Exploring Side Channel Attacks and Counter-Measures for GPGPUs

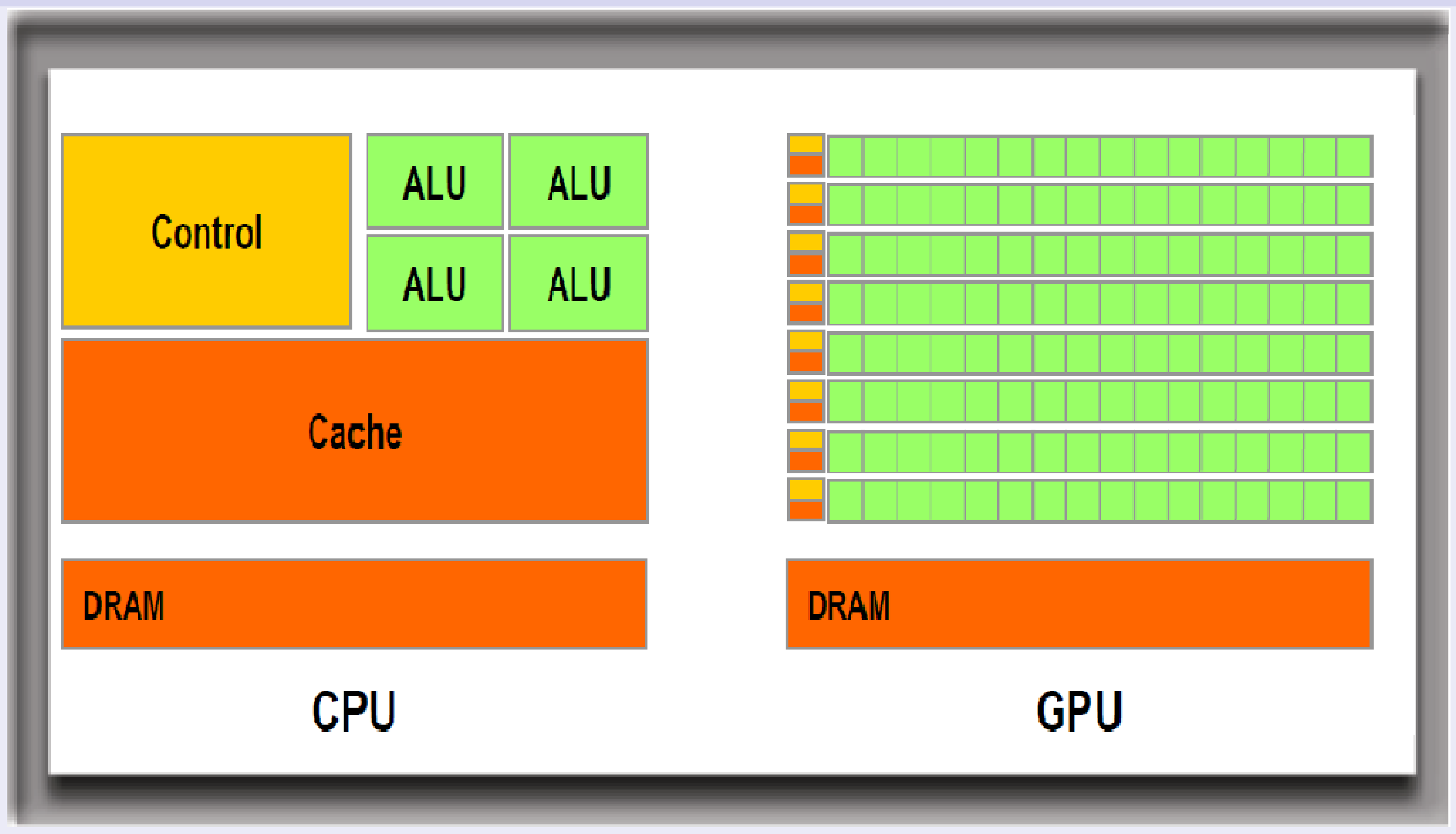
Student: Jose Vanterpool, Supervisor: Dr. Daniel Page, Project Type: research

University of Bristol, Department of Computer Science

Motivation

Due to recent advances in memory capacity and computational models, Graphics Processing Units (GPUs) are now able to facilitate a wider range of general purposes than originally designed for such as encryption and decryption. The security of CPUs for cryptographic purposes, the side channels they exhibit and the vulnerabilities that result, as well the measures which can be taken to mitigate these vulnerabilities are areas which have been researched extensively. However, the same cannot be said about GPUs which are currently being used for the same purposes. With the vast differences between CPU and GPU architectures, we may be vulnerable to new side-channel attacks or rendering past countermeasures to known attacks useless by switching to GPUs as the target platform. At the time of writing, there are several research papers which demonstrated the ability of GPUs to accelerate cryptographic algorithms such as AES, but only three papers investigated side channels on the platform. Two papers found that the shared memory access time was directly proportional to the number of bank conflicts which took place [1] [2]. The third showed that the execution time of a kernel is linearly proportional to the number of unique cache line requests generated. All 3 papers were able to use these finding as timing channels to successfully recover the secret key [3]. While these papers prove the existence of a timing channels, none of them explore any countermeasures to mitigate such an attack. In addition to this, they all target CUDA implementations which are only applicable to a subset of GPUs present in the market (produced by NVIDIA).

CPU vs GPU Architecture



src: https://commons.wikimedia.org/wiki/File:Cpu-gpu.svg

Project Objectives

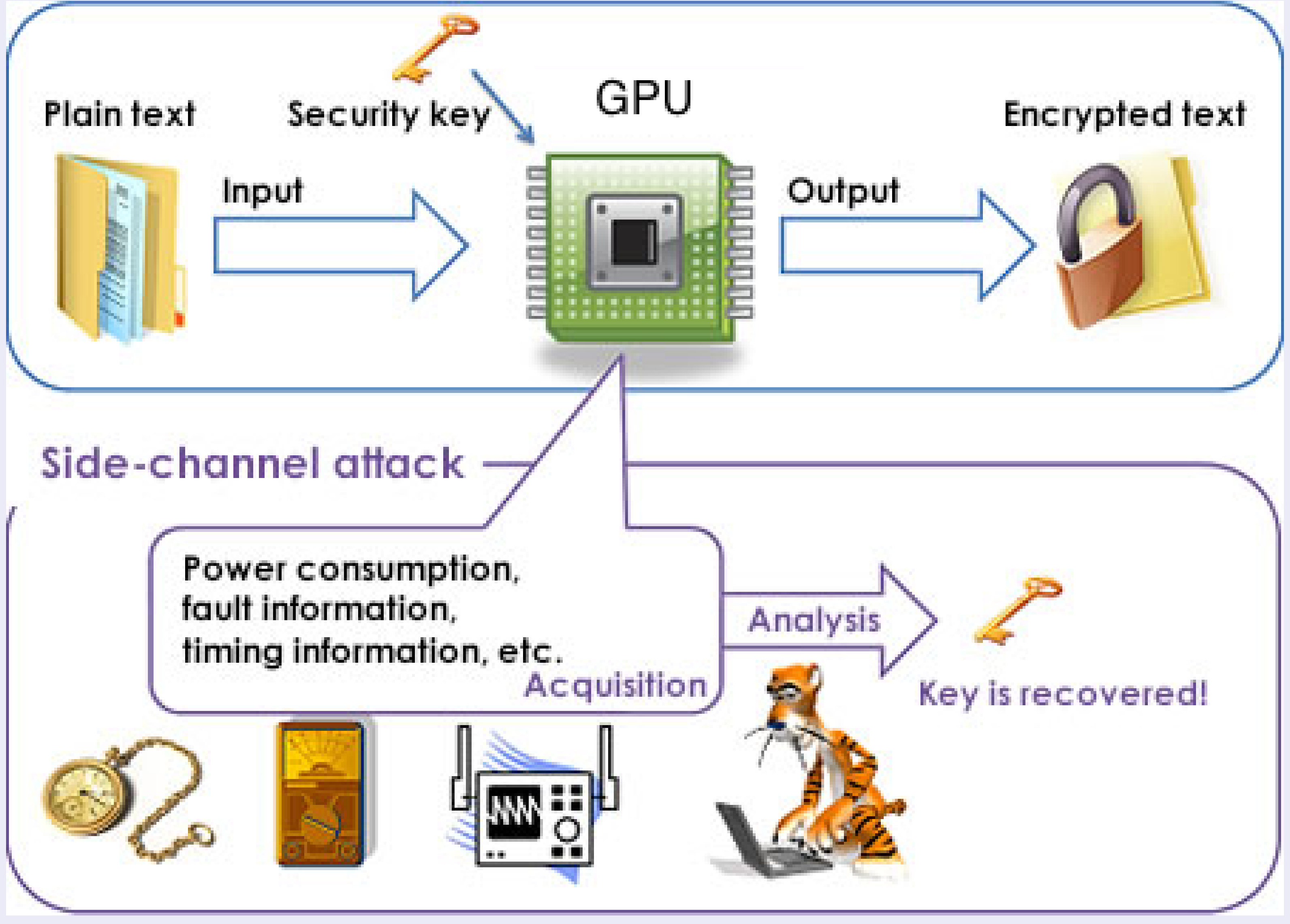
OpenCL is a cross platform framework used for writing parallel programs. By taking advantage of this framework as opposed to CUDA, we should be able to conduct investigations on a wider range of GPUs and determine if these channels exist within other architectures.

This project has the following objectives:

1. reproduce existing attacks focused on CUDA implementations using OpenCL
2. determine if OpenCL implementations are indeed susceptible to the attacks shown against CUDA
3. If 2. is found to be true, investigate countermeasures to the attacks on OpenCL platforms, else investigate why.
   In the event that all of these objectives are fulfilled with time to spare:
4. Investigate countermeasures to the CUDA implementations.

What are Side Channels?

Side Channels (accidentally) leak information through the physical implementation of cryptographic algorithms.



src: www.togawa.cs.waseda.ac.jp/English/research/app.html

Project Status

The researching phase of the project has been completed. Obejective 1, reproducing the known GPU attacks displayed against CUDA using the OpenCL platform, is currently undergoing. There are no preliminary results at the moment.

Open Questions

The open questions which exist at the moment include:

1. Are non-CUDA compatible GPU architectures vulnerable to the known attacks.
2. What are the similarities/differences between the different GPU architectures that make some/all of them susceptible to such attacks.
3. What countermeasures can be applied to mitigate these attacks and how effective are they?
4. Are the countermeasures generalisable or platform specific?

References

[1] Fomin, D.B. A timing attack on CUDA implementations of an AES-type block cipher

[2] Z. H.; Fei, Y.; Kaeli, D. A Novel Side-Channel Timing Attack on GPUs

[3] Z. H.; Fei, Y.; Kaeli, D. A Complete Key Recovery Timing Attack on a GPU

[4] Lim, R. K.; Petzold, L. R.; Koc, C. K. Bitsliced High-Performance AES-ECB on GPUs

[5] Kocher, P. Timing Attacks on Implementations of Dife-Hellman, RSA, DSS and Other Sys- tems, in the Proceedings of Crypto 1996, LNCS, vol 1109, pp 104113, Santa Barbara, CA, USA, August 1996.

[6] Kocher, P.; Jaffe, J; Jun, B. Differential Power Analysis, in the Proceedings of Crypto 1999, LNCS, vol 1666, pp 398412, Santa-Barbara, CA, USA, August 1999.

[7] Agrawal, D.; Archambeault, B.; Rao, J; Rohatgi, P. The EM Side-Channel(s), in the Proceedings of CHES 2002, LNCS, vol 2523, pp 2945, Redwood City, CA, USA, August 2002.