Masaryk University
Faculty of Informatics

GPU-based speedup of EACirc project

Bachelor Thesis

Jiří Novotný

Brno, Spring 2015

Declaration

Hereby I declare, that this paper is my original authorial work, which I have worked out by my own. All sources, references and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Jiří Novotný

Advisor: RNDr. Petr Švenda, Ph.D.

Acknowledgement

I thank CRoCS laboratory for provision of workspace and hardware resources to make this thesis happen. I would like to thank Petr Švenda for leading my work and Martin Ukrop for endurance to answering my numerous question about EACirc insides.

Last but not least I would like to thank my family for continuous support and for a help with a language side of my bachelor thesis.

Abstract

TODO

Keywords

acceleration, CUDA, CMake, GPU, GPGPU, EACirc, software circuit, randomness testing

Contents

1 **Introduction** 1
2 **CUDA** 3
2.1 *Hardware architecture* 5
2.2 *Thread hierarchy* 5
2.3 *Memory hierarchy* 7
2.4 *Heterogeneous programming* 8
2.5 *Compute capabilities* 9
2.6 *Programming language* 9
2.7 *Tools* 9
3 **CMake** 11
3.1 *CMake toolset* 11
3.2 *A closer look at the* `cmake` *executable* 12
3.3 *Changes made to the EACirc repository structure* 13
3.4 *The new build-system of EACirc* 14
3.5 *Project settings for CUDA* 15
4 **Gate Circuit of EACirc** 16
4.1 *Software representation of hardware circuit* 17
4.2 *CPU implementation* 18
4.2.1 Connector layers 18
4.2.2 Function layers 18
4.2.3 Circuit interpreter 18
4.3 *GPU implementation* 19
5 **Conclusions and future work** 20
Bibliography 21

1 Introduction

Random data and the concept of randomness are used in many branches of informatics. However, one of the fundamental ways how to use these principles is in cryptography and IT security. For instance, let there be a communication among several entities. The main content of the communication is meant to stay hidden from other entities, thus the communication needs to be encrypted by a chosen encryption protocol. The potential attacker[1] could intercept some encrypted messages and subject them to analysis. On the basis of certain traits of the protocol or similarities among the individual messages the encryption could be broken and the hidden content of the communication could be read by the attacker. Therefore, the goal of encryption protocols is that the encrypted messages are not similar or do not have some characteristic traits. In other words, the encrypted messages must look like random data to the attacker. However, this is very difficult to be ensured.

That is why tools have been created to test randomness, and thus quality, of ciphers. One of these tools is called EACirc and is being developed at the Faculty of Informatics of Masaryk University in CRoCS laboratory (Centre for Research on Cryptography and Security). It can tell how much the input data are close to the referential random data.[2] To achieve this EACirc uses raw computation power. However, the computations are not run in parallel. If it was the case the whole process would be significantly speeded-up. Faster evaluation could advance capabilities of EACirc and help to test the randomness in a more detailed manner. Speeding-up the EACirc is the primary objective of this thesis.

The speed-up of EACirc is achieved with running some chosen computations on a GPU. The GPU must have got a build-in support of a general purpose programming (GPGPU). Such chip can perform not only algorithms used in rendering of computer graphics but also almost every other algorithm that is runnable on a CPU. The main difference in comparison with CPU is that the CPU is optimized to minimize latency whereas GPU is optimized to maximize throughput. Latency is the time needed to start and finish the execution of a single instruction including time to load necessary data. On the other hand, throughput is a number which means how many instructions can be processed per one time unit. [2] Since some parts of EACirc process a lot of data with algorithms which does not need to be optimized for latency[3] the use of GPU's is suitable.

Several different solutions exist on the market which can be used for GPGPU programming. Each solution provides different special features. The solution used

---

1. The one who wants to know the hidden content of the encrypted communication without permission of legal participants.
2. This is only an approximative explanation. The exact definition and meaning of EACirc results are described in Martin Ukrop's thesis Usage of evolvable circuit for statistical testing of randomness [1] since the accurate understanding of EACirc tool is not relevant for this thesis.
3. An algorithm that needs to be optimized for latency in order to maximize performance is that one which has lots of edges in it's control flow graph.

for this thesis is called CUDA [3] and it is a proprietary technology developed by NVIDIA. [4] The decision to use CUDA was taken by my advisor.

Since the performance of GPGPU is dependable on the used hardware the achieved speed-up was measured by an experimental method. The benchmarks took place particularly on machines which are being used at CRoCS laboratory for their own computations and are capable to run CUDA programs.

To set EACirc project for using CUDA, a non-trivial intervention into the settings of the project was needed. If the original settings of EACirc had been applied then this intervention would have resulted into a chaotic and further unmaintainable project. Therefore, in addition to the primary objective of this thesis to speed-up EACirc, the secondary objective is to remade the settings completely from scratch in order to prevent the problems that emerged by using CUDA. For this purpose an open-source tool CMake [5] was used that was developed by Kitware corporation [6].

2 CUDA

As stated on the NVIDIA website [3], "CUDA is a parallel computing platform and programming model that enables dramatic increases in computing performance by harnessing the power of the graphics processing unit (GPU)." The strengths and weaknesses of GPU lie in it's architecture and in differences from CPU. A GPU that is able to execute CUDA programs is addressed as *CUDA capable device* or simply as the *device*.

Figure 2.1: "The GPU Devotes More Transistors to Data Processing." NVIDA. [7]

The figure 2.1 shows a high level view of the CPU and GPU architecture. They both contain the same parts: DRAM, Cache, Control, and ALU. DRAM and Cache are memory units, the difference is that Cache is much smaller but significantly faster. The Control unit is responsible mainly for instruction fetching, decoding, etc. ALU is simply a worker that processes the input data. CPU's Control unit and Cache is much bigger and focuses on flow control and data caching in order to reduce the latency. The GPU's counterparts are simpler but multiplied, which allows to focus on data processing (throughput) and data parallelism. It is worth mentioning that the DRAM of a GPU is significantly faster in order to supply enough data to the big number of ALUs and to keep them busy.[1]

The performance of GPU is mainly measured by two variables: throughput and memory bandwidth. Since GPU is mainly used to compute with real numbers throughput[2] is expressed in units of floating-point operations per second (FLOPS).[3] Memory bandwidth is the amount of data that can be processed per unit of time which is expressed in units of bytes per second (Bps). [2] The figures 2.2 and 2.3 show the theoretical maximum performance achievable on NVIDIA GPU's in contrast to Intel CPU's in terms of throughput and bandwidth.

1. The memory model of GPU is described in section 2.3.
2. For definition of throughput see section 1.
3. Floating-point operation is an operation on floating-point numbers which in informatics represents real numbers according to the international standard IEEE 754.

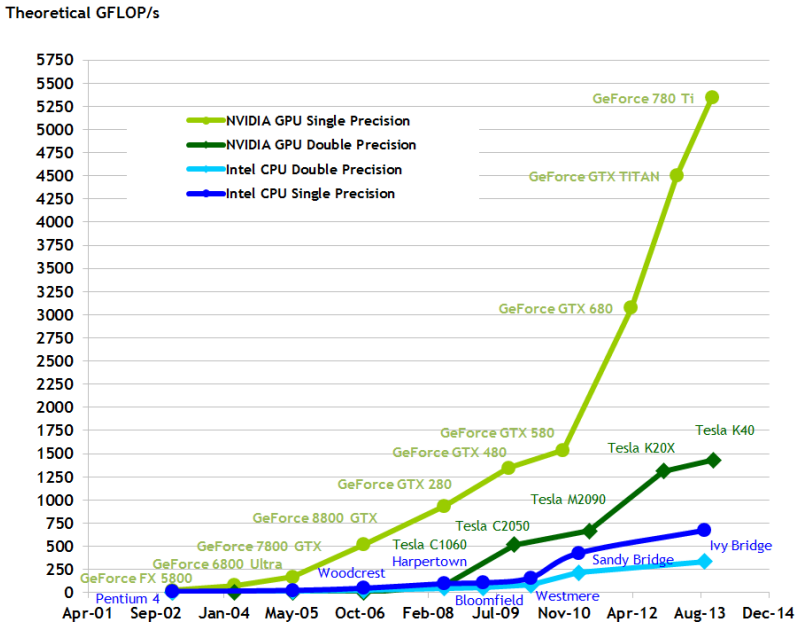

Figure 2.2: GPU vs CPU theoretical throughput. "Floating-Point Operations per Second for the CPU and GPU," NVIDIA. [7]

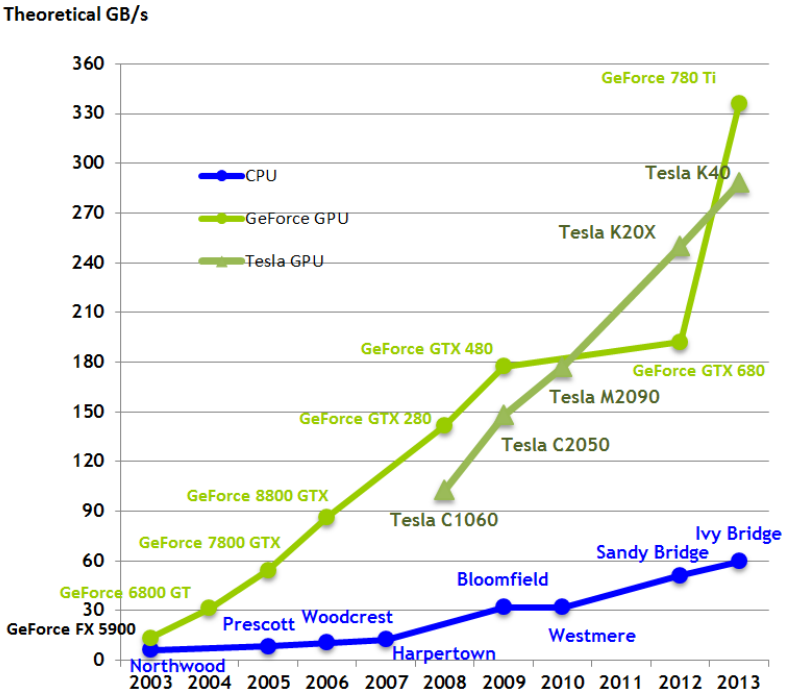

Figure 2.3: GPU vs CPU theoretical bandwidth. "Memory Bandwidth for the CPU and GPU." NVIDIA. [7]

2.1 Hardware architecture

In both, CPUs and GPUs, DRAM (figure 2.1) is significantly slower than ALU. If an ALU requires some data from DRAM, the ALU must wait hundreds of clock cycles for the data to became available (see latency). The waiting is highly ineffective and it is usually solved with some technique for latency-hiding. One of these techniques is executing another thread's instruction which has its data available. The difference between CPU and GPU is how often happens that an instruction wants data from DRAM.

Current CPUs use SIMD (Single Instruction, Multiple Data) execution model. [2] It processes a vector of data with only one instruction. The data in CPU are cached massively to reduce latency[4] and so the ALU does not need to wait. Thus, if big data are not accessed in a wrong way the probability of cache miss is low and switching context to a different thread can be relatively expensive operation.

The execution model of CUDA is called SIMT (Single Instruction, Multiple Threads). [2] Instead of vector of data, a *vector of threads* is executed with one instruction simultaneously. The vector of threads resides in one of the control units. Each thread of the execution vector is then mapped to an ALU related to the control unit. Each control unit has it's own cache. Since the cache is smaller, the cache miss is going to happen more often and another vector of threads, which has all its resources available, is executed. The switching of a thread context is done instantly with null overhead.[5] Therefore, to keep the GPU busy, more threads than the number of ALUs must be running.

In CUDA terminology the control units are called *Streaming Multiprocessors* (SMs). Each SM has its own ALUs referred to as *cores*. The single thread vector is composed of 32 threads and this is called *warp*. The SIMT architecture implies that all threads of the warp are performing the same instruction simultaneously at the same time. [7]

2.2 Thread hierarchy

The SIMT architecture of GPU is well suited and designed for computational problems that can be optimized using data parallelism. [2] Data parallelism is a parallelization technique that divides the input data to the independent parts and executes them separately (but evenly) on parallel computing nodes. The final result is then composed from each sub-result. [8] CUDA platform supports this technique through kernels and thread hierarchy.

---

4. Data caching is a technique to avoid waiting for data which are stored in a slow storage by introducing memory hierarchy. When data are requested they are firstly searched for in faster memory. When they are not found (cache miss) then a slower memory is searched as long as they are found. Then they are promoted to the faster memory to become available to subsequent requests (cache hit). The data stored in cache which were not accessed for a long time are replaced with a new ones.
5. The section 2.3 describes how is this achieved.

In CUDA context a *kernel* is a top-level function that is runnable on CUDA capable devices. [7] It is recommended that the kernel processes only the smallest portion of input data that can be processed separately. [8] For instance, when adding two vectors the kernel should just add two corresponding scalars of the vector.

For each kernel that is running a separate lightweight thread is created on the device. As shown in figure 2.4 a group of threads is forming a *block* and a group of blocks is forming a *grid*. Each thread has got unique ID dependant on its position in the block and each block has unique ID dependant on its position in the grid.[6]

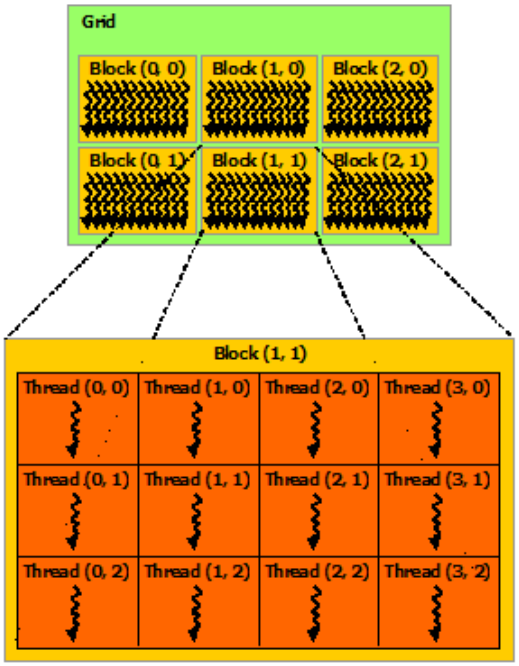

Figure 2.4: "Grid of Thread Blocks." NVIDIA. [7]

The dimensions of the grid should correspond to the dimensions of the computational problem. In the example of adding vectors the grid should have the same width as the number of scalars in the vector. Since each thread has a unique ID the kernel knows which scalars to add and where to put the result into the final vector.

The execution of a single kernel is initiated as soon as the device has enough available resources to run a whole block.[7] [7] This constraint allows that the threads of one block can communicate with each other (see section 2.3) and that the computational problem can be scaled across different types of CUDA GPUs that disposes with other hardware capabilities.[8] [9] The execution order of the blocks is not defined.

6. The grid might have up to 3 dimensions. [7]
7. Threads of the same block are running concurrently.
8. For instance the number of cores or available memory.
9. Any program scales if and only if a similar performance is achieved for arbitrary size of input data or across different hardware. [9] It is recommended that any well optimized program for CUDA scales.

To fully utilize the device the size of the block should be multiple of a warp size[10]. Each block is mapped to a single SM.[11] On a single SM several blocks may be active but the exact number is dependant on the GPU hardware parameters. Depending of the number of SMs several block may be run in parallel. This is fully done automatically by the CUDA platform. However, the programmer should know these constraints to produce optimized code for each device.[12]

2.3 Memory hierarchy

CUDA devices dispose with a multi level memory model. Each level differs in size, speed, and accessibility. The main levels are *global memory*, *shared memory*, and *local memory*.[13] [7]

The global memory is the slowest and the biggest. The data living in the global memory are accessible everywhere in the device. The access to the data is done via 32-, 64-, or 128-byte transactions. The access should fulfil several constraints to achieve maximum performance. One of these restrictions is a coalesced access.[14] The coalesced access appears if every thread in the block order reads or writes on the subsequent address simultaneously. The global memory should be mainly used for kernel's input/output data and the number of accesses should be minimal.

The shared memory is fast. It is almost as fast as registers and hundreds of times faster than the global memory. It resides in Streaming Multiprocessor's (SM) cache. The data are accessible only by threads of the same block. The number of running blocks on SM is mainly determined by the size of the shared memory required for a single block, which should be known before the block starts executing. Again, there are access restriction for maximum performance. The address space of the memory is alternately divided into 32 (warp size) memory banks of size 32- or 64-bytes. Each thread of the warp should access the different memory bank, which will result in only one transaction. Otherwise the access would be serialized to the number of transactions depending on the maximum number of accesses to one memory bank.[15]

The performance of the local memory is almost the same as of the global memory which is slow. The data lives only for the lifespan of a thread and is accessible only by the owning thread. The local memory is only used in a few scenarios described in CUDA C Programming guide [7] in section Device Memory Accesses.

---

10. For current devices the warp size is 32 (see. section 2.1).
11. For definition of Streaming multiprocessor (SM) see 2.1.
12. For various optimization techniques for CUDA platform see [9].
13. In heterogeneous programming the GPU global memory is denoted as subset of *device memory* and CPU memory is denoted as *host memory*. More about heterogeneous programming is in section 2.4.
14. Other constraints are not relevant for this thesis.
15. If multiple threads are requesting value from one address the access will not be serialized but the value will be broadcast resulting only in one transaction.

Besides global, shared and local levels of memory a *constant memory* exists.[16] [7] It is a special kind of memory that is meant for constants and is implemented in almost the same way as the global memory. A single access to the constant memory is as slow as an access to the global memory. Since the data in this memory are constants (read-only values) they can be massively cached and the subsequent readings are as fast as readings from shared memory. Lifespan of the data living in the constant memory is the same as of the data living in the global memory.

Every other suitable variable of the scope of a kernel is placed into register. Registers are very fast. The number of registers for each Streaming Multiprocessor (SM) is large so that each SM may have a lot of active threads and to switch their context easily.[17] The number of active blocks and threads is determined by the count of used registers by one kernel.

2.4 Heterogeneous programming

A heterogeneous system is a system composed of more than one kind of processor. [2] The CUDA philosophy supposes that CUDA executes on a physically separate *device* (GPU) that acts as a coprocessor to the program that is running on the *host* (CPU). The state of the device and the host is stored in their own physically separate memory space referred to as the *device memory* and the *host memory*. Therefore, the host program is in charge of the device resources and manages launching of kernels. [7]

The most often used scenario of kernel launch including device and host resource management is as follows:

1. Host program allocates the space for the input and output data in the host memory.
2. Host program allocates the space for the input and output data in the device memory.
3. Host program populates the space for input data in the host memory.
4. Host program sends the input data to the device.
5. Host program configures and launches the kernel on the device.
6. Device program is executed.
7. Host program copies the final results from the the device to the host.
8. Host program processes the results.

Since most of these actions are input/output operations, they may be performed either synchronously or asynchronously.[18] The execution of the kernel on the device is always asynchronous. [7]

16. There is also a *texture memory* but its description is irrelevant for this thesis. For more informations see [7]
17. See SIMT architecture and switching of thread context in section 2.1.
18. A synchronous operation blocks execution of the host program for the duration of the operation. An asynchronous operation does not block the execution of the host program and the incoming/outgoing transmission can overlap with computation. The host program is then notified whether the asynchronous operation succeeded or failed. [10]

2.5 Compute capabilities

As producing an optimized code for CUDA devices is closely linked to their hardware parameters [9] and because with almost every new product line of NVIDIA GPUs new features are introduced, NVIDIA established a system for backward and forward compatibility. The GPUs were divided to the classes reflecting technical parameters and runtime features of CUDA platform. These classes are referred to as compute capabilities.[19].

2.6 Programming language

The main programming languages for CUDA are *C* and *C++* which are enriched by several CUDA specific keywords. Since *C++* is a high-level language, some *C++* features are not supported in the device code. The source code for the device and for the host may be mixed together and placed into one source file jointly. [7]

The listing 1 shows a sample of CUDA code which produces a sum of two vectors on the device. The sample follows the scenario of launching the kernel as described in section 2.4.

However, one caution should be remembered before porting an algorithm to the CUDA platform. If an algorithm contains an *if-then-else* statement and any thread of the warp evaluates the condition differently then the different execution paths are serialized. The execution paths merge after every thread of the warp finished its execution path. Fortunately some techniques exists to avoid this artefact. This principle also applies on other language control flow constructs such as loops, goto statements, etc. [7]

2.7 Tools

NVIDIA provides the necessary tools for the development on CUDA platform through CUDA Toolkit package. [11] The source files of CUDA programs must be compiled by a special compiler. The compiler that comes with the CUDA Toolkit is called `nvcc`. [12] The compiler supports mixing the code for the host with the code for the device. The `nvcc` identifies the code for the device and compiles it to an intermediate object file. The remaining code for the host is then forwarded to the ordinary compiler for *C/C++* like `gcc`, `clang`, or `cl`. The object files from the `nvcc` and the host compiler are then linked into the binary form using ordinary linker or by `nvcc`. Therefore, the formed binary includes both the code for the host and for the device.

Debugging of the device code is slightly different from debugging of the code for the host. It requires a special debugger. The one that comes with CUDA Toolkit is called `cuda-gdb`. [13] The interface of this tool is almost the same as the interface of the known Linux compiler `gdb`.

19. For full list of compute capabilities corresponding to the date of release of this thesis see CUDA C Programming Guide [7] section G. Compute Capabilities

```
// kernel definition (the __global__ keyword declares the kernel)
__global__ void vector_add_kernel( float* a, float* b, float* c )
{
        // the id of this thread in the block as a local variable
        int i = threadIdx.x;

        // add corresponding scalars of the vector and store the result
        // vectors a, b, and c are stored in the global memory
        c[i] = a[i] + b[i];
}

int main()
{
        float* host_a, * host_b, * host_c;
        float* device_a, * device_b, * device_c;

        // allocate vectors on the host
        cudaMallocHost( &host_a, SIZE * sizeof( float ) );
        cudaMallocHost( &host_b, SIZE * sizeof( float ) );
        cudaMallocHost( &host_c, SIZE * sizeof( float ) );

        // allocate vectors on the device
        cudaMalloc( &device_a, SIZE * sizeof( float ) );
        cudaMalloc( &device_b, SIZE * sizeof( float ) );
        cudaMalloc( &device_c, SIZE * sizeof( float ) );

        // copy input vectors from host to device
        cudaMemcpy( device_a, host_a, size, cudaMemcpyHostToDevice );
        cudaMemcpy( device_b, host_b, size, cudaMemcpyHostToDevice );

        // launch kernel with only 1 block of size SIZE
        // a special CUDA syntax is used
        vector_add_kernel<<< 1, SIZE >>>( device_a, device_b, device_c );

        // retrieve the result from device
        // although the launch of the kernel is asynchronous this function
        // waits untill the execution of the kernel is not finished
        cudaMemcpy( host_c, device_c, SIZE, cudaMemcpyDeviceToHost );

        // free memory on the device
        cudaFree( device_a );
        cudaFree( device_b );
        cudaFree( device_c );

        // free memory on the host
        cudaFreeHost( host_a );
        cudaFreeHost( host_b );
        cudaFreeHost( host_c );

        return 0;
}
```

Listing 1: A sample program of vector addition on CUDA platform.

3 CMake

To set EACirc project for using CUDA, an intervention into the settings of the project was needed. Below the original settings and workflow of EACirc are described. However, this settings had to be remade from scratch.

The EACirc sources consist mainly of *C* and *C++* code. The code is divided into reasonably logical sections, but the overall structure and concept of the project are monolithic.[1] This leads to compilation of all sources into one big executable of approximately 9 MB, which takes some non-trivial time.

On top of this EACirc is developed as a cross-platform application. To provide native builds for each supported platform (Windows [14] and Linux) a special makefile or an IDE specific project file are used simultaneously. They describe how to build the application. When a change in the build is introduced, e.g. a new source file is added, the change has to be manually implemented to all makefiles to provide consistency. This workflow is not easy to maintain as the violation of these rules can cause an uncomfortable pitfall.

To solve these problems the CMake [5] tool was integrated into the project of EACirc along with some changes of the basic structure of EACirc. The CMake tool is developed and maintained by Kitware, Inc. [6] as an open-source software. The main purpose of this tool is to provide native builds of cross-platform applications and to minimize the effort to maintain the project.

Although there are many similar tools as CMake and some of them provide better features they are not so widely supported. For instance, CMake generates project files for almost every common IDE and some of these IDEs come with a built-in support for CMake.

3.1 CMake toolset

The CMake is actually a set of several tools that provide for building, testing, and deploying of user's *C* or *C++* project. These tools can be installed on Linux, Windows, or MacOSX. The CMake toolkit consists of the main tool `cmake` and the supportive `ccmake` (or `cmake-gui`), `ctest`, and `cpack`. [15]

The `cmake` tool takes a configuration file called `CMakeLists.txt` distributed with the project source files and generates the platform specific makefiles as an output. Then the user invokes a platform specific tool for building – usually `make`, `ninja` [16], or `MSBuild`. [17] If the process is successful the native binaries of the project are now made.

The `ctest` tool provides a simple platform for project testing. If the build is successful the user can run some custom made tests on the binaries.

---

1. A monolithic binary is an executable that does not need any other dependencies or resources at a runtime. In other words, the binary is independent.

The `cpack` tool provides a cross-platform mean to deploy your application on the target system.

The remaining `ccmake` and `cmake-gui` are just more convenient ways to use a `cmake` tool since `cmake` has only a command line interface. The former provides a TUI[2] and the latter provides GUI[3].

3.2 A closer look at the `cmake` executable

The `cmake` executable is not just a dummy build-system. The process of generating a makefile is quite sophisticated. First, the user chooses the *source directory* and the *build directory* and then invokes the `cmake` command in a *build directory* with appropriate parameters. The subsequent process consists of several phases – selection of a native build-system (in a CMake terminology referenced as a *generator*), configuration based on a user-specific input, and the generation of a makefile itself.[4] [15]

The *source directory* is simply a directory where the project sources are located as well as the top-level `CMakeLists.txt` file which is distributed with the sources. The build directory is an empty user-created directory in which the user wants the binaries to be build.

The selection of the *generator* depends on the user's platform, on the user-installed native build-systems, and on the user's intentions. The generator used on Linux is usually `make` or `ninja`. If the user wants to generate project files to a specific IDE, appropriate generator can be chosen – e.g. Visual Studio 2013 [18] on Microsoft Windows [14]. Usually the selection of the appropriate generator is done by CMake automatically.

The subsequent phase is configuration. Here the user specifies variable options for the build that the project supports. For instance, some features of the application can be switched on/off or the location of a third party dependencies can be specified. Also the different build configuration can be switched, i.e. release or debug.

If the configuration is correct then the makefile is successfully created in the *build directory*. Then the user just invokes the appropriate tool to execute the makefile and the binaries are build.

It is worth mentioning that the makefile automatically detects any changes made in the *source directory*. So the user invokes the `cmake` executable just once to generate the makefile or to change the variable options of the build. The makefile also provides a way to install the application and/or to test it.

The minimal and the most common sequence of commands to build and install a project on Linux using the CMake is shown in listing 2.

---

2. Text-based user interface (TUI)
3. Graphical user interface (GUI)
4. Note that the exact scheme of this process can differ according to which interface of CMake is used – i.e. `cmake`, `ccmake`, or `cmake-gui`.

```
mkdir <build_directory>
cd <build_directory>
cmake <path_to_source_directory>
make
make install
```

Listing 2: The minimal CMake workflow.

Note that the `make` is chosen as a default generator. In addition, the default project settings and configurations are applied. The binaries are installed to the platform specific location, i.e. on Linux it is `/usr/share/local`.

3.3 Changes made to the EACirc repository structure

There were several changes made to the EACirc repository structure. The new folder design reflects the logical structure of the EACirc philosophy. The changes are shown in the figure 3.1.

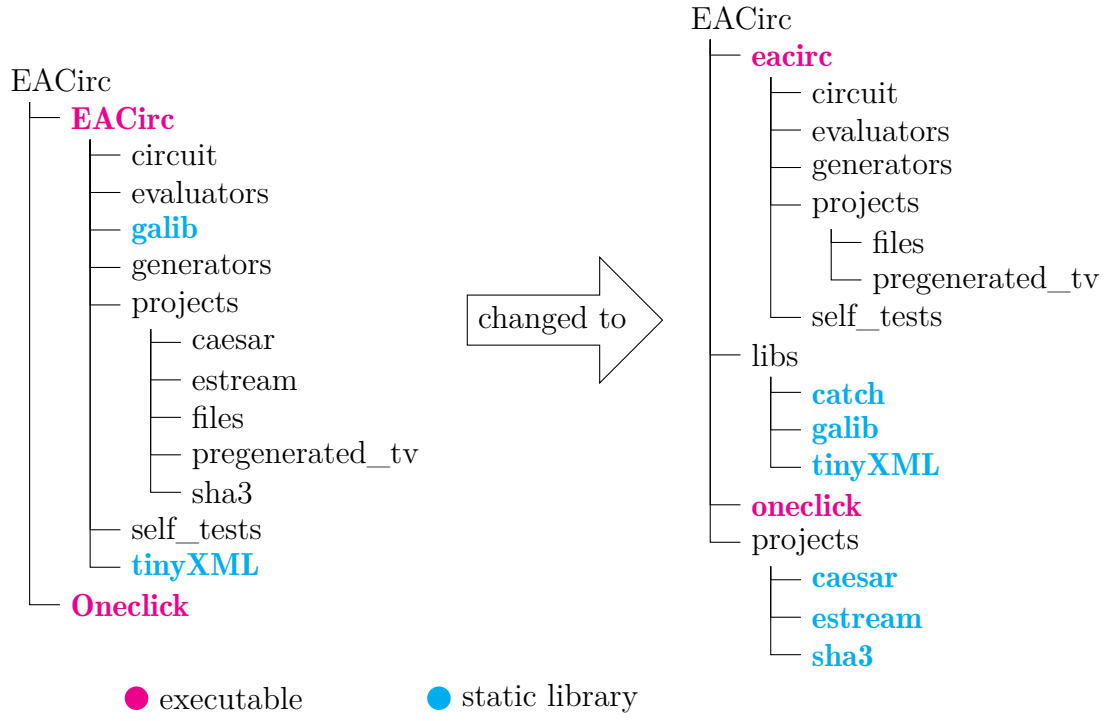

Figure 3.1: Old vs. new repository structure

The first and also the smallest change was to name all source folders with only small letters. Next the libraries from 3rd party providers `catch`, `galib`, and `tinyXML` were moved into the separate folder – the *libs* directory.

Then the so called *projects* were isolated. A *project* in EACirc terminology means a problem solving module. These *projects* are `caesar`, `estream`, `sha3`, `files` and `pregenerated_tv`. Since `files` and `pregenerated_tv` are both just small modules consisting of only one source file, it would be impractical to isolate them. Whereas the big modules `caesar`, `estream`, and `sha3` were moved to the separate folder called the *projects* folder. Each of the isolated projects was remade to compile into a static library.[5]

The content of folders `eacirc` and `oneclick` is build into executables which are named accordingly to their corresponding folder. The *projects* which are now compiled into the static libraries are now statically linked to the `eacirc` executable representing the EACirc tool as a whole. The `oneclick` executable is a supportive tool for the automated task management developed by Ľubomír Obrátil. [19]

3.4 The new build-system of EACirc

The new build-system is written on the CMake platform. This platform allows to define custom options for generating the build. A descriptive list of EACirc specific options is given below:

`BUILD_ONECLICK`
: Enable building of Oneclick, the supportive tool for EACirc.

`BUILD_CAESAR`
: Enable building of the Caesar project.

`BUILD_ESTREAM`
: Enable building of the Estream project.

`BUILD_SHA3`
: Enable building of the SHA-3 project.

`BUILD_CUDA`
: Enable to build the support for CUDA devices. This option is available only if the CUDA Toolkit [11] is installed on the build machine[6] and found by the CMake.

Since the *projects* are build into static libraries they must be linked to the `eacirc` executable at the compile time. This is done automatically when the option for the specific *project* is enabled. In the figure 3.2 dependencies of all the build targets are shown.

The build-system is also version aware. The current version is stored in the `eacirc/Version.h` header file. The version corresponds to git commit hash [20]. This means that for the correct build generation git tools must be properly installed on the build machine and found by CMake.[8]

---

5. There is a plan to remake the projects to modules loaded dynamically at runtime. This would require to compile them separately into the dynamic libraries.
6. A build machine is a physical or a virtual machine that is used to build the project.
8. If git tools are installed and not found automatically by CMake then the path to git tools can be specified manually.

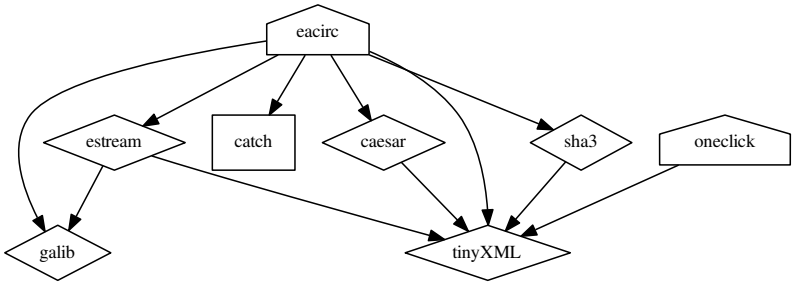

Figure 3.2: EAcirc dependency graph

The static libraries are shown in the rhombus. The executables have a house around them, squares represent interface libraries[7] and the direction of arrows describes dependency of build targets.

The use of CMake and the new options of building EACirc is explained in detail on the Github wiki project page under the Building EACirc section.

3.5 Project settings for CUDA

It is now much easier to set the project for CUDA support with CMake than with ordinal makefiles. When the CUDA Toolkit [11] is installed and automatically found by CMake[9] then the option `BUILD_CUDA` becomes available. If this option is enabled then the `eacirc` executable is build by using Nvidia `nvcc` compiler [12] and the C preprocessor macro `CUDA` is defined causing that the executable will be runnable on CUDA capable devices. When writing a code for CUDA the preprocessor macro `CUDA` can be queried.

9. If CUDA Toolkit is installed on the build machine but not found by CMake automatically then the path to CUDA Toolkit can be specified manually.

4 Gate Circuit of EACirc

The purpose of EACirc is to differentiate input data and a referential random data from one another without any context. The input data consists of thousands of sample outputs from an arbitrary random generator which are referred to as *input vectors*. The distinction is done by creating a gate circuit which processes the input data and outputs the result. The internal structure of the optimal gate circuit is unknown at the moment of invocation of the EACirc program. However, the optimal form of the circuit is constructed via a genetic algorithm. [1]

Genetic algorithms are inspired by processes of reproduction and natural selection in living systems. They are searching for a satisfactory optimal solution for a given problem. The process of producing the acceptable solution consists of creating a random initial generation of individuals and then iteratively applying evaluation of the generation, selection of the best individuals for the next generation, and creating next generation by applying genetic operators. [21]

The functionality of the gate circuit in EACirc is the same as an ordinary digital circuit that is composed from electronic components (*gates*) connected with wires (*connectors*). Each gate is performing some logical function on its input defined by connectors. The whole circuit takes one input vector, which is a fixed amount of logical data, and outputs if the input is random or not.[1] Since the gate circuit, in the context of EACirc, is stored in memory of a computer, the implementation differs from the real world.

Producing the final gate circuit via genetic algorithm is an iterative process. In each iteration a whole generation of circuits must be evaluated. The evaluation of a single circuit is done by processing all of the input vectors. All of these parts of the process must be done in large quantities to ensure quality and that is a computationally intensive task. Fortunately, the evaluation of a single circuit and even the evaluation of the whole generation can be run effectively in parallel. This thesis focuses mainly on parallelization of evaluation of a single circuit.

The evaluation of a single circuit is suitable for parallelization, particularly for data parallelism on GPGPU and CUDA platform. The size of the input data is relatively small (usually 16 KiB or more)[2] The input data are a set of input vectors (usually 1000 vectors). Each input vector is evaluated separately by the same circuit, which usually outputs only 1 byte of data. Therefore, the data transfers between host and device via a *slow* PCIe bus will be small.[3] The data parallelism can be achieved by mapping of execution of single input data to separate device thread. Single circuit

---

1. Actually the output of a circuit is not only a binary (random/non-random) but contains several other informations that are further processed.
2. The exact parameters of the circuit are runtime variables. The reported values in parenthesis are just the most used but if running on CUDA, bigger values are expected.
3. The PCIe bus has got a big latency, thus the number of transfers must be minimized or the transfers must be buffered.

processes different data equally, i.e. the data are different but the execution paths of multiple running circuits are same.

4.1 Software representation of hardware circuit

Follows the description of the CPU implementation and functionality of the gate circuit designed by Martin Ukrop. [1] This representation served as starting artwork for the GPU implementation.

From informatics point of view the gate circuit can be described as directed acyclic graph (DAG) with some other restrictions described further. Each node represents some logical function (*gate*), the edges (*connectors*) of the vertices represents inputs for the individual logical functions and the flow of data. The graph is divided into several layers. Every node in each layer is connected only to nodes which belongs to the previous layer. For an illustration of the circuit see figure 4.1.

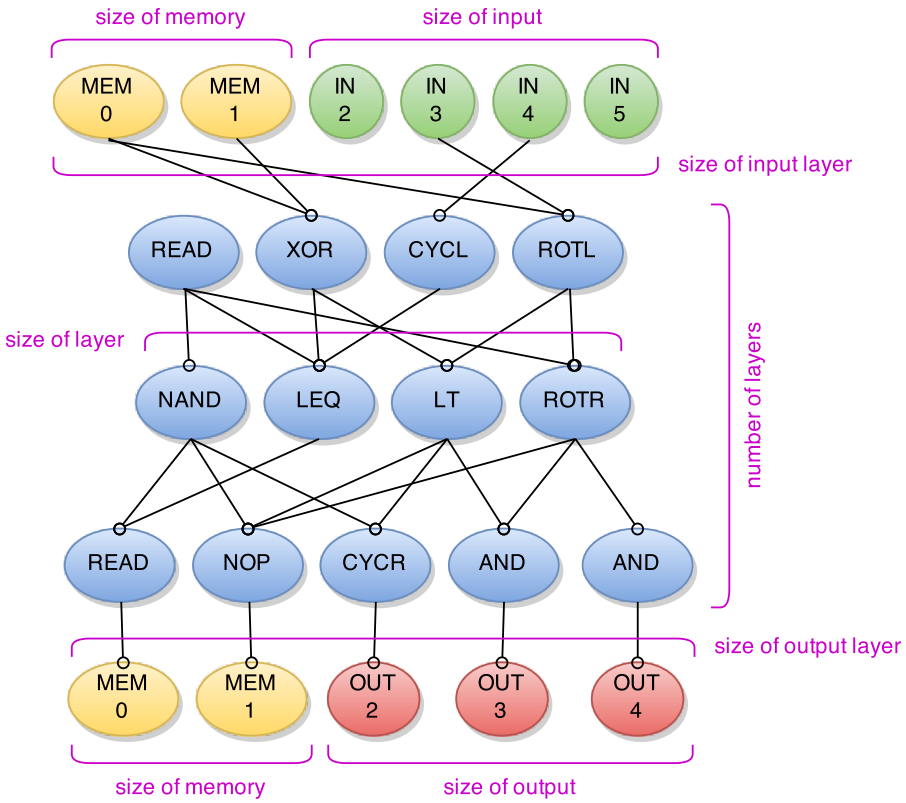

Figure 4.1: The dimensions of the gate circuit

TODO use memory
TODO size of layers

4.2 CPU implementation

In computer memory the gate circuit is represented as an 1-dimensional array of 32-bit unsigned integers. Each integer has its own meaning. The array is alternately divided into connection layers and function layers as shown in the figure 4.2. Each layer is aligned to multiple of *genome_width*.

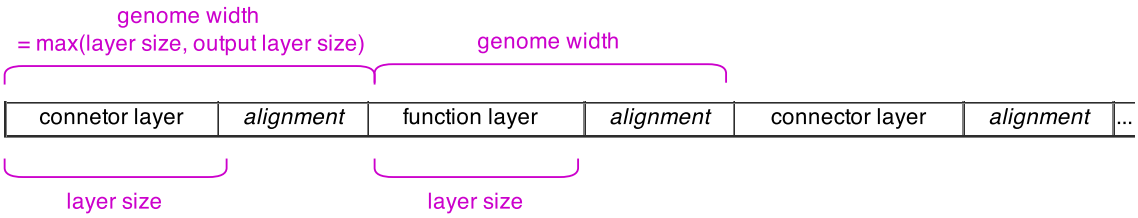

Figure 4.2: The representation of gate circuit in CPU memory.

4.2.1 Connector layers

The connection layers contains connectors masks which are represented as 32-bit unsigned integers. Every node has assigned its own connector mask. If the i-th bit of the connector mask is `true` then exists connection from the n-th node of the previous layer to the node the connector is assigned to, where n depends on the connector type. There are two types of connectors which are convertible to one another. The types are *absolute connectors* and *relative connectors*.

Relative connector is a representation of a connection which is defined through relative positioning to the node it belongs to. This representation is used in genetic algorithm when creating new generation, i.e. if the circuit is cut in half and crossed with another individual[4] the connector remains still valid.

Absolute connector is an representation of a connection by absolute positioning. This positioning is used when the circuit is being executed because then the process of resolving the absolute connector is much faster then resolving the relative connector.

4.2.2 Function layers

The function layers contains function masks which are represented as 32-bit unsigned integers. Every node has assigned its own function mask. The mask contains information about the function type and arguments.

4.2.3 Circuit interpreter

TODO

4. Crossing of individuals is one of the types of genetic operators used for creating a new generation of individuals.

4.3 GPU implementation

5 Conclusions and future work

Bibliography

[1] M. Ukrop, "Usage of evolvable circuit for statistical testing of randomness", Bachelor thesis, FI MU, 2013.

[2] J. Cheng, M. Grossman, and T. McKercher, *Professional CUDA ® C Programming*. Wrox, Sep. 9, 2014, ISBN: 978-1118739327.

[3] Nvidia Corporation. (2015). About CUDA, [Online]. Available: https://developer.nvidia.com/about-cuda.

[4] ——, (2015). Welcome to NVIDIA - World Leader in Visual Computing Technologies, [Online]. Available: http://www.nvidia.com.

[5] Kitware Inc. (2015). CMake, [Online]. Available: http://www.cmake.org/ (visited on 03/08/2015).

[6] ——, (2015). Kitware Inc. – leading edge, high-quality software, [Online]. Available: http://www.kitware.com/ (visited on 03/08/2015).

[7] Nvidia Corporation, *CUDA C Programming Guide*, Mar. 2015.

[8] W. D. Hillis and G. L. Steele Jr., "Data parallel algorithms", *Commun. ACM*, vol. 29, no. 12, pp. 1170–1183, Dec. 1986, ISSN: 0001-0782. DOI: 10.1145/7902.7903. [Online]. Available: http://doi.acm.org/10.1145/7902.7903.

[9] Nvidia Corporation, *CUDA C Best Practices Guide*, Mar. 2015.

[10] Microsoft. (2015). Synchronous and Asynchronous I/O (Windows), [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/aa365683(v=vs.85).aspx (visited on 05/06/2015).

[11] NVIDIA Corporation. (2015). CUDA Toolkit, [Online]. Available: https://developer.nvidia.com/cuda-toolkit.

[12] Nvidia Corporation, *CUDA Compiler Driver NVCC*, Mar. 2015.

[13] ——, *CUDA-GDB CUDA Debugger*, Mar. 2015.

[14] Microsoft. (2015). Windows – Microsoft Windows, [Online]. Available: http://windows.microsoft.com.

[15] Kitware, Inc. (2014). CMake Reference Documentation – CMake 3.0.2 Documentation, [Online]. Available: http://www.cmake.org/cmake/help/v3.0/.

[16] E. Martin. (Nov. 24, 2014). Ninja, a small build system with a focus on speed, [Online]. Available: https://martine.github.io/ninja/.

[17] Microsoft. (2015). MSBuild, [Online]. Available: https://msdn.microsoft.com/en-us/library/dd393574.aspx.

[18] ——, (2015). Visual Studio – Microsoft Developer Tools, [Online]. Available: https://www.visualstudio.com/.

[19] L. Obrátil, "Automated task management for EACirc and BOING", Bachelor thesis, FI MUNI, 2015.

[20] S. Chacon and B. Straub, *Pro Git*, 2nd editon. Apress, Dec. 24, 2014, ISBN: 978-1484200773.

[21] N. Pillay, "A genetic programming system for the induction of iterative solution algorithms to novice procedural programming problems", in *Proceedings of the 2005 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries*, ser. SAICSIT '05, White River, South Africa: South African Institute for Computer Scientists and Information Technologists, 2005, pp. 66–77, ISBN: 1-59593-258-5. [Online]. Available: http://dl.acm.org/citation.cfm?id=1145675.1145683.