**Bitsliced implementation of the AES algorithm on GPU**

Jardim Verdolin Dabreu Bruna\(^1\), Francesco Regazzoni\(^1\), Antonino Tumeo\(^2\)

\(^1\)ALaRI - University of Lugano, Lugano, Switzerland
bruna.jardim.verdolin.dabreu@usi.ch, regazzoni@alari.ch

\(^2\)Pacific Northwest National Laboratory, Richland, Washington, USA
antonino.tumeo@pnl.gov

Throughout the years, countless hardware-based and software-level optimizations have been done to improve the performance of cryptographic algorithms. In this poster, we discuss the state of the art of high throughput implementations of the Advanced Encryption Standard (AES), focusing on solutions targeting Graphic Processor Units (GPUs). We also propose, as an original contribution, a novel CUDA implementation of AES for GPUs, based on the bitslicing software technique.

GPUs can obtain speedups of orders of magnitude for several general purpose computations with respect to common processors, due to their massive parallelism. For this reason, they have become an interesting target platform for cryptography applications. However, to obtain significant benefits, designers must carefully map the applications to the GPU, often adapting the algorithms to fit their architectural constraints. To better exploit the potentials of such architectures, we explored the possibility to further increase the level of parallelism of the AES by relying on software optimizations previously used only in embedded general purpose processors.

We restructured the algorithm so to increase its parallelism, allowing the GPU to hide memory latencies through massive multithreading. We improved the resource utilization by optimizing the number of active threads per GPU’s multiprocessor, the register management, the partitioning between on-chip and off-chip memory, and the global memory bandwidth. We introduced streaming support to optimize the communication bandwidth among the GPU and the host.

Our experimental results show that the proposed implementation can achieve a speed of 9.8 Gbps with a 2GB input message, which nicely compares with the state-of-the-art fast implementations of the AES.
Abstract

Throughout the years, countless hardware-based and software-level optimizations have been done to improve the performance of cryptographic algorithms. In this poster, we explore the suitability for Graphic Processor Units (GPUs) of optimizations based on the bitslicing software technique. In particular, we explore a novel CUDA implementation of the Advanced Encryption Standard (AES) based on bitslicing, we analyse its performances using different configuration parameters, and we compare them with the state of the art of high throughput implementations of AES.

Graphic Processing Units

Architecture

Texture Processor Clusters

Execution time in devices with different number of SMs

Bitsliced implementation of the AES Algorithm

The algorithm

Configurations of registers

AES execution with one kernel

Bitsliced implementation of the AES algorithm on CUDA

Performances in GeForce

Performances in Tesla

Comparison

<table>
<thead>
<tr>
<th>NVIDIA Card</th>
<th>Max. Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our</td>
<td>9.8 Gbps</td>
</tr>
<tr>
<td>Di Biagio et al. [3]</td>
<td>12.5 Gbps</td>
</tr>
<tr>
<td>Agosta et al. [1]</td>
<td>12 Gbps</td>
</tr>
</tbody>
</table>

References

