参考文献

[1] nVIDIA,“NVIDIA CUDA Compute Unified Device Architecture ” 2008

[2] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback“Report on the Development of the Advanced Encryption Standard (AES)”

[3] Michael Kipper, Joshua Slavkin, Dmitry Denisenko University of Toronto “Implementing AES on GPU Final Report ”, April 20, 2009