USE OF GRAPHIC CARDS FOR HIGH PERFORMANCE COMPUTING

Jaromír Kuchyňka

High School Student (4), Purkyně Grammar school, Strážnice

E-mail: Jaromir.Kitchenet@outlook.com

Supervised by: Jan Hajný

E-mail: hajny@feec.vutbr.cz

Abstract: We live in the Information Age. Computer data is more valuable today than ever before and that is why it must be strongly protected. One of tools, that can be used to make our data safe, is encryption. This work deals with the probably uttermost pitfall of encryption – high time demand. The high performance of modern graphic cards can reduce the required amount of time. The aim of this work is to test and measure the performance of CPU and GPU in cryptography computation and summarize the results.

Keywords: encryption, graphics cards, high performance computing

1. ÚVOD

Kryptografie, jakožto oblast úzce související s informačními systémy, je v současnosti na vzestupu. Díky novým technologiím, jež se stále překotně vyvíjejí, dosahují nové technické komponenty vlastností, které byly ještě před pár lety nemyslitelné. Pro kryptologii znamenal tento posun nutnost reflektovat situaci. Byly tvořeny postupy, šifry a programy, s nimiž bylo možné maximalizovat výpočetní potenciál moderních zařízení.

K dosáhnutí většího stupně bezpečnosti šifrování je potřeba využívat operace s velmi velkými čísly, které následně znemožňují útočníkovi prolomit šifru v „rozumném“ čase. To ovšem samozřejmě vede k vyšším časovým nárokům, jež musí odrážet výpočetní výkon technických prostředků.

Ukazuje se, že využití grafických karet může být krokem správným směrem pro dosáhnutí nižších časových požadavků šifrování. Hlavní činnost této práce je tudíž směřována na zprovoznění, testování a zhodnocení knihovny CUMP, vytvořené pro využití výkonu grafických karet značky NVIDIA podporujících architekturu CUDA. Použitím této knihovny urychlíme celkový výpočet jeho rozdělením na velké množství mezivýpočtů, které jsou počítány paralelně.

Výsledky práce jsou zpracovány dokumentu, v němž lze nalézt podrobný návod, jak uvést veškeré potřebné programové prostředky spolu s knihovnou do chodu. Obsahuje ale také srovnání naměřených hodnot získaných na procesoru AMD PhenomII X2 555 a na grafické kartě NVIDIA GeForce GT 640.

2. UŽITÉ PROGRAMOVÉ PROSTŘEDKY

Ještě před zahájením měření výpočtů bylo nutné nahrát do počítače správné programové prostředky a nastavit je. Knihovna CUMP, jež byla klíčová pro celou práci, funguje nejlépe na 64bit operačních systémech na bázi Linuxu; z těchto byl zvolen OS Ubuntu 13.04 64bit. Dále bylo třeba nainstalovat balík CUDA Toolkit verze 5.5 starající se o ovládání grafické karty, který také poskytnul vývojové prostředí Eclipse Nsight pro tvorbu a kompilaci kódů. Poté zbývaly jen instalace knihoven GMP a CUMP.

2.1. GMP

The GNU Multiple Precision Arithmetic Library je open source počítačová knihovna určená pro počítání s teoreticky libovolně velkými čísly a jakýmikoliv aritmetickými operacemi. Jediné, čím je limitována, jsou technické parametry stroje, na kterém pracuje. Knihovna se orientuje na maximální zrychlení provádění výpočtu, díky čemuž je využívána především v oblasti kryptografie, výzkumu a bezpečnostních aplikacích [1].

2.2. CUMP

Knihovna CUDA Multiple Precision Arithmetic Library je založená na jádru GMP. Ovšem hlavními rozdíly knihoven jsou jejich rozsah, neboť CUMP obsahuje pouze aritmetické operace sčítání, odčítání a násobení, a konečné zařízení, na němž operují, protože CUMP, na rozdíl od GMP, jehož platformou jsou procesory, umožňuje práci s grafickou kartou [2].

3. MĚŘENÍ

S nainstalovanými programovými prostředky mohlo začít samotné programování, jehož výstupem bylo v konečné fázi 36 projektů, které se dělily do dvou stejně velkých hlavních skupin podle toho, zda počítaly na procesoru či grafické kartě. Těchto 18 projektů, se již od sebe lišilo pouze minimálně, a to počtem čísel, s kterými operovaly, anebo velikostí čísel. Naopak společnými znaky bylo provádění násobení dvou polí s pevně daným počtem náhodně generovaných prvků a měření času v tisíckrát opakujícím se cyklu, který nakonec vrátil průměrnou hodnotu.

Všechna měření byla provedena třikrát a uvedená výsledná hodnota je aritmetickým průměrem třech naměřených časů z každého projektu. Výsledky jsou uvedeny v tabulkách 1 až 3. Pro větší názornost je k dispozici také graf (obrázek), jehož osa x je zobrazena v logaritmickém měřítku.

Tabulka 1: Naměřené hodnoty pro 1024b čísla.

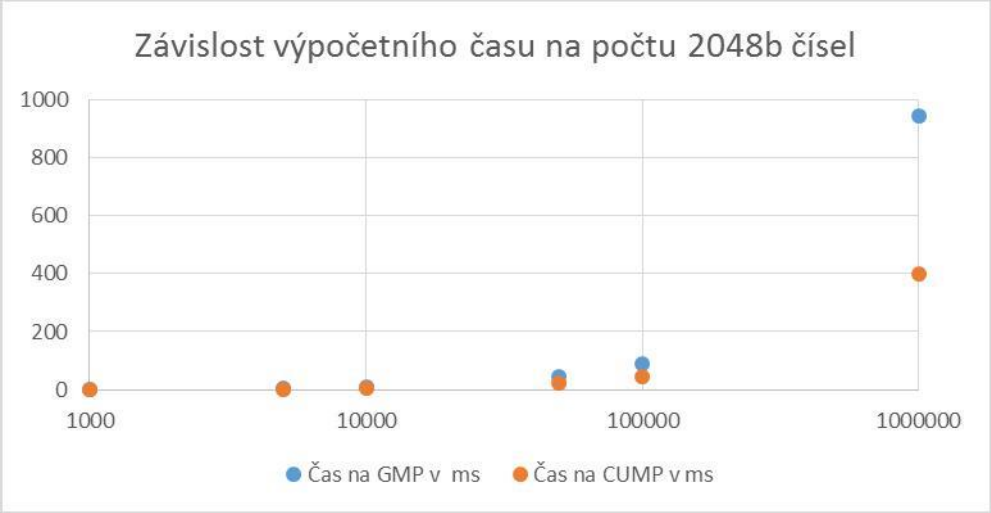
Počet 1024b čísel	Čas na GMP v ms	Čas na CUMP v ms
1000	0,258	0,243
5000	1,399	0,921
10000	2,823	1,501
50000	15,395	6,044
100000	31,347	11,602
1000000	341,857	98,725

Tabulka 2: Naměřené hodnoty pro 1536b čísla

Počet 1536b čísel	Čas na GMP v ms	Čas na CUMP v ms
1000	0,526	0,407
5000	2,682	1,777
10000	5,567	2,922
50000	28,111	12,754
100000	56,753	25,042
1000000	578,312	203,581

Tabulka 3: Naměřené hodnoty pro 2048b čísla

Počet 2048b čísel	Čas na GMP v ms	Čas na CUMP v ms
1000	0,791	0,647
5000	4,028	2,665
10000	8,798	5,165
50000	43,656	23,276
100000	89,586	45,629
1000000	942,177	397,641



Obrázek 1: Graf závislosti času na počtu operací

4. ZÁVĚR

Všechny vytyčené cíle byly splněny, jen lehce mrzí nemožnost testování většího počtu čísel, z nichž by bylo možné poskytnout relevantnější data a získat případné limity knihoven. Napravení tohoto neznámého problému bude ovšem určitě předmětem další aktivity autora práce.

Z celkového hlediska je ale práce úspěšná. Potřebné programové prostředky byly nainstalovány a následná měření proběhla bez větších obtíží. Z grafu lze pozorovat exponenciální závislost času na počtu operací a i získané výsledky odpovídají předpokladu, neboť grafická karta je rychlejší než procesor, přičemž tento rozdíl je názornější při větší náročnosti výpočtu. Velmi důležité je také zjištění, že výkonnostní rozdíl mezi CPU a GPU se s narůstajícím počtem zpracovávaných čísel značně zvyšuje.

PODĚKOVÁNÍ

Tento příspěvek vznikl za podpory AV ČR a pod dohledem Ing. Jana Hajného, Ph.D.

REFERENCE

[1] The GNU MP Bignum Library. The GNU MP Bignum Library [online]. 2000 [cit. 2014-03-02]. Dostupné z: https://gmplib.org

[2] The CUDA Multiple Precision Arithmetic Library - CUMP. The CUDA Multiple Precision Arithmetic Library - CUMP [online]. 2012 [cit. 2014-03-02]. Dostupné z: http://www.hpcs.cs.tsukuba.ac.jp/~nakayama/cump/