中国科学院研究生院学报 2011, 28(6) 776-785 DOI: ISSN: CN:

论文

基于GPGPU和CUDA的高速AES算法的实现和优化

顾青[1], **高能**[2], **包珍珍**[3], **向继**[2]

1. 国家863计划信息安全基础设施研究中心, 上海 200336;
2. 中国科学院研究生院信息安全国家重点实验室, 北京 100049;
3. 中国科学技术大学, 合肥 230026

摘要:

随着高性能计算需求的不断增长,人们开始将目光投向具有强大计算能力及高存储带宽的GPU设备.与擅长处理复杂性逻辑事务的CPU相比,GPGPU(general purpose graphic processing unit,通用图形处理器)更适合于大规模数据并行处理.CUDA(compute unified device architecture,统一计算架构)的出现更加速了GPGPU应用面的扩张.基于GPGPU和CUDA技术对AES算法的实现进行加速,得到整体吞吐量6~7Gbit/s的速度.如果不考虑数据加载时间,对于1MB以上的输入规模,吞吐量可以达到20Gbit/s.

关键词: 通用图像处理器 统一计算架构 AES算法 并行计算

Implementation and optimization of high speed AES algorithm based on GPGPU and CUDA

GU Qing[1], GAO Neng[2], BAO Zhen-Zhen[3], XIANG Ji[2]

1. National 863 Program Research Center for Information Security Infrastructure, Shanghai 200336, China;
2. State Key Laboratory of Information Security, Graduate University, Chinese Academy of Sciences, Beijing 100049, China;
3. University of Science and Technology of China, Hefei 230026, China

Abstract:

Compared with the CPU which is good at handling logic complexity service, GPGPU (general purpose graphic processing unit) is suitable for large-scale parallel processing computing. The emergence of CUDA (compute unified device architecture) accelerates the expansion of application of GPGPU. We accelerate the implementation of AES algorithm based on GPGPU and CUDA and achieve a total throughput of 6~7Gbit/s. Regardless of the time of data loading and storing, a throughput of 20Gbit/s towards an input size over 1MB can be achieved.

Keywords: GPGPU(general purpose graphic processing unit) CUDA(compute unified device architecture) AES algorithm parallel computing

收稿日期 2010-07-23 **修回日期** 2010-11-01 **网络版发布日期**

DOI:

基金项目:

中国科学院知识创新工程(YYYJ-1013)和国家科技支撑课题(2008BAH32B04)资助

通讯作者:

作者简介:

作者Email: gaoneng@lois.cn

参考文献:

[1] Kedem G,Ishihara Y. Brute force attack on UNIX passwords with SIMD computer //Proceedings of the 8th USENIX Security Symposium.1999.

[2] Olano M, Lastra A. A shading language on graphics hardware: the PixelFlow shading system [J]. Journal of Computer Graphics,1998:159-168.

[3] Cook D L, Keroymytis A D. Cryptographics: exploiting graphics cards for security //Advancements in Information Security Series. Springer, 2006.

[4] Cook D L, Ioannidis J, Keromytis A D, et al. CryptoGraphics: secret key cryptography using graphics cards //RSA Conference, Cryptographer's Track (CT-RSA). 2005.

[5] Cook D L, Baratto R, Keromytis A. Remotely keyed cryptographics secure remote display access using (mostly) untrusted hardware //ICICS05 Conference Proceedings. December 2005.

[6] Manavski S A. CUDA compatible GPU as an efficient hardware accelerator for AES cryptography //2007 IEEE International Conference on Signal Processing and Communications (ICSPC 2007). Dubai, United Arab Emirates,November 2007.

[7] Harrison O, Waldron J. AES encryption implementation and analysis on commodity graphics processing units //Ches 2007. LNCS,2007,4727:209-226.

[8] Fiorese C, Budak C. AES on GPU: a CUDA implementation //Proc of CHES. 2007.

[9] Yamanouchi T. GPU Gems 3 . chapter 36: AES encryption and decryption on the GPU . SEGA Corporation. http://http.developer.nvidia.com/GPUGems3/gpugems3_ch36.html.

[10] Biagio A D, Barenghi A, Agosta G, et al. Design of a parallel aes for graphics hardware using the cuda framework //IEEE International Symposium on Parallel& Distributed Processing. May 2009.

[11] Joppe W Bos1, Dag Arne Osvik, Deian Stefan. Fast implementations of AES on various platforms //EPFL IC IIF LACAL, Station 14, CH-1015 Lausanne, Switzerland Fjoppe Bos, Dept of Electrical Engineering. The Cooper Union, NY 10003, New York, USA,2009.

本刊中的类似文章

1. 王润泽 王颖 杨栋毅.大规模FFT并行计算中2维SRAM的设计[J]. 中国科学院研究生院学报, 2008,25(1): 123-128