3J-03

CUDAによるAES暗号化処理についての考察

菊池　丞太†　山口　実靖†
工学院大学工学部情報通信工学科†

1. はじめに

ビックデータ解析に期待が集まっているが，その活発な利活用には個人情報の保護などの利活用の壁[1]が存在し，高速なデータの暗号化などが重要な課題となっている．

データ処理を高速に行う手法の1つにGPUの活用がある．GPUでデータ処理を行う場合，データをホスト計算機の主記憶からGPUボードのVRAMに転送する必要があり，これに要する時間が機能低下の大きな要因となることがある．

本稿では様々なサイズのデータをオンデマンドでAES暗号化する処理に着目し，これをGPUを用いて高速化する手法について考察する．

2. AES

AES(Advanced Encryption Standard)は現時点で安全とされている共通鍵暗号の一つである．入力された平文に対し，128bit(16Byte)毎のブロックに区切って暗号化を行う．AESはラウンドと呼ばれる処理を複数回行って暗号化する．各ラウンドは SubBytes，ShiftRows，MixColumns，AddRoundKey と呼ばれる 4 つの変換処理から構成される．

3. CPUとGPUを併用するAES暗号化

3.1 基本性能評価

入力サイズを変更し，AES暗号処理にかかる時間をCPUとGPUでそれぞれ測定した．実験環境を表1に，AES処理時間を図1に，入力サイズ4000[Byte]以下の拡大図を図2に示す．

本研究において，AESはFIPS 197の論文[2]に基づき作成されたAES暗号化処理[3]を使用しており，鍵長は128bitを選択している．また，CUDAによるAES処理は1スレッドにつき4Byteの計算処理を行う[4]．鍵の生成はCPU側で行い，CPU，GPUともに鍵生成にかかる時間はデータに含んでいない．また，鍵とSboxの情報はconstant memoryに格納している．

表1 実験環境

CPU	Core i7-4770k
CPU memory	16GB
GPU	GTX760
GPU memory	4GB
OS	Windows7 64bit
Visual Studio	Microsoft Visual Studio 2012 Express for Windows Desktop
CUDA	CUDA5.5

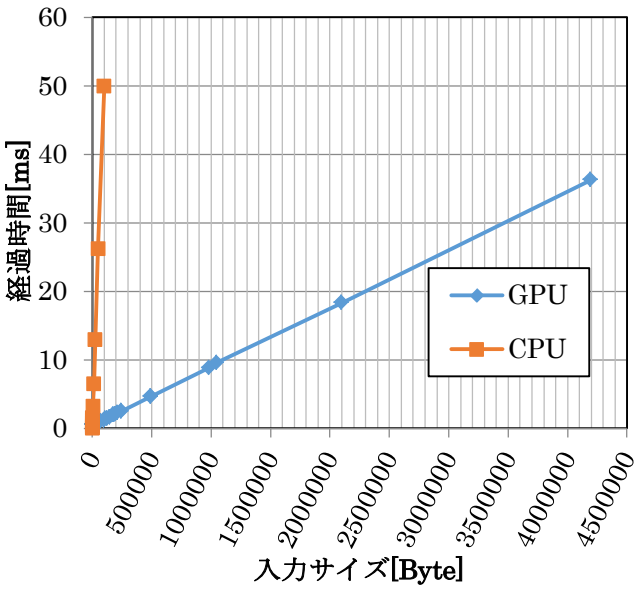

図1 暗号化処理時間

"Processing AES with GPU"
†Shota kikuchi, Saneyasu Yamagushi,
Information and Communication Technology, Kogakuin University

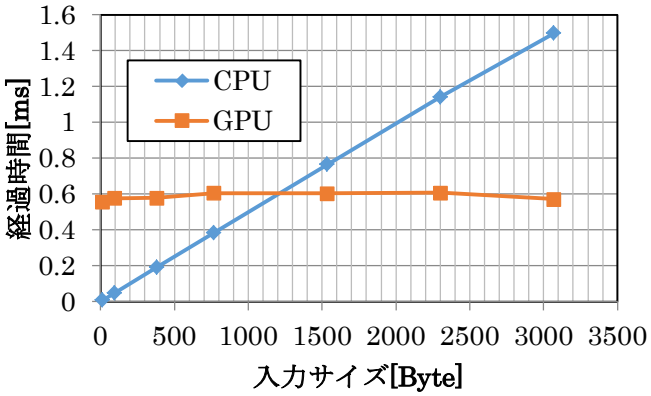

図２．少量データ時の暗号化処理時間

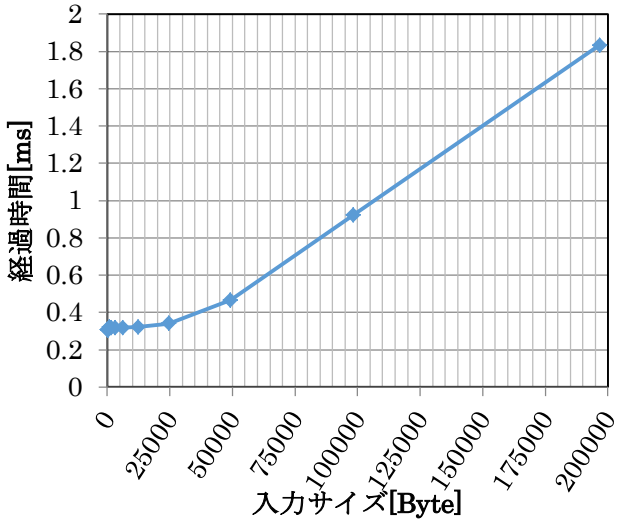

図 3 カーネル処理時間

図 1 から，データサイズが十分に大きい場合は GPU による処理の方が処理時間が短いことがわかる．また，図 2 より，データサイズが 1000[Byte] 以下では CPU により処理の方が処理時間が短いことがわかる．図 3 に GPU 処理におけるカーネル処理時間を示す．GPU ではデータサイズを小さくしても処理時間の短縮がほとんど生じていないが，図 3 よりデータサイズを大きくしても，入力サイズがあるサイズより大きくならないと AES 暗号化処理にかかる時間がほとんど増えていないことがわかる．この原因はデータサイズが小さい場合には GPU の計算処理にかかる時間に比べデータの転送に要する時間が大きく，データ転送時間を隠蔽することができないためであると考えられる．

3.2 提案

図 2 の CPU と GPU の処理時間が逆転している点に着目し，1280Byte を境に使用するハードウェアを切り替えることを提案する．

評価実験として，暗号化用平文データが複数ある場合を想定し，待ち行列を 50 個作成しておき，順序に処理を行う実験を行った．このときの暗号化用平文データのサイズは 16～2048Byte で 50 個の平均は 1057.5Byte である．

その結果を図 4 に示す．図より提案手法は CPU のみと GPU のみと比べ短い時間で AES 暗号化を処理することができることがわかる．

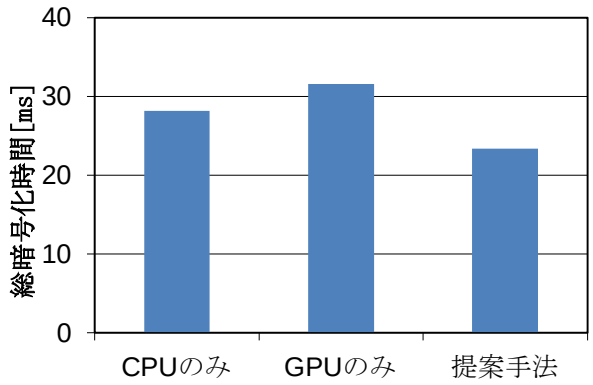

図 4．提案手法評価実験

4. おわりに

本稿では，ハードウェアごとに適したデータサイズが異なることに注目し，それを考慮して平文の長さによる効率的な AES 暗号化処理手法の提案を行った．評価より，平文の長さに応じて CPU と GPU を使い分けることが高速化につながることが分かった．

今後は，CPU と GPU のスケジューリングについて考察していく予定である．

謝辞

本研究は JSPS 科研費 24300034, 25280022, 26730040 の助成を受けたものである．

参考文献

[1]“パーソナルデータの利活用に関する制度改正の基本的な考え方について”, https://www.kantei.go.jp/jp/singi/it2/pd/dai10/siryou4-1.pdf
[2] FIPS 197 Announcing the ADVANCED ENCRYPTION STANDARD(AES) http://csrc.nist.gov/publications/fips/fips197/fops-197.pdf
[3] 共通鍵暗号方式を用いた AES 暗号 http://free.pjc.co.jp/AES/index.html
[4] 西川 尚紀,岩井 啓輔,黒川 恭一 “CUDA による AES 実装のための計算粒度最適化手法” 電子情報通信学会技術研究報告.RECONF 109(385), 107-112, 2010-01-19